TREND MICRO™

6.5 InterScan™ Web Security Virtual Appliance

Service Pack 2

Administrator's Guide

Antivirus and Content Security at the Web Gateway

Web Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Installation Guide, which are available from Trend Micro's Web site at:

http://www.trendmicro.com/download/documentation/

Release Date: August 2017

Protected by U.S. Patent No. 5,951,698

The Administrator's Guide for Trend Micro is intended to provide in-depth information about the main features of the software. You should read through it prior to installing or using the software.

For technical support, please refer to the Technical Support and Troubleshooting chapter for information and contact details. Detailed information about how to use specific features within the software are available in the Online Help file and online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Chapter 1: Introducing Trend Micro™ InterScan™ Web Security Virtual Appliance

Chapter 2: Deployment Wizard

Chapter 3: High Availability and Cluster Management for Transparent Bridge Mode

Chapter 4: Updates

Chapter 5: Application Control

Chapter 6: Bandwidth Control

Chapter 7: HTTP Configuration

Chapter 8: Policies and User Identification Method

Chapter 9: Configuring HTTP Scanning

Chapter 10: Access Quotas and URL Access Control

Chapter 11: URL Filtering

Chapter 12: FTP Scanning

Chapter 13: Command Line Interface Commands

Chapter 14: Reports, Logs, and Notifications

Chapter 15: Administration

Chapter 16: Testing and Configuring IWSVA

Appendix A: Contact Information and Web-based Resources

Appendix B: Mapping File Types to MIME Content-types

Appendix C: Architecture and Configuration Files

Appendix D: OpenLDAP Reference

Appendix E: Best Practices for IWSVA

Appendix F: WCCP Deployment & Troubleshooting

Appendix G: URL Filtering Category Mapping

Appendix H: URL Filtering Category Groups

Preface

Preface

Welcome to the *Trend Micro™ InterScan™ Web Security Virtual Appliance 6.5 SP2 Administrator's Guide*. This guide provides detailed information about the InterScan Web Security Virtual Appliance (IWSVA) configuration options. Topics include how to update your software to keep protection current against the latest risks, how to configure and use policies to support your security objectives, configuring scanning, configuring URL blocking and filtering, and using logs and reports.

This preface describes the following topics:

- *IWSVA Documentation*
- *Audience*
- *Document Conventions*
- *About Trend Micro*

IWSVA Documentation

In addition to the *Trend Micro™ InterScan Web Security Virtual Appliance Administrator's Guide*, the documentation set for IWSVA includes the following:

- **Installation Guide**—This guide helps you get "up and running" by introducing IWSVA, assisting with installation planning, implementation, and configuration, and describing the main post-upgrade configuration tasks. It also includes instructions on testing your installation using a harmless test virus, troubleshooting, and accessing Support.
- **Online Help**—The purpose of Online Help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online Help is accessible from the IWSVA Web console.
- **Readme file**—This file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and, release history.

  The latest versions of the Installation Guide, Administrator's Guide and readme file are available in electronic form at:

  `http://www.trendmicro.com/download/`
- **Knowledge Base**— The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  `http://esupport.trendmicro.com/en-us/business/pages/technical-support.aspx`
- **TrendEdge**—A program for Trend Micro employees, partners, and other interested parties that provides information on unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics.

  `http://trendedge.trendmicro.com`

Audience

The IWSVA documentation is written for IT managers and system administrators working in enterprise environments. The documentation assumes that the reader has in-depth knowledge of networks schemas, including details related to the following:

- HTTP, HTTPS, FTP and other Internet protocols used by an enterprise
- VMware ESX administration experience when installing on VMware ESX and Microsoft Hyper-V experience when installing on Hyper-V

The documentation does not assume the reader has any knowledge of antivirus or Web security technology.

Note: Silicom bypass cards are recognized by VMware and can be used as normal network cards.

Document Conventions

To help you locate and interpret information easily, the IWSVA documentation uses the following conventions.

TABLE 0-1. Document Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes

TABLE 0-1. Document Conventions (Continued)

CONVENTION	DESCRIPTION
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

About Trend Micro

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway-gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of risks to information, by offering centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point, before they ever reach the desktop.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

`http://www.trendmicro.com`

Chapter 1

Introducing Trend Micro™ InterScan™ Web Security Virtual Appliance

This chapter introduces the Trend Micro™ InterScan™ Web Security Virtual Appliance (IWSVA) and how it helps to ensure your organization's gateway security.

Topics in this chapter include the following:

Main Features

The following IWSVA features help you maintain Internet gateway security.

Application Control

The Application Control feature provides a security technology that automates the discovery of popular Internet applications and allows administrators to control them using policies. See details at: Application Control Overview on page 5-2.

Bandwidth Control

Bandwidth control reduces network congestion by controlling communications, reducing unwanted traffic and allowing critical traffic or services the appropriate bandwidth allocation. Bandwidth control gives all users fair access to resources and ensures better access to resources that are more central to the organization. See details at: Bandwidth Control on page 6-1.

HTTP Inspection

HTTP Inspection allows administrators to identify behavior and filter web traffic according to HTTP methods, URLs, and headers. It also allows them to create filters or use default filters to identify web traffic, as well as import and export filters. After the traffic is identified, IWSVA can control it according to policy settings that determine the appropriate actions for specific traffic. For example, an HTTP Inspection policy could prevent users from posting content on social networking or webmail sites while still allowing them to read content. See details at: HTTP Inspection Overview on page 9-3.

Data Loss Prevention

For convenience, IWSVA includes default content filtering data leakage prevention (DLP) policies. There are 10 default data leakage prevention policies configured by region. Compared to standard content filtering policies, keywords in the data leakage prevention policies are regular expression description strings and not the actual keyword.

For example, IBAN is the description for the regular expression:

[^\w](([A-Z]{2}\d{2}\s?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}\s){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}\s){2}[A-Za-z0-9]{3,4}))[^\w].

Messages that contain the string "IBAN" do not trigger this policy. Strings such as "BE68 5390 0754 7034 " will match the regular expression and trigger this policy.

Data Loss Prevention utilizes customizable data identifiers, templates, and policies to define, monitor, and protect your company-specific sensitive data from intentional or accidental loss.

Before you can monitor sensitive data for potential loss, you must be able to answer the following questions:

- What data needs protection from unauthorized users?
- How does the sensitive information transmit through the network?
- What users have permission to access or transmit the sensitive data?
- What action should occur if a security violation occurs?

This important audit typically involves multiple departments and personnel familiar with the sensitive information in your organization.

If you already defined your sensitive information and security policies, you can begin to define templates and company policies in the Data Loss Prevention system.

Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. You can define digital assets using the following data identifiers:

- **Expressions**: Data that has a certain structure. For details, see *Expressions* on page 1-3.
- **Keyword Lists**: A list of special words or phrases. For details, see *Keyword Lists* on page 1-4.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format “nnnn-nnnn-nnnn-nnnn,” making them suitable for expression-based detections.

Predefined Expressions

IWSVA comes with a set of predefined expressions. These expressions cannot be modified or deleted.

IWSVA verifies these expressions using pattern matching and mathematical equations. After IWSVA matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

Keyword Lists

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, “prognosis,” “blood type,” “vaccination,” and “physician” are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure IWSVA to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, “end,” “read,” “if,” and “at” can be combined to form keywords found in source codes, such as “END-IF,” “END-READ,” and “AT END.”

Predefined Keyword Lists

IWSVA comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

Data Loss Prevention Templates

Use Data Loss Prevention templates to tag and detect sensitive content by a set combination of data identifiers. A template combines data identifiers and operators (And, Or) in condition statements. When a set of data matches the criteria of a condition, Data Loss Prevention triggers a policy action. For example, a file containing data matching the All: Names from US Census Bureau AND US: HICN (Health Insurance Claim Number) templates, triggers the HIPAA policy.

You can use some Data Loss Prevention out-of-the-box templates for regulatory compliance initiatives, such as GLBA, PCI-DSS, SB-1386, US PII, and HIPAA. Companies can also create custom templates or modify existing templates to suit their business requirements. Companies that have pre-existing, user-defined templates can import and export templates to maintain policy consistency throughout their organization.

Data Loss Prevention Policies

Data Loss Prevention policies allow companies to monitor the flow of sensitive information over the network. Policy rules, through use of Data Loss Prevention templates, help to manage the distribution of sensitive data across the network. Administrators can scale policies to apply to the entire company, groups, or specific endpoints.

Administrators can apply policies to both outbound and inbound mail traffic, as well as to the exact message parts to monitor. Policy configurations can exempt certain groups or users from scans and define specific incident response actions.

IWSVA integrates Data Loss Prevention policy management with Control Manager 6.0. Administrators can create and manage the company's Data Loss Prevention policies from the Control Manager console and deploy the settings to all IWSVA servers registered to Control Manager.

Advanced Threat Protection

Advanced Persistent Threats (APTs) are targeted attacks with a pre-determined objective: steal sensitive data or cause targeted damage. APTs are usually not isolated incidents, but rather they are often conducted as a series of failed and successful attempts over time to get deeper and deeper into a target's network.

IWSVA scans the HTTP traffic flow to detect viruses and other security risks in uploads and downloads. HTTP scanning is highly configurable—for example, you can set the types of files to block at the HTTP gateway and how IWSVA scans compressed and large files to prevent performance issues and browser timeouts. In addition, IWSVA scans for many types of spyware, grayware, and other risks.

IWSVA also scans files and URLs for malicious scripts, and the Advanced Persistent Threats (APT) that launch continuous hacking processes on your computer.

HTTPS Decryption

IWSVA closes the HTTPS security loophole by decrypting and inspecting encrypted content. You can define policies to decrypt HTTPS traffic from selected Web categories. While decrypted, data is treated the same way as HTTP traffic to which URL filtering and scanning rules can be applied.

Web Reputation

Web Reputation guards end-users against emerging Web threats. It can improve the Web surfing experience by enhancing Web filtering performance. Because a Web Reputation query returns URL category information (used by the URL Filtering module), IWSVA no longer uses a locally stored URL database.

Web Reputation also assigns reputation scores to URLs. For each accessed URL, IWSVA queries Web Reputation for a reputation score and then takes the necessary action, based on whether this score is below or above the user-specified sensitivity level.

IWSVA enables you to provide feedback on infected URLs, which helps to improve the Web Reputation database. This feedback includes product name and version, URL, and virus name. (It does not include IP information, so all feedback is anonymous and protects company information.) IWSVA also enables you to monitor the effectiveness of Web Reputation without affecting existing Web-access policies. Results are located in the Internet Security Log and Dashboard (Top Threat Detection Count).

For more Web Reputation information, see Specifying Web Reputation Rules on page 9-44 and Web Reputation Settings on page 9-46.

High Availability

IWSVA supports high availability (HA) for service redundancy, providing active/passive failover in Transparent Bridge mode to ensure continuity in demanding business environments. HA in IWSVA is easily deployed through the Deployment Wizard and managed through the new cluster management feature. See High Availability Overview on page 3-2 for more information.

FTP Scanning

In addition to scanning FTP uploads and downloads, IWSVA can also block specified file types at the FTP gateway. To prevent performance issues, the FTP scanning module supports special configurations for compressed files and large files. Spyware and grayware scanning is also supported.

IWSVA FTP scanning can be deployed onto your environment in conjunction with another FTP proxy server, or IWSVA can act as an FTP proxy. To help ensure the security of Trend Micro™ InterScan™ Web Security Virtual Appliance, several security-related configurations are available to control access to IWSVA and its ports.

URL Filtering

With the URL Filtering option in IWSVA, you can set policies based on categories of URLs, such as “Adult”, “Gambling,” and “Financial Services.” When a user requests a URL, IWSVA first looks up the category for that URL and then allows, denies, or monitors access to the URL, displays warning, overrides password, or sets time quota based on the policies you have set up. You can also define a list of approved URLs that will not be filtered.

Content Caching

Web content caching is the caching of Web objects (for example, HTML pages, images) to reduce bandwidth usage, server load, and perceived lag. A Web cache stores copies of objects passing through it. Subsequent duplicate requests may be satisfied from the cache if certain conditions are met. The Content Cache capability provides users who access the Web through IWSVA with a quicker experience while saving bandwidth. See Using the Content Cache on page 9-49 for details.

IP Address, Host Name and LDAP-based Client Identification

IWSVA supports configuring policies for Application Control, Bandwidth Control, HTTPS decryption, HTTP virus scanning, HTTP Inspection, Data Loss Prevention, applets and ActiveX security, URL Filtering, and access quotas. The scope of policies can be configured using client IP address, host name or LDAP user or group name.

Hyper-V Installation Support

IWSVA now supports installation on Microsoft® Hyper-V® 2.0 with Windows Server 2008 R2 or later. The IWSVA installation for Hyper-V platforms supports forward proxy mode, WCCP mode, ICAP mode, reverse proxy mode, and transparent bridge mode. See Appendix F of the *IWSVA Installation Guide* for more information.

Notifications

IWSVA can issue several types of notifications in response to program or security events. Administrator notifications are sent through email to the designated administrator contacts. User notifications are presented in the requesting client’s browser. Both administrator and user notifications can be customized.

To work with network management tools, IWSVA can also issue several types of notifications as SNMP traps. IWSVA sends traps for security risk detections, security violations, program and pattern file updates, and service disruptions.

Because IntelliTrap is considered a type of security risk, it uses the same notifications as Advanced Threat Protection.

Real-time Statistics and Alerts

IWSVA provides dynamic statistics where the administrator can view the “real-time” information about the IWSVA system. Real-time statistics are displayed as graphs and tables on the System Status screen. These statistics include the following:

- Hard Drive

  Hard drive statistics are static and are only updated when you open the System Status page.
- Concurrent Connections
- CPU Usage
- Physical Memory Usage
- Bandwidth Control - Downstream/Upstream

Logs and Reports

IWSVA includes many pre-configured reports to provide a summary of your gateway security status. Reports can be run for a specific time period and customized to only provide information about clients that you are interested in. The following lists the main report classes:

- Internet Access
- Internet Security
- Bandwidth
- Policy Enforcement
- Data Security

Reports are generated from log information in the database. IWSVA writes log information to text-only logs, text and database logs, or database-only logs.

Reports can be generated on demand or scheduled on a daily, weekly, or monthly basis, or a certain time in the future. Log and report data can be exported to comma-separated value (CSV) files for further analysis. To prevent logs from consuming excessive disk space, a scheduled task deletes older logs from the server.

For more information, see Reports, Logs, and Notifications on page 14-1.

In addition to logs and reports, the dashboard screen displays the runtime system information and indicates whether the network or IWSVA is performing normally, the amount of traffic or Internet usage is consistent, and if there is unusual virus activity somewhere on the network.

For more information, see Dashboard on page 1-20.

Syslog Support

To provide enterprise-class logging capabilities, IWSVA allows sending logs using the syslog protocol (default UDP port 514) to multiple external syslog servers in a structured format.

Integration with Cisco WCCP

IWSVA supports Web Cache Communication Protocol (WCCP) version 2, a protocol defined by Cisco Systems. See your Cisco product documentation for more information on the protocol.

The following are the benefits gained when IWSVA supports WCCP:

- Transparency of deployment without endpoint configuration
- High availability and load balancing between multiple IWSVA systems
- Automated load balancing re-configuration when adding or removing IWSVA appliances
- Support Cisco router, switch, and firewall implementations of the protocol

The WCCP implementation for IWSVA is compatible with Cisco routers, switches, PIX firewalls, and ASA security devices.

Trend Micro recommends using the following Cisco IOS versions when configuring WCCP with IWSVA:

- 12.2(0) to 12.2(22). Avoid using releases 23 and above within the 12.2 family
- 12.3(10) and above. Avoid using releases 0-9 in the 12.3 family
- IOS 15.1(1)T3 or above

Trend Micro recommends using version 7.2(3) and above for the Cisco PIX firewall and avoiding version 7.2(2).

Non-Cisco devices that support WCCP version 2 have not been explicitly tested by Trend Micro. Therefore, interoperability cannot be guaranteed.

Reverse Proxy Support

IWSVA is usually installed close to clients to protect them from Internet security risks. However, IWSVA also supports being installed as a reverse proxy to protect a Web server from having malicious programs uploaded to it. As a reverse proxy, IWSVA is installed close to the Web server that it protects. IWSVA receives client requests, scans all content and then redirects the HTTP requests to the real Web server.

For more information, see Reverse Proxy on page 7-10.

Support for Multiple Trend Micro™ InterScan™ Web Security Virtual Appliance Installations

The method to fully administer multiple IWSVA devices from a single console is done through Trend Micro Control Manager (TMCM) for the InterScan Web Security product family. TMCM provides the ability to manage multiple Trend Micro products and allows you to activate multiple IWSVA units from a central console.

Command Line Interface

IWSVA provides a native Command Line Interface (CLI) to perform system monitoring, system administration, debug, troubleshooting functions and more through a secure shell or a direct console connection.

IWSVA's CLI uses industry standard syntax to provide a familiar interface for configuring the appliance. For security, IWSVA allows administrators to access the CLI through the console or an SSH connection only. You can enable this feature in the IWSVA Web console.

What’s New?

The following features are new in IWSVA 6.5 SP2:

- ICAP over SSL
- Bandwidth control
- Content cache enhancement
- TLS/SSL version selection for HTTPs encryption
- New "Ransomware" URL filtering category support
- Enhanced PAC file management
- Removed Web Security Hybrid

System Specifications

Web Browser Requirements

- Internet Explorer (IE) 9.0, 10

- Firefox 39+
- Chrome 44+

Hardware Requirements

For a complete description of the minimum IWSVA server requirements and to install for a basic evaluation, see the Installation Guide.

The minimum requirements specified provide enough resources to properly evaluate the product under light traffic loads. The recommended requirements specified provide general production sizing guidance.

For more detailed sizing information, refer to the *IWSVA Sizing Guide* at:

http://trendedge.trendmicro.com/pr/tm/te/web-security.aspx

Search for "sizing guide."

Minimum Requirements

- Single 2.0 GHz Intel™ Core2Duo™ 64-bit processor supporting Intel VT™ or equivalent
- 4GB RAM
- 50 GB of disk space (IWSVA automatically partitions the detected disk space as required)
- 50 GB of disk space is only appropriate for the testing environment. See Recommended Requirements on page 1-12 for the disk space in the production environment.Monitor that supports 1280x1024 resolution with 32-bit true color

Recommended Requirements

- Dual 3.16 GHz Intel QuadCore™ 64-bit processor or equivalent
- 300 GB of disk space or more and 16 GB RAM for log intensive environments for logging and reporting. IWSVA automatically partitions the detected disk space as per recommended Linux practices.

For more information on capacity sizing, refer to the *IWSVA Sizing Guide* at:

http://trendedge.trendmicro.com/pr/tm/te/web-security.aspx

Compatible Directory Servers for End-User Authentication

- Microsoft Active Directory™ 2003, 2008, and 2012
- Linux™ OpenLDAP Directory 2.2.16, 2.3.39, or 2.4.11
- Sun™ Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)

Integration with ICAP 1.0-compliant Caching Devices

Cache servers help moderate Web traffic congestion and save bandwidth. The “retrieve once, serve many” method employed by cache servers permits integration with third-party applications such as virus scanning through IWSVA. An open protocol, Internet Caching Acceleration Protocol (ICAP), allows seamless coupling of caching and virus protection. IWSVA works with cache servers that support the ICAP 1.0 standard.

X-Authenticated ICAP Headers Support

IWSVA supports X-Authenticated ICAP Headers that are provided by supported ICAP clients, such as Blue Coat (SGOS 4.2.1.1+). The X-Authenticated Headers come in two forms: X-Authenticated-User and X-Authenticated-Groups. The advantage of using X-Authenticated Headers is two-fold: first, it reduces LDAP query overhead in IWSVA and second, it allows ICAP clients to provide LDAP searches on LDAP servers with different schemas.

System Status

The IWSVA console opens to the Dashboard screen that displays real-time, dynamic system information. Other available reports display static information. Information on the System Status page provides access to the following:

- *Enabling Threshold Alert Settings*
- *Bandwidth Control Display*
- *Concurrent Connections Display*
- *Interface Status*
- *CPU Usage Display*
- *Physical Memory Usage Display*

- *Hardware Status*
- *Hard Drive Display*

Enabling Threshold Alert Settings

You can specify threshold alert values and the frequency of alerts so that you are notified when the level of any of the following items reaches a critical level:

- Virus
- Spyware
- Database
- Hard drive
- Bandwidth

IWSVA can send these alerts either through email, SNMP trap/notification (if enabled), or both. See *Notification Email Settings* on page 14-17.

Note: Configure threshold alert settings for email notifications. Threshold alert settings do not affect when IWSVA sends SNMP traps.

To enable threshold alerts:

1. Click **System Status** in the main menu, then click **Threshold Alerts**.
2. Under **Thresholds**, specify the desired thresholds and either accept the defaults or specify new values in the **Threshold Value** and **Limit 1 Notification Every** columns.
3. If you do not want to use the default notification messages under **Notification Message**, highlight the default text and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 14-18.
4. Click **Save**.

Concurrent Connections Display

This dynamic display shows concurrent connections usage for HTTP/HTTPS in purple and FTP in orange. It shows the number of connections and connection time (in seconds.)

This display can have two graphs: one for FTP and the other for HTTP(S). For FTP, the connection measured is the session for both commands and data. For HTTP(S), the connection measured is the session for both requests and responses. The default refresh rate is 30 seconds. Both the X and Y axis scales are variable. The X axis scale is determined by the set refresh rate and the Y axis scale is determined by the number of concurrent connections at a given time.

Bandwidth Control Display

This is a dynamic display that shows the current upstream and downstream bandwidth control status on IWSVA.

Interface Status

Icons shown *Table 1-1* represent the status of the interfaces:

TABLE 1-1. Interface Status Indicators

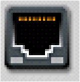
ICON	DESCRIPTION
	Link not detected. Could be an empty port, cable may be loose or broken, or the peer machine may be down.
	Link OK
	Link error
	Link disabled
D	Data interface

TABLE 1-1. Interface Status Indicators (Continued)

ICON	DESCRIPTION
M	Management interface
H	High availability interface

Hardware Status

The Hardware Status feature provides the administrator with the ability to monitor hardware information about fans, voltage, temperature, and so on. on Intelligent Platform Management Interface (IPMI)-enabled devices.

Note: IWSVA hardware monitoring is only compatible with the Baseboard Management Controller (BMC) with Intelligent Platform Management Interface (IPMI) v2.0 support installed on bare metal.

Administrators can query the hardware status information using the IWSVA Web console or by SNMP request. If SNMP trap is enabled, an alert will be sent when system events are detected, such as "temperature threshold exceeded," "voltage threshold exceeded," and so on.

Alerts can be sent to notify administrators of any problems. They are configured at: **Notification > SNMP Notifications Settings > Hardware monitoring events** (check box).

The following provides a brief description of the options available on the Hardware Status screen:

- **Hardware Type**—shows Voltage, Fan, CPU, Storage and Temperature statistics
- **Status**—shows the current status of the hardware. Usually it shows **"**Normal,**"** but if an abnormal event occurs, it displays Critical or Failed, depending on the event. The five available status are:
    - **Normal**—Component status is ok
    - **Warning**—Component status is compromised
    - **Critical**—Component status is in danger of failing

  - **Failed**—Component is not working
  - **Unknown**—No component information is available
- **Sensor Information**—displays information about the status of the type of hardware monitored.

SNMP Queries and Traps

Administrators can poll the hardware status using SNMP queries and receive alerts through SNMP traps. To do this, administrators need import the hardware-monitoring MIB file into an SNMP tool like iReasoning MIB Browser.

IWSVA also supports two standard MIB files for network interface card statistics:

- RFC1213-MIB
- HOST-RESOURCES-MIB

These are available from:

`http://www.simpleweb.org/ietf/mibs/`

The third Trend Micro-specific MIB for hardware events monitoring is: TM-HWMONITOR-MIB

located on the Trend Micro download site at:

`http://www.trendmicro.com/ftp/documentation/guides/MIBs.zip`

To receive traps from IWSVA, administrators need configure the SNMP trap destination at **Administration > Network Configuration > SNMP Settings**.

CPU Usage Display

This is a dynamic display that shows CPU utilization on the local system. In the case of multiple CPUs, the display shows the average IWSVA usage across all CPUs. It does this by displaying a single line for all CPU utilization. IWSVA determines the CPU utilization based on CPU cycles used, CPU cycles used by IWSVA, and total CPU cycles used by the backend, CPU-monitoring API.

By default, IWSVA samples the CPU usage each second for two minutes, giving you 120 data points (1 data point per sec * 120 sec (2 min) = 120 data points). In the file `/etc/iscan/intscan.ini`, under `[metrics]` section, you can change the default refresh rate by modifying the parameter `cpu_refresh`. After modifying the file, restart the Tomcat service by using the following command:

```
/etc/iscan/S99IScanHttpd restart
```

Clicking the 1-day or 30-day button opens a window that shows a static chart with one or 30 days of CPU usage, respectively. IWSVA retrieves this information from the database. If the database does not contain enough data, then the display shows the data that is available.

Note: The 30-day display option shows each day's CPU usage data by a single point. For the 1-day display option, the screen shows the CPU usage for each hour of the day by a single point. IWSVA cannot start graphing data until there are at least two points worth of data available.

Physical Memory Usage Display

This is a dynamic display that shows the amount of physical memory used by the local IWSVA server.

By default, IWSVA samples the physical memory usage each second for two minutes, giving you 120 data points (1 data point per sec * 120 sec (2 min) = 120 data points). In the file `/etc/iscan/intscan.ini`, under `[metrics]` section, you can change the default refresh rate by modifying the parameter `memory_refresh`. After modifying the file, restart the Tomcat service by using the following command:

```
/etc/iscan/S99IScanHttpd restart
```

Clicking the 1-day or 30-day button opens a window that shows a static chart with one or 30 days of physical memory usage, respectively. IWSVA retrieves this information from the database. If the database does not contain all the data, the display shows the data that is available.

Note: The 30-day display option shows each day's physical memory usage data by a single point. For the 1-day display option, the screen shows the physical memory usage for each hour of the day by a single point. IWSVA cannot start graphing data until there are at least two points worth of data available.

Manual Updates on page 4-11 for more information.

Hard Drive Display

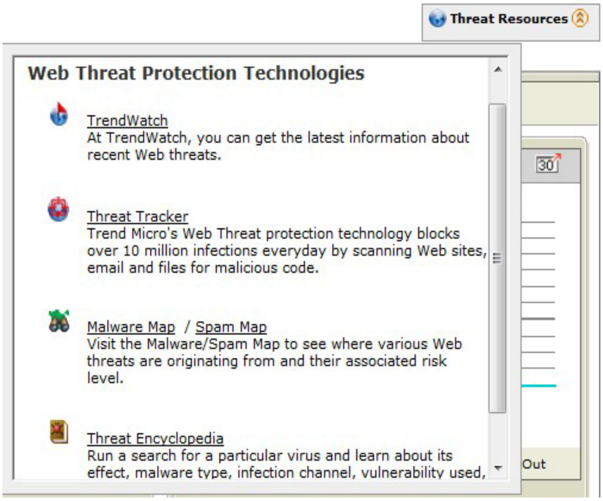
This is a static display that shows the status of the disk(s) used by IWSVA for its system files, quarantine space, temporary space, and logs. The Hard Drive display can monitor up to 12 disks.

If the database resides on the same drive as any of these directories, then the database disk usage is also included in the display. The scale along the Y-axis ranges from 10 to 100 percent.

You can specify threshold alert values and the frequency of alerts so that you are notified when any of the hard disk statuses reach a critical level. IWSVA can send these alerts either through email, SNMP trap/notification (if enabled), or both. SNMP traps are sent when a configured threshold value is met.

Accessing Additional Web Threat Information

From the **Threat Resources** drop-down list in the upper right corner of the **System Status** page, you can access the links to Trend Micro's Web threat protection sites to learn more about the latest Web threats, research from where various Web threats are originating, access Trend's Threat Encyclopedia, and see real-time Web and email malware statistics.See Enabling Advanced Threat Protection and Applets and ActiveX Security on page 9-2 to view the **Threat Resources** drop-down list.



Web Threat Protection Technologies

TrendWatch
At TrendWatch, you can get the latest information about recent Web threats.

Threat Tracker
Trend Micro's Web Threat protection technology blocks over 10 million infections everyday by scanning Web sites, email and files for malicious code.

Malware Map / Spam Map
Visit the Malware/Spam Map to see where various Web threats are originating from and their associated risk level.

Threat Encyclopedia
Run a search for a particular virus and learn about its effect, malware type, infection channel, vulnerability used,

FIGURE 1-1. Web threat protection technologies that can be accessed in IWSVA

Dashboard

The dashboard indicates whether the network or IWSVA is performing normally, the amount of traffic or Internet usage is consistent and within the norm, and if there is unusual virus activity somewhere on the network. The IWSVA dashboard shows a summary of device group transactions that have occurred in the last one, 12, and 24 hours, as well as the last week-long increments.

IWSVA provides dynamic displays where you can view the "real-time" statistics of the IWSVA server.

Also, above the left menu on every page, IWSVA provides a Search field where you can enter a feature name and be directed to the appropriate page for that feature.

Note: Role-based access rights are not breached by the Search feature.

- **Top URL Categories Accessed** - This widget shows URL category-related violations. Also, the time period displayed can show information for the last hour, day, week, or month. Also, the time period displayed can show information for the last hour, day, week, or month. Users can refresh the data manually by clicking Refresh icon in the upper right corner of the widget. The default display is bar-chart style, but it can be toggled to display in table format. To configure how many sources to be displayed, click the Edit icon beside Refresh icon, and set the needed value in the pop-up window.
- **Top Users Blocked by Internet Security (default)** - Shows which users access the most blocked sites for a specified range of time to help understand the user-awareness of Internet security and acceptable usage. Defaults: Top 5, Last 1 Day
- **Top URL Categories Blocked (default)** - Shows the URL categories being blocked the most for a specified range of time to provide high-level view of potential security, bandwidth, and productivity problems. Defaults: Top 5, Last 1 Day
- **Application Bandwidth (default)** - Shows the traffic trend of bandwidth (kbps) by Application usage for a specified range of time. Default time period: Last 1 Day.
- **Top Blocked Applications** - Shows the application categories being blocked the most for a specified range of time to provide high-level view of potential security, bandwidth, and productivity problems. Defaults: Top 5, Last 1 Day
- **Payload** - This is a dynamic display that can have two graphs: one for FTP and the other for HTTP(S). For FTP, the connection measured is the session for both commands and data. For HTTP(S), the connection measured is the session for both requests and responses. Default: Last 1 Day
- **Top Allowed Applications** - Shows the total number of access instances for the top allowed applications within a specific period of time.
- **Top Threat Detection Count (default)** - Shows the total count of different threat types (Malicious URLs, Virus, Spyware, Botnet, Exploit) detected by IWSVA for a specified range of time to provide the high-level view of the risk level of various threat vectors. Default: Last 1 Day

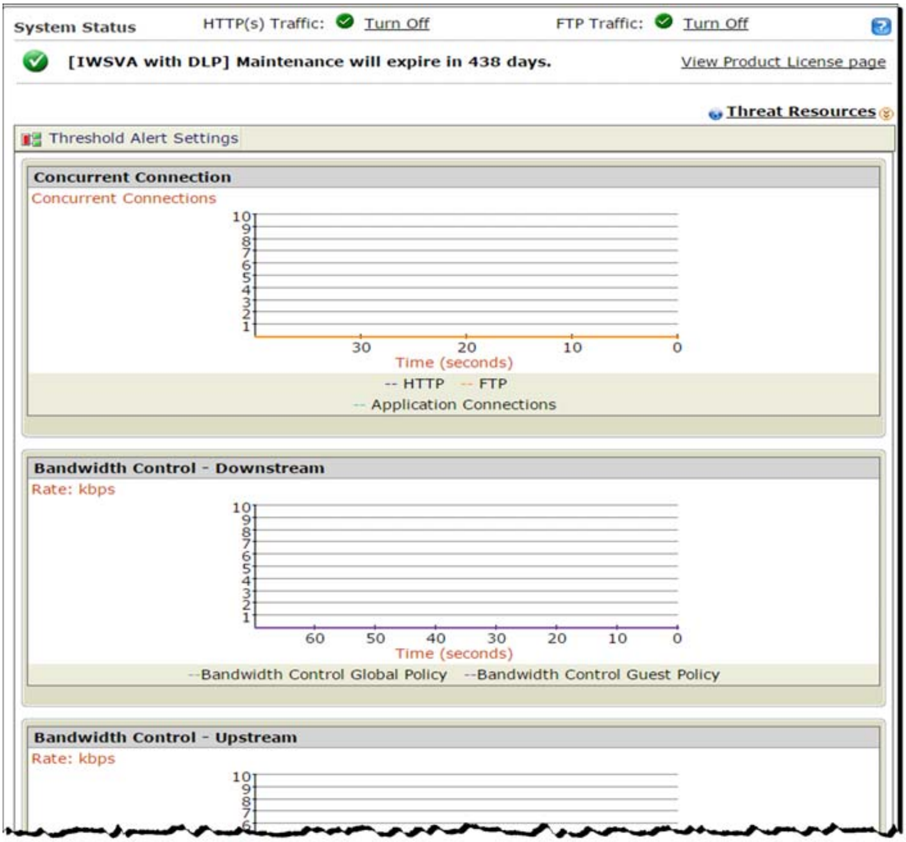
- **Top Policy Enforcement - Application Control** - Shows which policies were violated by how many requests for a specified range of time to provide the effectiveness of policies and to identify needs to change. Defaults: Top 5, Last 1 Day
- **Top Policy Enforcement – URL Filtering** - Shows which policies were violated by how many requests for a specified range of time to provide the effectiveness of policies and to identify needs to change. Defaults: Top 5, Last 1 Day
- **Top Policy Enforcement - DLP** - Shows which policies violated (block/monitor) by how many requests for a specified range of time to provide the effectiveness of policies and to identify needs to change.
- **C&C Callback Attempts (Command-and-Control Callback Attempts)** - Shows C&C Callback Attempts noted within a specific period of time.

When mousing over the target component in the widget, corresponding numerical data-value displays. For example: when mousing over the Malicious-URLs bar on the "Total Threat Detection Count" widget, corresponding data-values are shown.

When clicking within a widget, the page is redirected to a log-analysis page that details the current widget setting parameters.

Web Traffic Security Risk Overview

Web traffic exposes corporate networks to many potential security risks. While most computer viruses enter organizations through messaging gateways, Web traffic is a common infection vector for new security risks. For example, "mixed risks," which take advantage of multiple entry points and vulnerabilities using HTTP to spread.



System Status HTTP(s) Traffic: ✓ Turn Off FTP Traffic: ✓ Turn Off

✓ [IWSVA with DLP] Maintenance will expire in 438 days. View Product License page

FIGURE 1-2. IWSVA System Status displays security risk information

Significant assessment, restoration, and lost productivity costs associated with outbreaks can be prevented. IWSVA is a comprehensive security product that identifies and protects multiple Internet protocols, including HTTPS, HTTP, and FTP traffic in enterprise networks from viruses and other risks.

In addition to content-based antivirus scanning, IWSVA also helps with other network security issues:

- The Application Control feature provides a security technology that automates the discovery of popular Internet applications and allows administrators to control them using policies.
- The Bandwidth Control feature allows administrators to configure policies to control communications, reduce unwanted traffic and allow critical traffic or services the appropriate bandwidth allocation.
- Monitor and enable block/allow policies for any of several hundred Internet applications that may be misused by employees.
- Web Reputation scrutinizes URLs before you access potentially dangerous Web sites, especially sites known to be phishing or pharming sites.
- URL filtering feature can allow, block, block with override, warn but allow, or monitor access to Web sites with content prohibited by your organization.
- HTTPS decryption feature allows encrypted traffic to pass through IWSVA scanning and filtering policies as "normal" HTTP traffic and verifies certificates from HTTPS servers.
- Applets and ActiveX security helps to reduce the risk of malicious mobile code by checking digital signatures at the HTTP/HTTPS gateway, and monitoring applets running on clients for prohibited operations. With Applets and ActiveX security modules and URL Filtering now included in the IWSVA, these come at no extra cost to you.

Smart Search Support

The search field above the left menu allows users to find the features they need quickly, without navigating through the menu.

To use the Smart Search function:

1. Go to any page in IWSVA Web console.
2. In the Smart Search search field above the left menu, begin to type the name of the feature to be located. (See *Figure 1-3*.)
3. Select the appropriate feature from the options provided in the drop-down list.
4. Press **Enter**.

   The page of your request feature displays.

Note: Smart Search is an instance-level feature. Passive nodes in High Availability environments will not be searched unless the administrator is logged into the passive member.

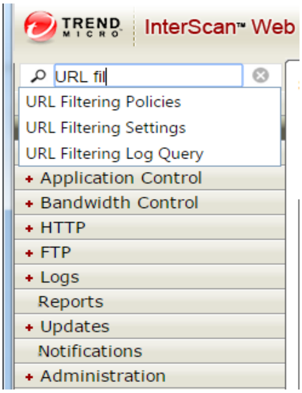


FIGURE 1-3. Smart Search available to find the location of features

Chapter 2

Deployment Wizard

The contents of this chapter help to guide you through the deployment process as you configure InterScan Web Security Virtual Appliance (IWSVA) for your network.

Topics in this chapter include the following:

Overview of the Deployment Wizard

The Deployment Wizard display automatically at first login and will walk you through the deployment process. It can be manually invoked from **Administration > Deployment Wizard** at any time to review or change settings.

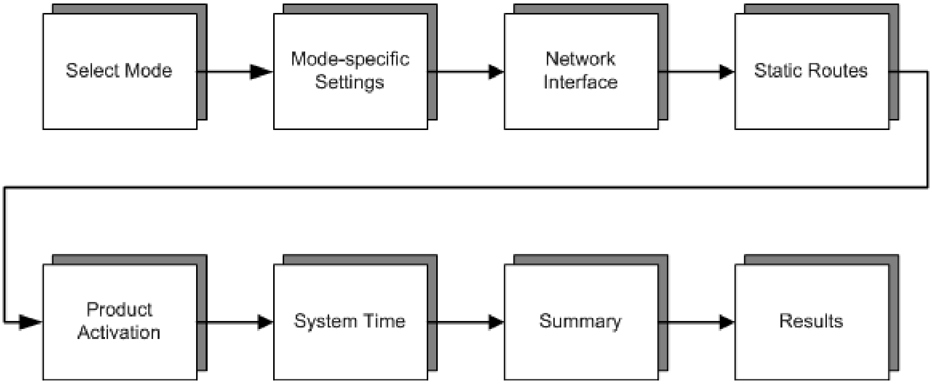


FIGURE 2-1. Deployment Wizard Flow

Mode Selection

IWSVA can be deployed in different modes, depending on your network security needs. For more information on which mode to select, see the Deployment Primer in Chapter 2 of the *IWSVA Installation Guide*.

The Deployment Wizard allows you to configure IWSVA in one of seven modes.

- Transparent Bridge Mode on page 2-3
- Transparent Bridge Mode - High Availability on page 2-4
- Forward Proxy Mode on page 2-9
- Reverse Proxy Mode on page 2-10
- ICAP Mode on page 2-11
- Simple Transparency Mode on page 2-13
- Web Cache Coordination Protocol (WCCP) Mode on page 2-14

Transparent Bridge Mode

IWSVA acts as a bridge between network devices such as routers and switches. IWSVA scans passing HTTP and FTP traffic without the need to modify browser or network settings. This is the easiest deployment mode with traffic scanned in both directions.

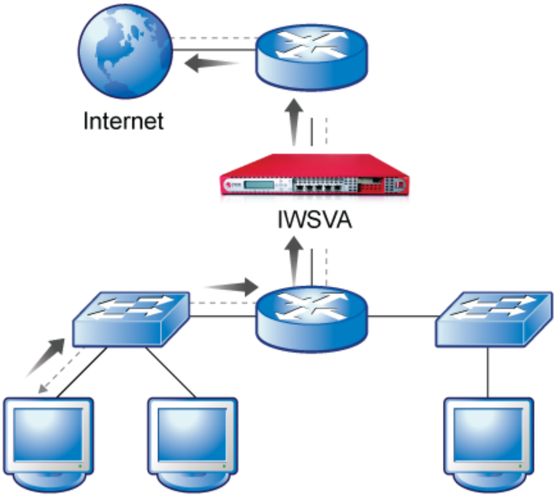


FIGURE 2-2. Transparent Bridge Mode

Transparent Bridge Mode and Transparent Bridge Mode - High Availability are also the only deployment modes that allow for the Application Control reporting and policies to function. For these reasons, Trend Micro strongly recommends deploying the product in one of these modes to realize maximum visibility and protection for Internet traffic.

The additional dependency for this deployment mode is two network interface cards per transparent bridge segment protected with IWSVA. Trend Micro recommends the following network cards be used to ensure maximum compatibility:

- Broadcom NetXtreme Series
- Intel Pro/1000 PT Dual Port Server Adapter
- Intel Pro/1000 MF Dual Port Fiber

Note: For more information on setting up IWSVA in Transparent Bridge mode, see Network Configuration and Load Handling on page 7-12.

To deploy IWSVA in Transparent Bridge mode:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Transparent Bridge Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Network Interface on page 2-27 to continue.

Note: Transparent Bridge Mode for a single node requires no mode-specific settings. For more information on setting up IWSVA, see Network Configuration and Load Handling on page 7-12.

To use a Silicom bypass card to do an ESX bypass:

1. Check `www.silicom-usa.com` to obtain the necessary drivers and tools appropriate for your specific Vmware EXSi version.
2. Disable IWSVA's built-in LAN-bypass function.
3. Use the Silicom-provided command line tools to control the LAN-bypass function.

Transparent Bridge Mode - High Availability

The IWSVA High Availability (HA) solution currently supports active/passive pairs utilizing the Transparent Bridge mode. To deploy an IWSVA cluster with an IPv4 address, each IWSVA unit must use a separate management interface.

The Transparent Bridge Mode - High Availability deployment requires at least the following network interfaces cards (NICS) for cluster deployment:

- Two for bridge data interfaces
- One for the HA interface
- One for the separate management interface

Note: For more information about high availability and cluster management, see *High Availability and Cluster Management for Transparent Bridge Mode* starting on page 3-1.

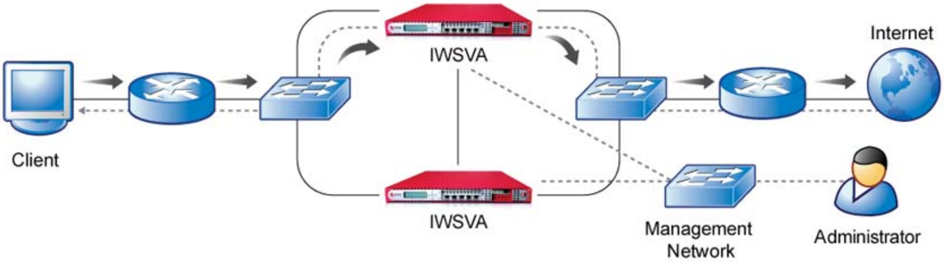


FIGURE 2-3. Transparent Bridge Mode - High Availability

Note: IWSVA only supports two HA nodes in a single HA cluster.

Using the Deployment Wizard, you can either:

- Create a New Cluster on page 2-6
- Join an Existing Cluster on page 2-8

About Cluster IP Addresses

The Cluster IP address is the floating IP address of the management port of the cluster. Users access this IP address through the Web console or the CLI to manage the cluster. The floating IP address floats in the cluster. If a switchover occurs, the floating IP address of cluster (the cluster IP address) always points to the parent device.

About Weighted Priority Election

Enabling Weighted Priority Election allows the device with the highest weight to always be selected as the parent member. Disabling the Weighted Priority Election process means the current parent member remains the parent member even when a new cluster member with a higher weight is added into the cluster.

The weight is the user-defined priority of the member in the cluster. If two members have the same weight assigned, there will still be one parent and one child, but the selection of the parent member is based on an internal algorithm. If you enable Weighted Priority Election, cluster members are prohibited from having equal weights.

Create a New Cluster

To create a new cluster:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Transparent Bridge Mode - High Availability** option on the Deployment Mode page.
4. Click the **New Cluster** option.
5. Click **Next**.
6. Set the Cluster Settings, which include:
   a. Type a cluster name.
   b. Type an (optional) cluster description.
   c. Type the Cluster IP address. See About Cluster IP Addresses on page 2-5 for details.
   d. Select Enable or Disable from the Weighted Priority Election drop-down list.

      Note: For more information on Weighted Priority Election, see About Weighted Priority Election on page 2-6.

Note: Cluster IP address does not support IPv6.

- If enabled, the HA pair launches an election to choose the maximum-weighted machine.
- If disabled, the HA pair only launches an election when the current active (primary) machine is not available.

Note: The HA mode displays as Active/Passive and the Deployment mode always shows Bridge to indicate Transparent Bridge Mode - High Availability.

e. Using the information in the Interface Status section, select the HA Interface from the drop-down list (eth0, eth1, eth2, eth3, etc.)

Active and passive IWSVAs are connected directly though the HA or “Heartbeat” interface. The interface, labeled H in the interface status graphic, has two functions:

- Active and passive virtual appliances send a package per second to notify each other they are up and running.
- The interface is used in the synchronization process.

See *Figure* on page 2-29 and *Table 2-2* on page 2-29 for more information on using the Interface Status graphic. Also see Determining the Status of the Interfaces on page 2-28.

f. Enter the Weight value. (Default 128)

- The member with the higher weighting has higher priority and becomes the parent member.

7. Click **Next**.

8. Set up the Network Interface on page 2-27 to continue the deployment.

Join an Existing Cluster

To join an existing cluster:

1. Go to **Administration > Deployment Wizard**.

Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Transparent Bridge Mode - High Availability** option on the Deployment Mode page.
4. Click the **Join a Cluster** option.
5. Click **Next**.
6. Set the Cluster settings, which include:

   a. Using the information in the Interface Status section, select the HA Interface from the drop-down list (eth0, eth1, eth2, eth3, etc.)

   Active and passive IWSVAs are connected directly though the HA or "Heartbeat" interface. The interface, labeled H in the interface status graphic, has two functions:

   - Active and passive virtual appliances send a package per second to notify each other they are up and running.
   - The interface is used in the synchronization process.

   See *Figure* on page 2-29 and *Table 2-2* on page 2-29 for more information on using the Interface Status graphic. Also see Determining the Status of the Interfaces on page 2-28.

   b. Enter the Weight value. (Default 64)

7. Click **Next**. A progress bar displays, showing connection to the existing cluster.
8. Review the cluster information page that displays after connecting to the cluster and click **Next**.
9. Set up the Network Interface on page 2-27 to continue the deployment.

Forward Proxy Mode

IWSVA can act as an upstream proxy for network clients. Client browser settings must be configured to redirect traffic to IWSVA. IWSVA scans HTTP and FTP traffic and there is no separate need for another dedicated proxy server. Content is scanned in both the inbound and outbound directions. The Application Control and Bandwidth control reports and polices also function in proxy mode because IWSVA recognizes the HTTP, HTTPS, and FTP protocols.

Forward Proxy Mode also provides the following additional capabilities:

- Forwards all traffic to another upstream proxy server
- Participates in a proxy chain configuration with other proxy servers and supports X-Forwarded-For functionality
- Uses Guest port to provide a dedicated traffic channel to guest users. IWSVA applies the Guest policies to the traffic that passes through the Guest port.

Note: For more information on setting up IWSVA in Forward Proxy mode, see Network Configuration and Load Handling on page 7-12.

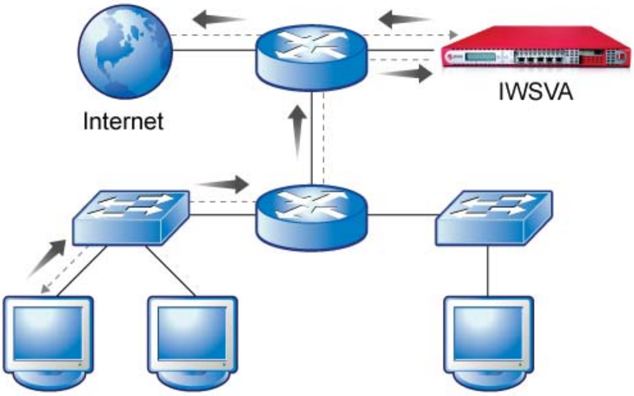


FIGURE 2-4. Forward Proxy Mode

To deploy IWSVA in Forward Proxy Mode:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Forward Proxy Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

Reverse Proxy Mode

In this deployment mode, IWSVA is deployed in front of a Web server. IWSVA scans HTTP and FTP content from the clients that are uploaded to a web server as well as content that is downloaded from the Web server to the clients and helps secure the Web server.

WARNING! The DLP functionality will be disabled in this mode.

Note: For more information on setting up IWSVA in Reverse Proxy mode, see Network Configuration and Load Handling on page 7-12.

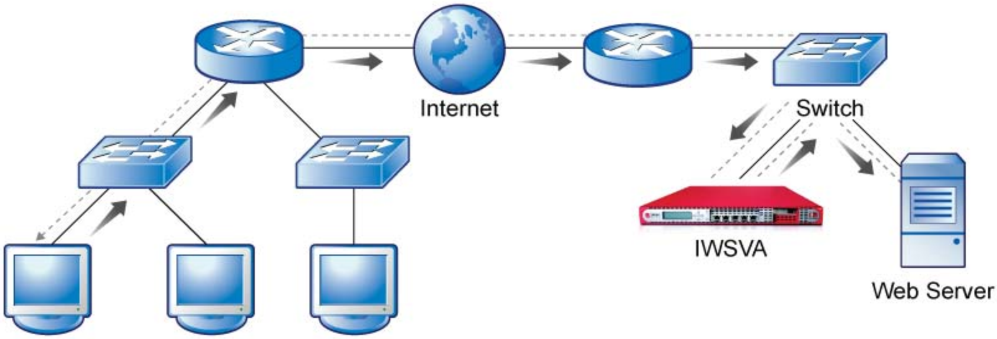


FIGURE 2-5. Reverse Proxy Mode

To deploy IWSVA in Reverse Proxy Mode:

1. Go to **Administration > Deployment Wizard**.

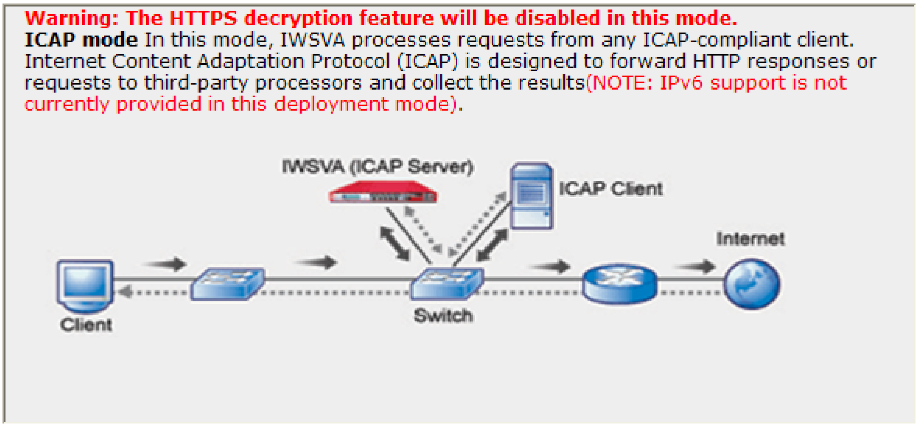
   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Reverse Proxy Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

ICAP Mode

IPv6 support is not currently provided for this deployment mode. In this deployment mode, IWSVA acts as an ICAP server and accepts ICAP connections from an ICAP v1.0 compliant cache server (acting as a client to IWSVA). Cache servers can help reduce the overall bandwidth requirements and reduce latency by serving cached content locally. IWSVA scans and secure all content returned to the cache server and to the end-user clients.

Note: To enable and configure ICAP mode, see Network Configuration and Load Handling on page 7-12 and Setting Up IWSVA ICAP on page 2-45.



Warning: The HTTPS decryption feature will be disabled in this mode.

ICAP mode In this mode, IWSVA processes requests from any ICAP-compliant client. Internet Content Adaptation Protocol (ICAP) is designed to forward HTTP responses or requests to third-party processors and collect the results(NOTE: IPv6 support is not currently provided in this deployment mode).

FIGURE 2-6. ICAP Mode

Deploying IWSVA in ICAP Mode in the Deployment Wizard

To deploy IWSVA in ICAP mode:

1. Go to **Administration > Deployment Wizard**.

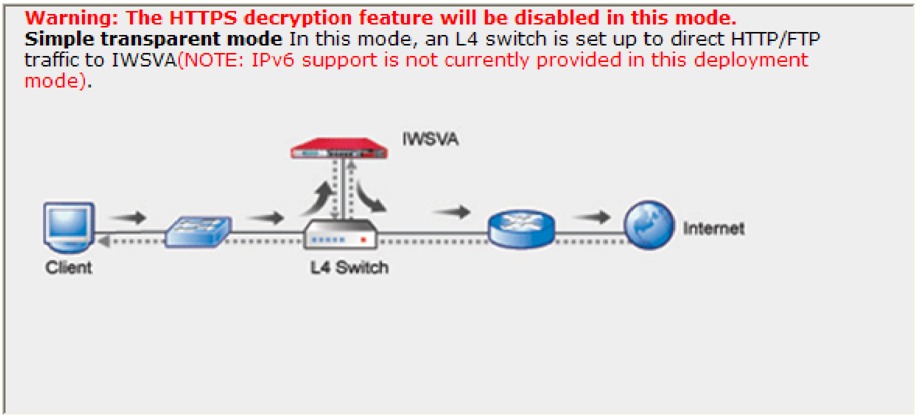
   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **ICAP Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

Simple Transparency Mode

IPv6 support is not currently provided for this deployment mode. IWSVA's Simple Transparent Mode supports simple transparency with popular Layer 4 load balancing switches and provides HTTP scanning without the need to modify the client's browser settings. The HTTPS decryption feature is disabled in this mode.

Note: For more information on setting up IWSVA in Simple Transparency mode, see Network Configuration and Load Handling on page 7-12.



Warning: The HTTPS decryption feature will be disabled in this mode.
Simple transparent mode In this mode, an L4 switch is set up to direct HTTP/FTP traffic to IWSVA(NOTE: IPv6 support is not currently provided in this deployment mode).

FIGURE 2-7. Simple Transparency Mode

To deploy IWSVA in Simple Transparency Mode:

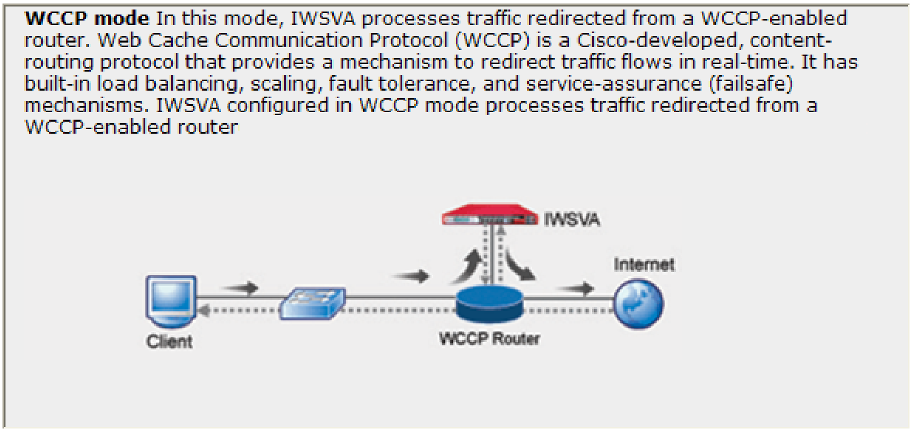
1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Simple Transparency Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

Web Cache Coordination Protocol (WCCP) Mode

IPv6 support is provided for this deployment mode. IWSVA works with Cisco's WCCP protocol to provide content scanning for Web and FTP traffic without the need to modify client configurations and allows redundancy and saleability to be designed into the architecture without additional hardware.



WCCP mode In this mode, IWSVA processes traffic redirected from a WCCP-enabled router. Web Cache Communication Protocol (WCCP) is a Cisco-developed, content-routing protocol that provides a mechanism to redirect traffic flows in real-time. It has built-in load balancing, scaling, fault tolerance, and service-assurance (failsafe) mechanisms. IWSVA configured in WCCP mode processes traffic redirected from a WCCP-enabled router

FIGURE 2-8. WCCP Mode

Note: For more information on setting up your WCCP server for use with IWSVA, see Network Configuration and Load Handling on page 7-12 and your Cisco product documentation.

To deploy IWSVA in WCCP Mode:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **WCCP Mode** radio button on the Deployment Mode page.

4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

Mode-specific Settings

Some deployments modes have settings that are unique to that mode. The second step in the Deployment Wizard allows you to configure those settings. The Transparent Bridge Mode has no mode-specific settings.

TABLE 2-1. Mode-specific Settings

MODE	MODE-SPECIFIC SETTINGS	PAGE
Transparent Bridge Mode	None	N/A
Transparent Bridge for High Availability Mode	New: • Cluster settings • Weighted Priority Election (Y/N) • HA Interface • Weight Existing: • HA Interface • Weight	New: 2-6 Existing: 2-8
Forward Proxy Mode	Proxy settings	2-16
Reverse Proxy Mode	Proxy settings	2-16
ICAP Mode	ICAP settings	2-19
Simple Transparency Mode	Transparency settings	2-22
WCCP Mode	WCCP settings	2-23

Proxy Settings

Proxy settings must be configured if you are installing in the following modes:

- Forward Proxy, Standalone Mode - See Standalone Proxy Mode Settings on page 2-16
- Forward Proxy, Upstream Proxy Mode -See Upstream Proxy (Dependent) Mode Settings on page 2-17
- Reverse Proxy Mode - See Reverse Proxy Settings on page 2-18

Forward Proxy Mode

Depending on your network configuration, you can either specify:

- Standalone Proxy Mode Settings on page 2-16
- Upstream Proxy (Dependent) Mode Settings on page 2-17

Standalone Proxy Mode Settings

To configure the proxy settings for Standalone Mode:

1. Select the **Forward Proxy mode** radio button on the Deployment Mode page.

See Forward Proxy Mode on page 2-9 for details.

2. Click **Next**.

3. Follow the configuration recommendations in *Table 2-1*.

TABLE 2-1. Standalone settings in Forward Proxy Mode

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections.	8080
Enable upstream proxy (check box)	Enable / disable upstream proxy	Leave unchecked if you do not use another proxy device upstream of IWSVA.

TABLE 2-1. Standalone settings in Forward Proxy Mode (Continued)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Enable guest user login	Enable / disable Guest port	Leave unchecked if you do not use Guest port.
Port Number	Port number of Guest port	8081

4. Click **Next**.
5. Set up the Network Interface on page 2-27 to continue the deployment.

Upstream Proxy (Dependent) Mode Settings

To configure the Proxy Settings for Upstream Mode:

1. Select the **Forward Proxy mode** radio button on the Deployment Mode page.

   See Forward Proxy Mode on page 2-9 for details.
2. Click **Next**.
3. Follow the configuration recommendation in *Table 2-2*.

TABLE 2-2. Upstream Proxy (Dependent) settings in Forward Proxy Mode

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections	8080
Enable upstream proxy (check box)	Enable / Disable upstream proxy	Check (enable)
Proxy Server	Upstream proxy server address	Type in the value of the upstream proxy server

TABLE 2-2. Upstream Proxy (Dependent) settings in Forward Proxy Mode

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Port	Port of the upstream proxy server	Type in the port number of the upstream proxy server
Enable guest user login	Enable/disable Guest port	Leave unchecked if you do not use Guest port
Port Number	Port number of Guest port	8081

4. Click **Next**.
5. Set up the Network Interface on page 2-27 to continue the deployment.

Reverse Proxy Settings

To configure the Proxy Settings for Reverse Proxy Mode:

1. Select the **Reverse Proxy mode** radio button from the Deployment Mode page. See Reverse Proxy Mode on page 2-10 for details.
2. Click **Next**.
3. Follow the configuration recommendation in *Table 2-3*/

TABLE 2-3. Reverse Proxy Mode Proxy Settings

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections for reverse proxy.	80
Protected server	This is the IP address of the Web server IWSVA is protecting.	Type in the IP address of the protected server.

TABLE 2-3. Reverse Proxy Mode Proxy Settings (Continued)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Port number	This is the port of the Web server IWSVA is protecting.	Type in the port number of the server being protected.
SSL Port number	This is the SSL port of the Web server IWSVA is protecting.	Default is 443, the SSL port number of the server being protected.
Enable SSL Port (check box)	Enable / Disable SSL.	Leave disabled unless required. Check to enable.

4. Click **Next**.
5. Set up the Network Interface on page 2-27 to continue the deployment.

ICAP Settings

Note: ICAPS is not available for ICAP clients using SSLv2 or SSLv3 for SSL handshake. IWSVA only supports TLSv1, TLSv1.1, and TLSv1.2 for secure ICAP communication.

Deploying in ICAP Mode requires addition configuration settings.

IWSVA can return four optional headers from the ICAP server whenever a virus is found or information about users and groups. "X-Virus-ID" and "X-Infection-Found" are not returned by default for performance reasons, because many ICAP clients do not use these headers. They must be enabled in the IWSVA Web console.

- **X-Virus-ID:** Contains one line of US-ASCII text with a name of the virus or risk encountered. For example:

```
X-Virus-ID: EICAR Test String
```

- **X-Infection-Found:** Returns a numeric code for the type of infection, the resolution, and the risk description.

  For more details on the parameter values, see:

  `http://www.icap-forum.org`

- **X-Authenticated - User:** If enabled, IWSVA requests the username sent in the X-Authenticated-User ICAP header. The username obtained from the ICAP header allows IWSVA to identify of the user issuing the request if you configure IWSVA to use the user/groupname method of user identification.
- **X-Authenticated - Group:** If enabled, IWSVA requests the group membership information sent in the X-Authenticated-Groups ICAP header if you configure IWSVA to use the user/groupname method of user identification. If disabled, IWSVA queries LDAP for the group membership information.

Note: Some ICAP clients do not offer the recursive group membership search. For example, if a user belongs to group A, and group A belongs to group B, the ICAP client only sends group A information in the header. If you require recursive group membership information, Trend Micro recommends disabling the x_authenticated_groups header.

To configure the ICAP settings:

1. Select the **ICAP mode** radio button from the Deployment Mode page of the Deployment Wizard.

   See ICAP Mode on page 2-11 for details.
2. Click **Next**.
3. Follow the configuration recommendations in *Table 2-4*.

TABLE 2-4. ICAP Mode-specific Settings

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections for ICAP.	1344

TABLE 2-4. ICAP Mode-specific Settings (Continued)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Enable ICAP over SSL	Enable/Disable secure ICAP communication	Disable
ICAPS Port Number	This is the port that IWSVA listens on to receive connections for ICAPS.	11344
Certificate	Import server certificates for SSL-secured requests from clients.	
Private Key	Import the private key for SSL-secured communication.	
Passphrase	Enter the passphrase for the private key.	
Confirm Passphrase	Enter the passphrase again to confirm.	
Enable X-Virus-ID ICAP header (check box)	Enable / Disable the ICAP short name of the infection detected being recorded.	Disable
Enable X-Infection-Found ICAP header (check box)	Enable / Disable ICAP details about malware detected and passing details back to the ICAP device.	Disable
Enable X-Authenticated-User ICAP header	Enable / Disable ICAP details about username information.	Enable

TABLE 2-4. ICAP Mode-specific Settings (Continued)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Enable X-Authenticated-Groups ICAP Header	Enable / Disable ICAP details about group membership information.	Disable

4. Click **Next**.
5. Set up the Network Interface on page 2-27 to continue the deployment.

Note: Complete all steps in the Deployment Wizard to deploy in ICAP mode. After receiving a successful deployment message, configure the IWSVA ICAP set up as shown in *Setting Up IWSVA ICAP* on page 2-45.

If you enable ICAP over SSL and import a certificate on IWSVA, Trend Micro recommends that you disable the ICAP server certificate verification function on ICAPS clients. This prevents connection failure on ICAPS clients due to invalid server certificate checks. For information on configuring ICAP clients (for example, Bluecoat ProxySG), refer to the related documentation.

Simple Transparency Settings

Simple Transparency Mode requires mode-specific settings.

To configure mode-specific settings for Simple Transparency Mode:

1. Select the **Simple Transparency mode** radio button from the Deployment Mode page.

   See Simple Transparency Mode on page 2-13 for details.
2. Click **Next**.

3. Enter the following settings on the Simple Transparency Settings page. (See *Table 2-5*.)

TABLE 2-5. Simple Transparency Mode-specific Settings

CONFIGURATION PARAMETER	DESCRIPTION	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections.	80
Anonymous FTP over HTTP	The email address passed to FTP sites.	Type in an appropriate email address

4. Click **Next**.
5. Set up the Network Interface on page 2-27 to continue the deployment.

WCCP Settings

WCCP Mode requires mode-specific settings.

To configure mode-specific settings for WCCP Mode:

1. Select the **Web Cache Coordination Protocol (WCCP) mode** radio button from the Deployment Mode page.

   See Web Cache Coordination Protocol (WCCP) Mode on page 2-14 for details.
2. Click **Next**.
3. Enter the following settings on the WCCP Settings page. (See *Table 2-6*.)

TABLE 2-6. WCCP Mode-specific Settings

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections.	80

TABLE 2-6. WCCP Mode-specific Settings (Continued)

<table>
<tr><th>CONFIGURATION PARAMETER</th><th>DETAILS</th><th>RECOMMENDED VALUE</th></tr>
<tr><td>Router IP address</td><td>Detail which router or switch to communicate with via WCCP</td><td>Type in the router or switch IP address</td></tr>
<tr><td>Password</td><td>Password for WCCP authentication</td><td>Type in the password for the WCCP authentication</td></tr>
<tr><td>Auto-negotiate</td><td>Provides automatic negotiation of the forwarding method and the assignment method.</td><td>Select **Enable** (default.)</td></tr>
<tr><td colspan="3">**Note:** If you select **Enable**, the Forwarding and Assignment Methods parameters are grayed out since they are automatically configured. After the Deployment Wizard finishes, you can see the values of the auto-negotiated parameters at: **Administration > Network Configuration > WCCP**.
- If the route supports L2/GRE as a forwarding method, IWSVA should select L2 when the router and IWSVA are in the same network segment. (This takes performance into account.)
- If one route supports L2/GRE as forwarding method, IWSVA should select GRE when the router and IWSVA are not in the same network segment.
-If one route supports HASH/MASK as assignment method, IWSVA should select MASK. (This takes performance into account.)</td></tr>
<tr><td>WCCP forwarding method</td><td>The WCCP forwarding method determines how intercepted traffic is transmitted from the WCCP server (IOS) to the WCCP client.</td><td>Select the Generic Routing Encapsulation (GRE) or Layer 2 (L2) as the WCCP forwarding method</td></tr>
</table>

TABLE 2-6. WCCP Mode-specific Settings (Continued)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Note: - GRE forwarding, which is the default forwarding method, encapsulates the intercepted packet in an IP GRE header with a source IP address of the WCCP server (IOS) and a destination IP address of the target WCCP client. This has the effect of a tunnel, allowing the WCCP server (IOS) to be multiple Layer 3 hops away from the WCCP client. - L2 forwarding simply rewrites the destination MAC address of the intercepted packet to equal the MAC address of the target WCCP client. L2 forwarding requires that the WCCP server (IOS) is Layer 2 adjacent to the WCCP client		
Assignment method	WCCP provides packet distribution through two algorithms, Hash tables and Mask/value sets.	Select Hash tables or Mask/value sets as the WCCP assignment method.
With hash assignment, the router runs a value in the header of the packet it is redirecting through a hashing function. With mask assignment, each router/switch in the service group has a table of masks and values that it uses to distribute traffic across the proxy appliances in the service group.		

TABLE 2-6. WCCP Mode-specific Settings (Continued)

Configuration Parameter	Details	Recommended Value
Service Group	Standard or Dynamic	• **Standard**—Well-known services, also referred to as static or standard services, have a fixed set of characteristics that are known by both IOS and WCCPv2 client devices. • **Dynamic**—Dynamic services are initially only known to the WCCPv2 clients within the service group.
Note: For example, a single well-known (standard) service called web-cache has a Service ID is 0. This service redirects all TCP traffic with a destination port of 80. The characteristics of a dynamic service are initially only known to the WCCPv2 clients within the service group. The characteristics of the service group are communicated to the IOS devices by the first WCCPv2 client device to join the service group.		
Unique Service ID	Identifies service groups Default: • Standard service = 0 • Dynamic service = 80	Range: • Standard = 0-50 • Dynamic = 51-255
Anonymous FTP over HTTP	The email address passed to FTP sites.	Type in an appropriate email address

4. Click **Next**.
5. Set up the Network Interface on page 2-27 to continue the deployment.

Network Interface

All modes need the relevant network interface settings configured. Some modes require slightly different information than other modes. The following procedures calls out the different settings needed.

Network interface settings include:

- Host Information on page 2-27
- Data Interface on page 2-31
- Separate Management Interface on page 2-33
- Miscellaneous Settings (IPv4 and IPv6) on page 2-34

Host Information

All modes require the host information to be entered. Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings

To enter the host information:

1. Using the Deployment Wizard, select the appropriate deployment mode radio button and click **Next**.
2. Set any mode-specific settings and click **Next**.
3. Type the applicable Fully Qualified Domain name (FQDN) for the IWSVA host.

Note: A fully qualified hostname is required. Trend Micro recommends creating a DNS entry for the IWSVA server's hostname in their DNS server.

4. Continue to the section about the Interface Status starting on page 2-28.

Note: For IWSVA to function properly, make sure that a DNS server is available to resolve hostnames.

Interface Status

IWSVA provides a graphical representation of the physical Ethernet ports on the IWSVA server to simplify the configuration of the network ports. The Interface Status graphic shows the status and function of the available interfaces.

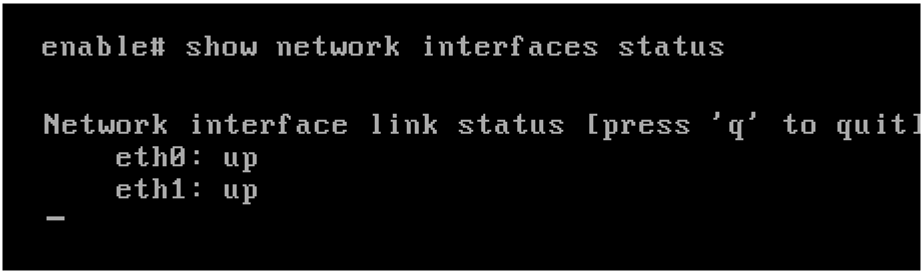
Use *Figure* on page 2-29 to interpret the status and function of the Ethernet ports used for configuration purposes in the Interface Status section.

Determining the Status of the Interfaces

IWSVA is a software virtual appliance that can be installed on all types of hardware. As such, the network information displayed in IWSVA's Web UI may not directly relate to the physical network interfaces installed in the server running IWSVA. For example, if the server came with two network interfaces installed on the motherboard and then an additional four-port Ethernet card was installed in the server to increase the network interfaces available, the IWSVA Web UI may display the first network port as Eth0 when it is actually mapped to physical network interface Eth2 on the new Ethernet card.

In order to positively identify the IWSVA Web UI network interface to the physical network interface, IWSVA provides a command line interface (CLI) command to display the real time status of the physical network interfaces and the Interface Status graphic in the Deployment Wizard.

By using the `show network interfaces status` CLI command from the IWSVA console, you can quickly see the link status of the physical interface. In the example below, you can see that Eth0 and Eth1 is up with a physical link connection.



```
enable# show network interfaces status

Network interface link status [press 'q' to quit]
    eth0: up
    eth1: up
_
```

FIGURE 2-9. "show network interfaces status" CLI command

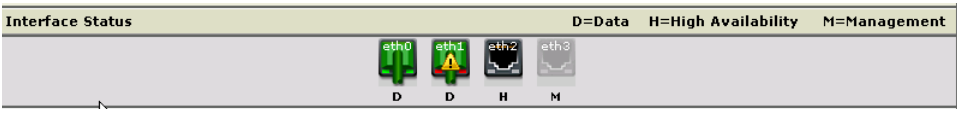


FIGURE 2-10. Interface Status

Figure 2-10 depicts the interface status information displays in the Deployment Wizard. *Table 2-2* defines the icons used in the interface status graphic.

TABLE 2-2. Interface Status Icons

CALLOUT	POINTS TO
M	Management interface
D	Data interface
H	HA or Heartbeat Interface
eth0	Link not detected. Could be an empty port, cable may be loose or broken, or the peer machine may be down.

TABLE 2-2. Interface Status Icons (Continued)

CALLOUT	POINTS TO
eth0	Link ok
eth1 ⚠	Link error
eth1	Link disabled

About Interface Mapping

Trend Micro recommends mapping the interfaces with physical interfaces before configuring or modifying your interface settings.

After rebooting IWSVA, the numbering for unused interfaces may change, however the occupied interfaces (for data, management, or HA) will not change.

Before dissolving a cluster, interfaces might be mapped as shown in *Table 2-7*.

TABLE 2-7. Original Interface Mapping

PHYSICAL INTERFACE	A	B	C	D
RELATIVE INTERFACE	eth1	eth2	eth0	eth3
PURPOSE	D (internal)	H	D (external)	M

After dissolving a cluster, joining a cluster, or rebooting, the interface mapping might change as shown in *Table 2-8*.

TABLE 2-8. Changed Interface Mapping

PHYSICAL INTERFACE	A	B	C	D
RELATIVE INTERFACE	eth2	eth1	eth0	eth3
PURPOSE	(internal)	(unused)	D (external)	M

Data Interface

The Data Interface supports end-user Internet traffic to and from the internal network. Use the following procedure to configure the host name and IP settings for the data (bridge or proxy) interfaces. You can use both IPv4 and IPv6 addresses.

WARNING! **Do NOT configure the data interface and the management interface in the same network subnet. If they are in the same network segment, the IWSVA internal firewall will prevent proper forwarding of HTTP and FTP traffic.**

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the IWSVA host information

To configure the Data Interface settings:

1. Continue working from the **Network Interface** page of the Deployment Wizard.
2. Configure the Data Interface settings:
   a. **All modes except Transparent Bridge mode:** Select the appropriate Ethernet port from the **Ethernet Interface** drop-down list for the data interface.

      The dynamic Interface Status graphic displays your selection.

   b. **Transparent Bridge Mode and Transparent Bridge Mode - High Availability only:** Select the appropriate Ethernet ports from the drop-down lists for the Internal and External interfaces.

      The Interface Status graphic displays your selection.

   c. Select the IP address type from the drop-down list:

      - **Static IP address** - to configure IP settings for the interface manually.
      - **Obtain from (DHCP)** - to have a DHCP server assign IP settings to the interface. (IPv6 addresses, gateways, and DNS can be obtained from DHCPv6.

   d. Enter the IP address and Netmask.

   e. Check the **Enable Ping** check box to allow the connection to be checked with the ping utility.

   f. (Optional) **Transparent Bridge Mode and Transparent Bridge Mode - High Availability only:** Click the check box to enable the VLAN ID (1-4094)

      Note: The HA parent unit and the HA child unit have separate, unique VLAN ID settings.

   g. Do one of the following:

  - Continue with the deployment mode settings, if you are setting up IWSVA for the first time or
  - Click **Next** and click through the remaining screens if you have already setup your deployment mode and are only modifying the data interface.

3. If needed, set up Data Interface access control list. See Configuring Internet Access Control Settings on page 7-13.
4. Continue to the section about Separate Management Interface starting on page 2-33.

Separate Management Interface

The separate management interface offers administrators an independent interface to log into the IWSVA device, either through the Web console or via SSH.

Enabling and disabling the separate management interface is done by setting the values and enabling them through the Network Settings page of the Deployment Wizard. You can use both IPv4 and IPv6 addresses.

Note: The separate management interface must be enabled for HA environments.

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the IWSVA host information
- Configured the Data Interface information

To setup the separate management interface:

1. Continue working from the **Network Interface** page of the Deployment Wizard.
2. Check the check box for the **Enable Management Interface**.
3. Select an **Ethernet interface** from the drop-down list.
4. Enter a **Static IP address** for the management interface device.
5. Enter the **Netmask** for the management interface device.
6. Check the Enable Ping check box to allow the connection to be checked with the ping utility.
7. Do one of the following:

- Continue with the deployment mode settings, if you are setting up IWSVA for the first time or
- Click **Next** and click through the remaining screens if you have already setup your deployment mode and are just adding the separate management interface.

Miscellaneous Settings (IPv4 and IPv6)

The Miscellaneous Settings (IPv4 and IPv6) sections allow you to obtain the dynamic information from DHCP or enter static information for:

- Gateway IP addresses
- Primary DNS server IP addresses
- Secondary DNS server IP addresses

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the IWSVA host information
- Configured data and management interface information

To configure the Miscellaneous settings:

1. Continue working from the **Network Interface** page of the Deployment Wizard.
2. Scroll to the **Miscellaneous Settings** section.

3. Do one of the following:
   - Check the **Obtain from DHCP** check box to have IWSVA obtain the dynamic Gateway, Primary, and Secondary DNS information OR
   - Type in the Gateway, Primary, and Secondary DNS information if it is static.

TABLE 2-9. Miscellaneous Settings information

PARAMETER	DESCRIPTION
Gateway	For static IP address configuration of the network device, type in the applicable (IPv4 or IPv6) IP address used as the gateway for this IWSVA installation.
Primary DNS	For static IP address configuration of the network device, type in the applicable IP address used as the primary DNS server for this IWSVA installation.
Secondary DNS	For static IP address configuration of the network device, type in the applicable IP address used as the secondary DNS server for this IWSVA installation.

4. Click **Next**.
5. Continue to the section on Static Routes starting on page 2-35.

Static Routes

Static routes allow IWSVA to overcome problems routing traffic to and from network segments beyond the next router hop to which IWSVA connects. Static routes allow you to manually control the router connection used to send traffic to the Internet or back to the end users.

For example, if IWSVA updates patterns with an internal ActiveUpdate (AU) server through a different router, a static route should be added for AU server.

Note: If you bind a static route to an interface, the router port must be in the same network segment as the interface.

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the network interface information

To configure settings for Static Routes:

1. From the Static Routes page in the Deployment Wizard, go to the Settings section and configure the following:
    - Network ID
    - Netmask
    - Router
    - Interface

Note: You can also add IPv6 routes into these static routes.

2. Click **Add to List**.

   The static route displays in the Static Routes list.
3. Add additional static routes.
4. Click **Next**.
5. Continue to Product Activation starting on page 2-36.

Product Activation

After completion of the registration process, performed during deployment, you must activate (or enable) your software. Trend Micro products do not scan traffic or enforce policy settings unless a valid Activation Code is entered.

To receive your Activation Code, you must enter your registration key with the Trend Micro Product Registration server.

To activate IWSVA:

1. Go to the Product Activation page in the Deployment Wizard.
2. Type the Activation Code for IWSVA.
3. Click **Next**.
4. Continue with *System Time Settings* on page 2-40.

About Licenses

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis according to Trend Micro’s Maintenance Fee pricing.

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement. The Maintenance Agreement expires but your License Agreement will not.

Note: The Maintenance Agreement expires but your License Agreement will not. If the Maintenance Agreement expires, your system will continue scanning, but you will not be able to update the virus pattern file, scan engine, or program files (even manually). Nor will you be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the upcoming discontinuation. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

`https://olr.trendmicro.com/registration/`

Third-party Licensing Agreements

Access third-party licensing agreements in the following directory:

`/usr/share/doc`

Registering Online

Registration must take place prior to activating the product.

There are several ways to register IWSVA:

- To register if you are a new customer: on page 2-38
- To register if you are a registered user: on page 2-38

To register if you are a new customer:

1. Click the **Trend Micro Product Registration Server** link in your product at **Administration > Product License**.
2. In the Enter Registration Key screen, use the Registration Key that came with your product (Trend Micro Enterprise Protection DVD or License Certificate).
3. Click **Continue**, and then **I CONFIRM**.

   The Confirm Product Information screen appears.
4. Click **Continue with Registration** to confirm all the product information.
5. Next, type all the required contact information in the fields provided and click **Submit**.
6. From the Confirm Registration Information screen, click **Edit** to update your contact information and click **OK** to continue.

   The Activation Code screen appears. Your Activation Code will be sent to your registered email address.
7. Click **OK** to finish.

To register if you are a registered user:

1. Click the **Trend Micro Product Registration Server** link in your product at **Administration > Product License**.
2. Type your Logon ID and password in the fields provided, and then click **Login**.

   You will be prompted to change your password the first time you log on.
3. In the My Products screen, click **Add Products** and type the Registration Key.
4. To edit your company profile, click **View/Edit Company Profile.**

   Your Activation Code appears on the next screen.
5. To receive a copy of your Activation Code at your registered email address, click **Send Now**.

Note: For maintenance renewal, contact Trend Micro sales or your reseller. Click Check Status Online at Administration > Product License to update the maintenance expiration date on the Product License screen manually.

About Activation Codes

An Activation Code is required to enable scanning and product updates. You can activate IWSVA during Setup or anytime thereafter. Register IWSVA during installation to receive an Activation Code.

Note: After registering IWSVA, you will receive an Activation Code via email. An Activation Code has 31 characters (including the hyphens) and looks like:

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

A Registration Key has 22 characters (including the hyphens) and looks like:

```
xx-xxxx-xxxx-xxxx-xxxx
```

- You can use a Registration Key to obtain an Activation Code online

You can find an evaluation Registration Key on the Trend Micro Enterprise Protection DVD. Use this key to obtain an Activation Code. You will get an evaluation Activation Code by email when you download IWSVA from the Web.

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the network interface information
- Configured the static routes

To activate IWSVA:

1. Go to the **Product Activation** page in the Deployment Wizard.
2. Type the **Activation Code** for IWSVA.
3. Click **Next**.
4. Continue with System Time Settings starting on page 2-40.

System Time Settings

System Time and Time Zone settings allow you to:

- Use the current system time
- Synchronize with your NTP server
- Enter the date and time manually
- Select your time zone

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the network interface information
- Configured the static routes
- Entered product activation information

To set the system time and time zone settings:

1. Access the System Time page of the Deployment Wizard.
2. Select from one of the following options:
   - Current system time - keep the time already set on the system
   - Synchronize with NTP server (should support both IPv4 and IPv6 servers) -
   - Manually - Set the date and time manually
3. Set the appropriate time zone.
   - Select your continent from the drop-down list.
   - Select your city (or a city near you with the same time as your location) from the drop-down list.
4. Click **Next.**

Results

The results page will let you know if your settings were entered successfully and that IWSVA has been deployed. It will also indicate if your settings were not accepted.

The system checks deployment settings at the time of entry, before you move from one page in the Deployment Wizard to the next. Successful results are the most common outcome.

Deployment Status

This messages displays if your IWSVA deployment was successful with a status bar that reflects the on-going deployment your mode settings.

> "Congratulations! Your appliance has been set up and deployed."
>
> You will be redirected to <IWSVA Web Console IP address> shortly. It may take several minutes for the system to implement the new configuration changes and to restart before allowing you to log in."

Note: Trend Micro recommends you apply the latest software and/or OS updates for IWSVA as soon as you receive this message. For more information, see Chapter 4 Updates starting on page 4-1.

Even if your deployment is successful, you could receive a message indicating a problem accessing the Web console. The message contains a suggestion on how to fix the problem. See the following example:

> "You designated DHCP protocol to configure the IWSVA network interface, which prohibits the Deployment Wizard from finding the Web console IP address automatically. The IP address and port number can be obtained from the IWSVA server display."

Post Deployment

After the Deployment Wizard is successfully configured, IWSVA automatically reboots. When rebooting the machine, the CLI shell login page should prompt all access addresses including the IPv4 and IPv6 URLs if you have configured an IPv6 address.

If you have configured an IPv6 address for IWSVA, you can access the Web console and CLI using the very IP address (IPv4 or IPv6 addresses) configured during the installation process. After IWSVA reboots, Trend Micro recommends you update IWSVA as soon as possible. See Updates on page 4-1 for details.

Also:

- If you deployed in Transparent Bridge mode, see LAN Bypass Function on page 2-42 for details on failopen NIC support.
- If you deployed in ICAP mode, see Setting Up IWSVA ICAP on page 2-45 for details on setting up an ICAP-compliant cache server to work with IWSVA.
- See Testing and Configuring IWSVA on page 16-1 for step-by-step processes to validate your installation.

LAN Bypass Function

The LAN bypass function allows the customer to install a Trend Micro supported fiber or Gigabit network interface card (NIC) into the supported server platform to allow the network traffic to be bypassed on specific error conditions.

Note: IWSVA only supports LAN bypass functionality in Transparent Bridge Mode.

Note: The IWSVA Admin console contains a bypass button that allows users to bypass traffic manually without having the LAN-Bypass card in bridge mode.

Setup the by-pass function in one of three settings:

- **Auto**—Bypass is OFF when the system is in a normal state; Bypass mode is ON when system detects an abnormal state such as kernel panic issue or when power is cut off from the IWSVA unit
- **On**—Always bypass traffic
- **Off**—Never bypass traffic

Note: When the LAN bypass function is set to ON, the data interface is not available. However, the customer can still access IWSVA via the separate management interface, if configured.

The LAN bypass function supports two port Silicom cards:

- **PE2G4BPI35A-SD-OU**:

http://silicom-usa.com/Networking_Bypass_Adapters/PE2G4BPi35-Quad_Port_Copper_Gigabit_Ethernet_PCI_Express_Bypass_Server_Adapter_Intel_based_58

- **PEG2BPI6-SD-OU-ROHS**

  http://silicom-usa.com/Networking_Bypass_Adapters/PEG2BPi6-Dual_Port_Copper_Gigabit_Ethernet_PCI_Express_Bypass_Server_Adapter_Intel_based_58

- **PEG2BPFI6-SD-OU-ROHS**

  http://silicom-usa.com/Networking_Bypass_Adapters/PEG2BPFi6-Dual_Port_Fiber_Gigabit_Ethernet_PCI_Express_Bypass_Server_Adapter_Intel_based_58

- **PEG2BPFI6-LX-SD-OU-ROHS**

  http://silicom-usa.com/Networking_Bypass_Adapters/PEG2BPFi6-Dual_Port_Fiber_Gigabit_Ethernet_PCI_Express_Bypass_Server_Adapter_Intel_based_58

Enabling the LAN Bypass Function

The following procedure allows you to change the default settings for the LAN bypass feature. Change parameters when:

- Installing a new LAN bypass card
- Selecting NICs supporting LAN bypass for the data interface
- Changing the default LAN bypass mode

If you select one of the supported NICs that can perform hardware bypass in the Deployment Wizard, it will be enabled with the AUTO setting. Under the AUTO setting, the IWSVA monitors the critical services and OS kernel for crashes. If it detects an unrecoverable error, it will open the NIC into “fail open” or bypass mode.

Use the `show network lanbypass` command to check the LAN bypass status on IWSVA.

To display/enable/disable/change the LAN bypass service on the IWSVA unit:

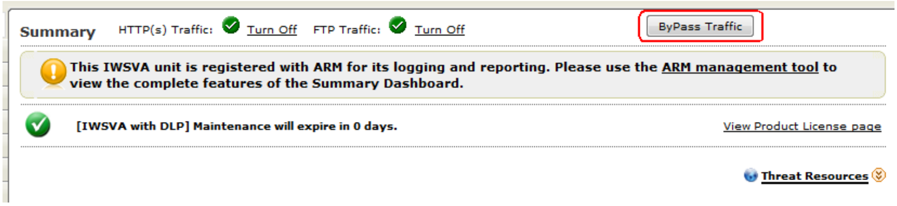
1. Login to the CLI interface.
2. Execute one of the following commands in *Table 2-10*.

TABLE 2-10. LAN Bypass CLI Commands

COMMAND	DESCRIPTION
`show network lanbypass`	Displays the current configuration status of LAN bypass function.
`configure network lanbypass on`	Always bypasses traffic. After running this command, all traffic will be bypassed by LAN bypass card. Administrators may not be able to access the IWSVA device from the network data interface. The system will not adjust the LAN bypass status at any time.
`configure network lanbypass off`	Never bypasses traffic. The system will not adjust the LAN bypass status at any time.
`configure network lanbypass auto`	The system will auto-adjust the LAN bypass status. For example, when system starts and stops, the bypass will be turned off and turned on. When system is in an abnormal state (such as kernel panic), the bypass will be turned on. After recovery, the bypass will be turned off automatically.

The LAN bypass card configuration is saved at: /etc/lanbypass.conf. Migration updates the mapping table to import or export the LAN bypass configuration.

Note: The "ByPass Traffic" option allows an administrator to bypass traffic manually (without the LAN-Bypass card) in bridge mode.



This IWSVA unit is registered with ARM for its logging and reporting. Please use the ARM management tool to view the complete features of the Summary Dashboard.

✓ [IWSVA with DLP] Maintenance will expire in 0 days.

FIGURE 2-11. ByPass Traffic Option

Setting Up IWSVA ICAP

Perform these configuration steps if you are running IWSVA with an ICAP handler.

1. Setting up an ICAP 1.0-compliant Cache Server on page 2-45
2. Flushing Existing Cached Content from the Appliance on page 2-51

Note: The ICAP setup procedures below apply to the ICAP versions listed under X-Authenticated ICAP Headers Support on page 1-13. They are provided for your convenience; consult the native documentation for complete information.

Setting up an ICAP 1.0-compliant Cache Server

Configure an ICAP client (for example, Network Appliance Blue Coat Port 80 Security Appliance cache server/Cisco ICAP server) to communicate with the ICAP server.

See the appropriate process for your ICAP client:

- To set up ICAP for the Blue Coat Port 80 Security Appliance: on page 2-45
- To set up Cisco CE ICAP servers: on page 2-48

To set up ICAP for the Blue Coat Port 80 Security Appliance:

1. Log onto the Web console by typing `https://{SERVER-IP}:8082` in the address bar of your Web browser.

Note: The procedure for setting up ICAP on a Blue Coat appliance might vary depending on the product version.

2. Select **Management**.

   Type the logon user name and password, if prompted.
3. Click **ICAP** in the left menu, then click the **ICAP Services** tab.
4. Click **New**.

   The **Add ICAP Service** screen opens.
5. In the **ICAP service name** field, type an alphanumeric name. Click **Ok**.
6. Highlight the new ICAP service name and click **Edit**.

   The **Edit ICAP Service name** screen opens.
7. Type or select the following information:
   a. The ICAP version number (that is, 1.0)
   b. The service URL, which includes the virus-scanning server host name or IP address, and the ICAP port. The default ICAP port is 1344.
      - Response mode:

      `icap://{ICAP-SERVER-IP}:1344`
      - Request mode:

      `icap://{ICAP-SERVER-IP}:1344/REQ-Service`

      where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP.
   c. The maximum number of connections (ranges from 1-65535). The default value is 5.
   d. The connection time-out, which is the number of seconds the Blue Coat Port 80 Security Appliance waits for replies from the virus-scanning server. The range is an interval from 60 to 65535. The default time-out is 70 seconds.
   e. Choose the type of method supported (response or request modes).
   f. Use the default preview size (bytes) of zero (0).
   g. Click **Sense settings** to retrieve settings from the ICAP server (recommended).
   h. To register the ICAP service for health checks, click **Register** under the **Health Check Options** section.
8. Click **Ok**, then click **Apply**.

Note: You can edit the configured ICAP services. To edit a server configuration again, select the service and click **Edit**.

9. Add the response or request mode policy.

The Visual Policy Manager requires the Java 2 Runtime Environment Standard Edition v.1.3.1 or later (also known as the Java Runtime or JRE) from Sun™ Microsystems, Inc. If you already have JRE on your workstation, the Security Gateway opens a separate browser window and starts the Visual Policy Manager. The first time you start the policy editor, it displays an empty policy.

If you do not have JRE on your workstation, a security warning window opens. Click **Yes** to continue. Follow the instructions.

To add the response mode policy:

1. Select **Management**.

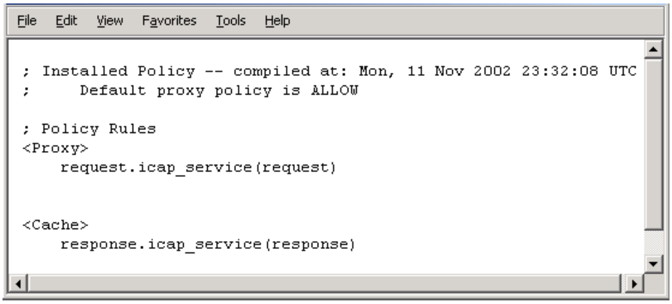
   Type the logon user name and password if prompted.
2. Click **Policy** on the left menu, then click the **Visual Policy Manager** tab.
3. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.
4. On the menu bar, click **Edit > Add Web Content Policy**. The **Add New Policy Table** screen opens.
5. Type the policy name under the **Select policy table name** field. Click **OK**.
6. Under the **Action** column, right-click **Bypass ICAP Response Service** and click **Set**. The **Add Object** screen opens. Click **New** and select **Use ICAP Response Service**. The **Add ICAP Service Action** screen opens.
7. Choose the ICAP service name under the **ICAP Service/Cluster Names** field. Enable **Deny the request** under the **On communication error with ICAP service** section. Click **OK**, then click **OK** again.
8. Click **Install Policies**.

To add the request mode policy:

1. Follow Step 1 through Step 5 in the previous procedure.
2. Under the **Action** column, right-click **Deny** and click **Set**. The **Add Object** screen opens. Click **New** and select **Use ICAP Request Service**. The **Add ICAP Service Action** screen opens.

3. Choose the ICAP service name under the **ICAP Service/Cluster Names** field.
4. Enable **Deny the request** under the **On communication error with ICAP service** section.
5. Click **OK** and then **OK** again.
6. Click **Install Policies**.
7. Configure both the request and response mode ICAP services.

   To check the current policy, go to the Policy screen, click the **Policy Files** tab, and then click **Current Policy**.



```
; Installed Policy -- compiled at: Mon, 11 Nov 2002 23:32:08 UTC
;     Default proxy policy is ALLOW

; Policy Rules
<Proxy>
    request.icap_service(request)


<Cache>
    response.icap_service(response)
```

FIGURE 2-12. Install Policies screen

To set up Cisco CE ICAP servers:

IWSVA supports Cisco ICAP servers (CE version 5.1.3, b15). All ICAP settings are performed through a command line interface (CLI); there is no user interface associated with the Cisco ICAP implementation.

1. Open the Cisco CE console.
2. Type **`config`** to enter the configuration mode.
3. Type **`icap?`** to display a list of all ICAP-related commands.
4. Create a response modification service, by typing:

   ```
   icap service RESPMOD SERVICE NAME
   ```

   This takes you into the ICAP service configuration menu. Type **`?`** to display a list of all available commands. Type the following commands:

   `server icap://ICAP SERVER IP:1344/resp` (to assign a server type)

vector-point respmod-precache (to assign the proper vector point type)

error-handling return-error (to assign the proper error-handling type)

enable (to enable the ICAP multiple server configuration)

5. Type **exit**.
6. Create a request modification service, by typing

```
icap service REQUESTMOD SERVICE NAME
```

This command takes you into the ICAP service configuration menu. Type **?** to display a list of all available commands. Issue the following commands:

server icap://ICAP SERVER IP:1344/REQ-Service (to assign a server type)

vector-point reqmod-precache (to assign the proper vector point type)

error-handling return-error (to assign the proper error-handling type)

enable (to enable the ICAP multiple server configuration)

7. Type **exit**.
8. For additional configuration steps, type the following:

icap append-x-headers x-client-ip (to enable X-client headers for reports)

icap append-x-headers x-server-ip (to enable X-server headers for reports)

icap rescan-cache ISTag-change (to turn on ISTAG rescan for updates)

icap bypass streaming-media (to exclude streaming media from ICAP scanning)

icap apply all (to apply all settings and activate ICAP type)

show icap (to display current ICAP configuration at root CLI menu)

Configuring Virus-scanning Server Clusters

For the Blue Coat Port 80 Security Appliance to work with multiple virus-scanning servers, configure a cluster in the Security Gateway (add the cluster, and then add the relevant ICAP services to the cluster).

To configure a cluster using the Web console:

1. Select **Management**.

   Type the logon user name and password if prompted.
2. Click **ICAP** on the left menu, then click the **ICAP Clusters** tab.

3. Click **New**.

   The **Add ICAP Cluster** screen opens.
4. In the **ICAP cluster name** field, type an alphanumeric name and click **Ok**.
5. Highlight the new ICAP cluster name and click **Edit**.

   The **Edit ICAP Cluster name** screen opens.
6. Click **New** to add an ICAP service to the cluster.

   The **Add ICAP Cluster Entry** screen opens. The pick list contains a list of any services available to add to the cluster.
7. Choose a service and click **Ok**.
8. Highlight the ICAP cluster entry and click **Edit**.

   The **Edit ICAP Cluster Entry name** screen opens.
9. In the **ICAP cluster entry weight** field, assign a weight from 0-255.
10. Click **Ok**, click **Ok** again, and then click **Apply**.

Deleting a Cluster Configuration or Entry

You can delete the configuration for an entire virus-scanning server cluster, or you can delete individual entries from a cluster.

Note: Do not delete a cluster used in a Blue Coat Port 80 Security Appliance policy if a policy rule uses a cluster name.

To delete a cluster configuration using the Web console:

1. Select **Management**.

   Type the logon user name and password if prompted.
2. Click **ICAP** on the left menu, then click the **ICAP Clusters** tab.
3. Click the cluster you want to delete.
4. Click **Delete**, then click **Ok** to confirm.

Flushing Existing Cached Content from the Appliance

There is a potential risk of infection from content cached to the Blue Coat Port 80 Security Appliance or the Cisco ICAP servers before IWSVA ICAP started scanning HTTP traffic. To safeguard against this possibility, Trend Micro recommends flushing the cache immediately after configuring IWSVA ICAP. All new requests for Web content are then served from the Internet and scanned by IWSVA ICAP before caching. Scanned content is then cached on the Blue Coat Port 80 Security Appliance or the Cisco ICAP servers. The the Blue Coat Port 80 Security Appliance or the Cisco ICAP servers serve future requests for the same Web content by your network users. Because the request is not sent to the Internet, download time is accelerated.

To flush the cache in the Blue Coat Port 80 Security Appliance:

1. Select **Management**.

   Type the logon user name and password if prompted.
2. Click **Maintenance**.
3. Click the **Tasks** tab and click **Clear**. Click **OK** to confirm.

To flush the cache in the Cisco ICAP server:

1. Telnet to Cisco CE.
2. At the root CLI menu, type **cache clear**.
3. Press **Enter**.

Verifying that InterScan Web Security Virtual Appliance is Listening for ICAP Requests

To verify that IWSVA is listening on the correct port, use PuTTY to access IWSVA via SSH as the “admin” user.

After logging in as the “admin” user, issue the CLI command `show network connections all CLI command` to show all active network connections through IWSVA. There should now be a TCP port access available on port **1344**.

Sample of command and output:

```
enable# show network connections all
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address
State
tcp       0      0 0.0.0.0:9091               0.0.0.0:* LISTEN
tcp        0      0 127.0.0.1:8005              0.0.0.0:* LISTEN
tcp        0      0 0.0.0.0:1812                0.0.0.0:* LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:* LISTEN
tcp        0      0 0.0.0.0:5432                0.0.0.0:* LISTEN
tcp        0      0 10.204.170.156:22           10.204.170.158:2665
ESTABLISHED
udp        0      0 0.0.0.0:514                 0.0.0.0:*
udp        0      0 0.0.0.0:21273               0.0.0.0:*
udp        0      0 0.0.0.0:35739               0.0.0.0:*
udp        0      0 0.0.0.0:7068                0.0.0.0:*
udp        0      0 0.0.0.0:17437               0.0.0.0:*
udp        0      0 0.0.0.0:22688               0.0.0.0:*
udp        0      0 0.0.0.0:9911                0.0.0.0:*
udp        0      0 0.0.0.0:30138               0.0.0.0:*
udp        0      0 0.0.0.0:60733               0.0.0.0:*
udp      0     0 127.0.0.1:9925           127.0.0.1:9925
ESTABLISHED
udp        0      0 0.0.0.0:36946               0.0.0.0:*
udp        0      0 0.0.0.0:41560               0.0.0.0:*
udp        0      0 0.0.0.0:29294               0.0.0.0:*
udp        0      0 0.0.0.0:12655               0.0.0.0:*
udp        0      0 0.0.0.0:38390               0.0.0.0:*
udp        0      0 0.0.0.0:7036                0.0.0.0:*

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State     I-Node    Path
unix  2   [ ACC ] STREAM  LISTENING 6643358 /tmp/ssh-ddgvf12499/agent.12499
unix  2   [ ACC ] STREAM  LISTENING 634599   /var/run/nscd/socket
unix  2   [ ACC ]  STREAM LISTENING   7249   /var/run/dbus/system_bus_socket
unix  2   [ ACC ]  STREAM LISTENING   7368   @/var/run/hald/dbus-uIGJbIMMam
unix  2[ ]          DGRAM                6421523 /tmp/tmsyslog
unix  2   [ ]       DGRAM                6421525 /tmp/log
unix  2   [ ACC ]  STREAM LISTENING   3065236/tmp/.s.PGSQL.5432
unix  2   [ ]       DGRAM                1274   @/org/kernel/udev/udevd
unix  2   [ ]       DGRAM                7379 @/org/freedesktop/hal/udev_event
unix  2   [ ACC ]  STREAM LISTENING   7369 @/var/run/hald/dbus-0oDgnh6zwa
unix  5   [ ]       DGRAM                6430159 /dev/log
unix  2   [ ]       DGRAM                6643350
unix  2   [ ]       DGRAM                6603791
unix  2   [ ]       DGRAM                6430163
unix  2   [ ]       DGRAM                065234
unix  3   [ ]       STREAM CONNECTED   8017 /var/run/dbus/system_bus_socket
unix  3   [ ]       STREAM CONNECTED   8016
unix  3    [ ]      STREAM  CONNECTED   8003 @/var/run/hald/dbus-uIGJbIMMam
unix  3    [ ]      STREAM  CONNECTED   8002
unix  3    [ ]      STREAM  CONNECTED   7872 @/var/run/hald/dbus-uIGJbIMMam
unix  3    [ ]      STREAM  CONNECTED   7870
unix  3    [ ]      STREAM  CONNECTED   7835 @/var/run/hald/dbus-uIGJbIMMam
unix  3    [ ]      STREAM  CONNECTED   7834
unix  3    [ ]      STREAM  CONNECTED   7372 @/var/run/hald/dbus-0oDgnh6zwa
unix  3    [ ]      STREAM  CONNECTED   7371
unix  3    [ ]      STREAM  CONNECTED   7257
unix  3    [ ]      STREAM  CONNECTED   7256
    enable#
```

Understanding the Differences between Request Mode and Response Mode

ICAP Request Mode: When a new request is received, the request is sent to the scanning server to ensure it is a valid access request.

ICAP Response Mode: When the new request is valid, any returned content is scanned.

It is possible to use only one scanning vector; however, this reduces the ability to scan all appropriate traffic by 50%.

Triggering a Request Mode Action

The steps outlined below are specifically for the triggering of a request mode action through IWSVA:

1. Log into a client that is passes traffic through IWSVA.
2. Open a Web browser and open the site www.goodclup.com/caiink/t1.exe

The outbound URL is passed to InterScan Web Security Suite and is blocked. Damage Cleanup Services is still configured to perform an automatic cleanup, the workstation also has an automatic remediation attempt performed against it.

Triggering a Response Mode Action

The steps outlined below are specifically for the triggering of a response mode action through IWSVA.

1. Log into a client that is passes traffic through IWSVA.
2. Open a Web browser and open the site www.eicar.org.
3. Click on the button labeled **AntiMalware Testfile**.
4. Scroll to the bottom of the page where it details **Download area using the standard protocol http.**
5. Select the **eicar.com.txt** file to download.

The outbound URL is valid, thus the request mode allowed the URL to pass. The response of the traffic — the actual download triggers InterScan Web Security to block the download from occurring.

Chapter 3

High Availability and Cluster Management for Transparent Bridge Mode

This chapter discusses how High Availability functions in Transparent Bridge mode and how to use the Cluster Management interface.

Topics in this chapter include the following:

High Availability Overview

IWSVA provides native High Availability (HA) to ensure business continuity using active/passive pairs deployed in Transparent Bridge mode.

Note: The IWSVA HA solution currently only supports active/passive pairs in "Transparent Bridge mode" for High Availability. It only supports two HA nodes in one HA cluster. Redundancy among multiple IWSVAs deployed in the other supported deployment modes is handled externally to the IWSVA. Specifically, load balancers support redundancy in any of the proxy modes. The Cisco WCCP device can manage traffic to redundant IWSVAs in WCCP mode. The ICAP client can manage traffic to redundant IWSVAs in ICAP mode.

The four terms to describe HA cluster members are:

- **Active member**—The IWSVA unit providing real-time content scanning.
- **Passive member**—The IWSVA unit in passive standby mode.
- **Parent member**—The IWSVA unit responsible for accepting all configuration changes and synchronizing the policy and configuration with the child member.
- **Child member**—The IWSVA unit that is receiving the policy and configuration changes in the background.

HA switchover can be automatic (failover) or manual.

For failover:

- IWSVA's HA service monitors the critical services of the IWSVA application and the underlying OS for failures. If an abnormality occurs on the active unit, the HA service switches from the active node to the passive node automatically.
- Some of the administrator's HA management operations—like joining of a node or the shutdown of the parent—can trigger an automatic switchover. HA handles this type of switchover gracefully and automatically.

For manual switchover:

- Administrators can manually force an HA switch over using the Web console on the parent node.

Note: 1) HA disables the LAN By-pass feature. It is not required with HA.
2) HA requires the enabling of the Spanning Tree Protocol (STP). This prevents the creation of Layer 2 loops in the network.
3) If the switch used by the HA solution supports Rapid Spanning Tree Protocol (RSTP), then this requires that STP be disabled on the IWSVA to provide faster switching.
4) Enabling STP/RSTP requires disabling the PortFast Bridge Protocol Data Unit (BPDU) guard on both switches because BPDU disables the ports on the switches and prevents HA from functioning.

About Active/Passive Pairs

The active/passive pair can be connected directly together or through a dedicated switch. The active/passive pair requires two private IP addresses and a private reserved subnet for proper configuration. These private IP addresses are reserved for the HA function's internal use and are used for HA heartbeat information and data synchronization. No user devices are allowed on this private subnet.

IWSVA uses a cluster IP address for the active/passive pair, which is used for managing the HA cluster. This cluster management IP address floats between the two HA units and is always associated with the active member of the HA pair.

The active node scans HTTP, HTTPS, and FTP traffic. The passive node works as stand-by device which does not scan traffic in normal conditions. The passive node can become the active node if an abnormal condition occurs in the active node, such as:

- Data link failure
- OS kernel panic
- Critical services of the IWSVA application fail

IWSVA triggers a failover when the active unit goes down, whether it is caused by a heartbeat down, application down, or system down condition. When a failed unit is brought back online, a user-defined policy determines which unit becomes the newly elected active unit. Administrators can configure the election policy to allow the passive unit to remain as the active unit (normal mode), or configure the election policy with node weighting to always allow a specific HA member to regain control as the active unit.

The HA Agent Handles Status Changes

The IWSVA device that joins the cluster as the first member becomes the active parent node by default.

If the Weighted Priority Election feature is not enabled, the second IWSVA device that joins an existing cluster becomes the passive child node by default.

If the Weighted Priority Election feature is enabled, and a second IWSVA device joins an existing cluster with a higher weighting than the first cluster member, that higher weighted, second machine becomes the active parent member and the original member becomes the passive child member.

Failover vs. Switchover

Failover occurs when the active node crashes or fails to handle traffic normally. IWSVA automatically switches over to the passive standby machine in the cluster and elects the new machine to be the active member.

Switchover occurs when a manual role change is forced through the parent's web management interface—allowing the original child/passive unit to become the new parent/active unit.

HA Agent and Interfaces

The HA Agent can be configured with the following management features:

- About the Deployment Wizard on page 3-4
- About the Application Health Monitor on page 3-5
- About Central Management on page 3-6
- About Cluster Management on page 3-10

About the Deployment Wizard

Use the Deployment Wizard to access the following operations:

- Creating a Cluster on page 3-5
- Joining a Cluster on page 3-5

Note: For more about using the Deployment Wizard, see Chapter 2, *Deployment Wizard*..

Creating a Cluster

A new HA cluster is created through the Deployment Wizard interface. When a new HA cluster is created, the management system configures the HA Agent with the desired policy settings and stores it on the parent member. Parent members are the only units that can be actively configured. A child member receives regular updates from the parent member to stay synchronized with the latest configuration and policy information. See step-by-step instructions for creating a cluster at Create a New Cluster on page 2-6.

Note: HA Cluster IP's do not support IPv6 addresses.

Joining a Cluster

When HA members are added to the HA cluster, the Deployment Wizard captures and configures each member with the appropriate network and weight information to setup the parent and child members.

The member with the higher weighting becomes the parent member. This allows you to manually elect the machine that will become the primary active unit.

The HA Agent is responsible for synchronizing the information between the cluster members and for initiating the failover or switchover.

See step-by-step details at Join an Existing Cluster on page 2-8.

About the Application Health Monitor

The Application Health Monitor is a separate service that monitors the IWSVA application and operating system health. It also communicates all necessary information with the HA Agent to allow rapid failover between the active and passive members.

Link Loss Detection

The parent node monitors the Layer 2 switch connection for failures. If network connectivity is lost on the data port, a switchover is automatically generated to allow a rapid failover to the passive standby member.

The `linkloss_timeout` parameter controls the amount of downtime for the link loss detection. When the timer value set in the linkloss_timeout parameter is reached, the failover process is initiated.

The Health Monitor configuration file allows you to configure the `linkloss_timeout` value. The default is 2 seconds. It is located at in the Health Monitor configuration file at: `/etc/iscan/intscan.ini`.

```
[health-monitor]

linkloss_timeout=2
```

After modifying the file, restart the `svcmonitor` services by using the following command:

/etc/iscan/S99ISsvcmonitor restart

Note: IWSVA can detect link loss in the bare metal environment.

About Central Management

Central Management is the feature used to manage two HA nodes as a single device. This allows configuration changes to take place on the parent unit and be automatically synchronized with the child unit.

Note: Central Management only applies to the active/passive pair scenario. It cannot be used for single devices.

Central Management automatically synchronizes configuration information between the parent and child members every five minutes. Administrators can also manually trigger synchronization by clicking the "Synchronize Now" button on the title bar of the IWSVA Web console System Status page accessed through the parent node.

IWSVA supports two synchronization mechanisms:

- **Automatic synchronization**—The parent node runs a scheduled task every five minutes to synchronize policies and configurations to the child node.
- **Manual synchronization**—Users can force a synchronization by clicking **Synchronize Now** on the **Administration > IWSVA Configuration > Cluster Management** page of the Web console of the parent node.

Users cannot perform a manual switchover if the configurations on the two nodes are not synchronized. If the configurations are not synchronized during a switchover attempt, IWSVA displays a warning message instructing you to manually synchronize the two members first.

For automatic failovers, the switchover happens immediately without a forced synchronization, and any configuration changes made since the last completed synchronization are lost.

Synchronizing Nodes Manually

Synchronization from the parent member to the child member occurs every five minutes. Administrators can manually trigger an immediate synchronization between the cluster members from the Cluster Management page.

To manually synchronize two nodes:

1. Go to the **System Status** page in the parent member Web console.
2. Click **Synchronize Now** at the top of the System Status page.
3. Click **OK** in the confirmation to immediately synchronize your policies and deployment settings from the parent member to the child member.

Centrally Managed and Non-centrally Managed Features

CLUSTER-LEVEL -- Centrally Managed, settings only can be display and configuration on parent node, and then synchronized to child node.

INSTANCE-LEVEL -- Non-centrally Managed, settings may be difference for parent and child node, can be configuration them on parent or child node separately.

Some features may be managed centrally, while others require administrators to log into the Web console of the parent or child node. See *Table 3-1* for details.

TABLE 3-1. Centrally Managed vs. Non-centrally Managed Features

CLUSTER-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT NODE	INSTANCE-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT OR CHILD NODE
Enable/disable HTTP/HTTPS/FTP traffic	• Dashboard /Virus/Malware/URL/Spyware/ Security Risk Report
All HTTP/HTTPS policies and settings (under HTTP/HTTPS section) • Includes HTTPS certifications	Reports (features and data) • Report Template • Manual Reports data • Scheduled Reports data
All FTP policies and settings (under FTP section)	Logs (features and data) • Log Analysis
Report Settings • Report Templates	Updates (manual update)
Log Settings • Syslog Configuration • Log Settings	Test database connection feature (under Administration > IWSVA Configuration > Database Connection)
Update Settings • Scheduled Update Settings • Connection Settings	Interface Configuration for data port and management port • Hostname • IP address and net mask • Port for data interface or management interface

TABLE 3-1. Centrally Managed vs. Non-centrally Managed Features (Continued)

CLUSTER-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT NODE	INSTANCE-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT OR CHILD NODE
Notification settings • Notification page • Threshold Alert Settings on Summary page • SMTP settings • SNMP settings under Administration > Network Configuration > SNMP Settings	TMCM Registration
Quarantine Management (under Administration > Quarantine Management)	System patch
System Time	Update OS
Network Settings (Except Hostname, IP, net mask, and port) • Enable Ping for each interface • DNS • Default Gateway • Static Routes **Note:** DHCP is removed in HA	Support
Web Console settings (under Administration > Network Configuration > Web Console)	
Remote CLI settings (under Administration > Network Configuration > Remote CLI)	
User accounts (under Administration)	

TABLE 3-1. Centrally Managed vs. Non-centrally Managed Features (Continued)

CLUSTER-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT NODE	INSTANCE-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT OR CHILD NODE
Configuration backup/restore	
Product License	
DEPLOYMENT WIZARD CONFIGURATIONS	
System time Deployment Mode Static Routes Data Interface & Management Interface • DNS • Default gateway • Static Router • Enable PING	Data Interface and Management Interface • Hostname • IP address and net mask • Port number

About Cluster Management

The Cluster Management screen is located at **Administration > IWSVA Configuration > Cluster Management** and is used to configure the HA cluster. The cluster settings are saved in the cluster configuration file and used by the Central Management feature and the HA Agent to create the HA policies and failover priorities. Changing the weight values of the cluster members allow manual parent/active member selection, but may also cause a switchover to occur. See About Weighted Priority Election on page 2-6 for details.

Cluster Configuration

Cluster configurations are settings that are replicated cluster-wide and every HA member is configured with the same cluster configuration information. The Central Management and Cluster Management components use cluster information to provide rapid failover without loss to critical policy and configuration information.

The cluster configuration file, `cluster.ini`, is stored in the `/etc/iscan` folder and is used to store the HA cluster settings. You can configure the following elements of a cluster through the Web console Cluster Management page:

- **Cluster Name—**The name of the cluster
- **Cluster Description—**The description of the cluster
- **Cluster IP Address—**The floating management IP address of the cluster is always associated with the active node. IWSVA can show both IPv4 and IPv6 addresses if configured for cluster, parent, and child, for example, as 172.16.2.200/2001:10::101.
- **Weighted Priority Election—**Enable or disable (default)
- **Cluster Members—**The list of the nodes (IPv4 or IPv6) belonging to the HA cluster with login access provided to the child nodes.

Note: For this version of IWSVA, the following items are not configurable:
- Cluster Deployment Mode—Always Transparent Bridge mode.
- HA Mode—Always active/passive.
- HA Cluster IP's do not support IPv6 addresses.

Node Configuration

Node configuration settings are applied to a specific HA member and are not cluster-wide settings. These node-specific settings are never synchronized between the HA members. Node specific settings include the following:

- **Hostname—**The name of the node
- **Role**—Either parent or child
- **IP Address—**The IP address used on the heartbeat port. If this is empty, a new IP will be negotiated between the cluster members and written to the IP address parameter.
- **Weight—**The weight of the node. Valid values are 1-255. The higher the weight, the greater the chance the node will be selected to act as the parent node.
- **Status**—Status of the node. Green is up, red is down.
- **Last Synchronization**—Gives the date and time of the last successful synchronization
- **Synchronization Status**—Green is successful, red is failed. If failed, a reason displays in the tooltip.

Cluster Logs and Notifications

The HA cluster logs and records the following events:

- Creating a cluster
- Dissolving or breaking apart an existing cluster
- Adding a member to a cluster
- Changing the configuration of a cluster
- Removing a member from a cluster
- Changing the role of a cluster member
- Performing manual synchronization
- Failing over
- Detecting an abnormality

Cluster notifications are issued when:

- Abnormalities are detected
- A failover occurs
- A member is restored
- A failover or switchover cannot be performed

Accessing the Cluster

To access the parent node:

Administrators can access the parent member's Web management interface through one of two IP addresses:

- Parent member's management IP address and port number
- Cluster IP address and port number

Example:

```
https://<parent management IP address>:<portnumber>
```

```
https://<cluster IP address>:<portnumber>
```

To access the child node:

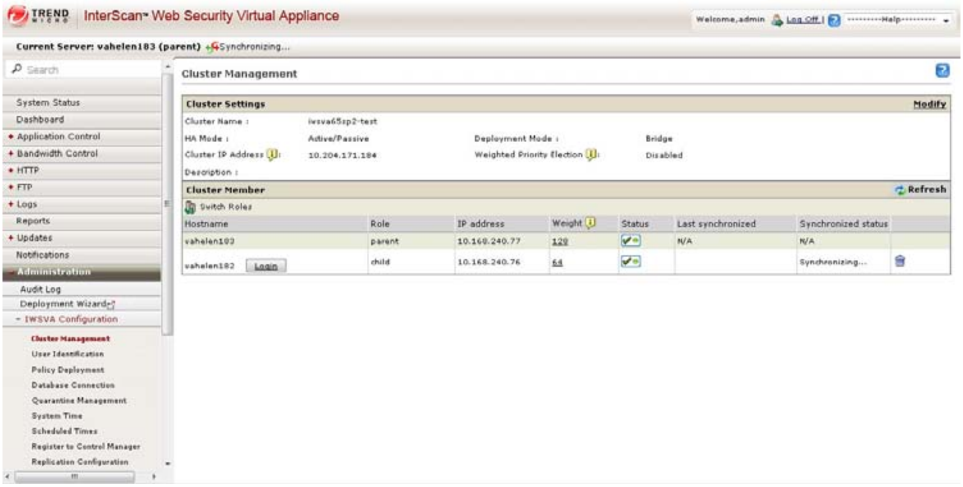
Administrators can log into the Web management console of the child node two ways:

- Through the link on the Cluster Management page (**Administration > IWSVA Configuration > Cluster Management > Login** button for child node)
- Through the management port IP address of the child node

Example:

```
https://<child node IP address>:<portnumber>
```

To protect against accidental configuration, all cluster-level features are hidden or blocked in the child member's Web management interface. (Compare the parent node left menu in *Figure 3-1* with the child node left menu in *Figure 3-2*.) Only the child member applicable configuration parameters that apply specifically to the child member are exposed and configurable through the child member's Web management interface. *Table 3-1* gives a detailed list of child-level settings and features.



Current Server: vahelen183 (parent) Synchronizing...

Cluster Management

Cluster Settings

Cluster Name :	iwsva65sp2-test		
HA Mode :	Active/Passive	Deployment Mode :	Bridge
Cluster IP Address :	10.204.171.184	Weighted Priority Election :	Disabled
Description :			

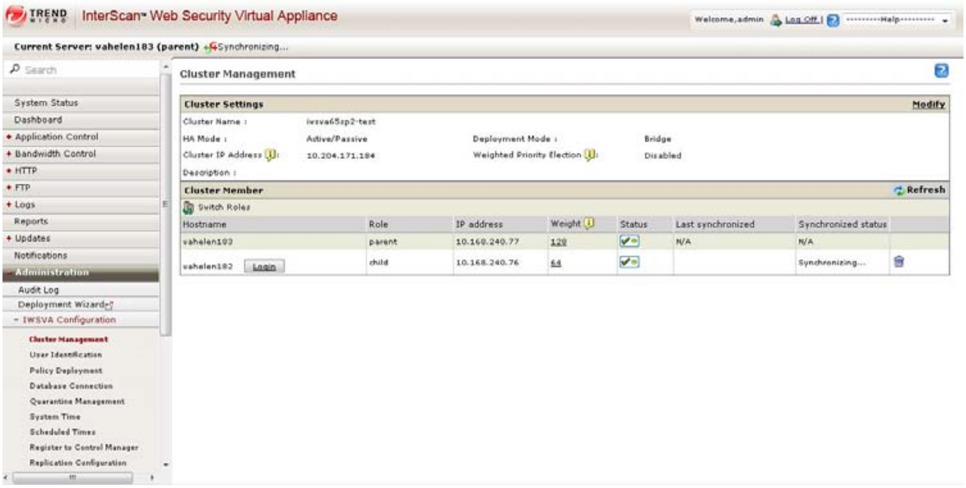
Cluster Member

Hostname	Role	IP address	Weight	Status	Last synchronized	Synchronized status
vahelen183	parent	10.168.240.77	128	✓	N/A	N/A
vahelen182 Login	child	10.168.240.76	64	✓		Synchronizing...

FIGURE 3-1. Parent Node Cluster Management Page has Child Node Login Access

If administrators need to change cluster-level settings while logged into the child member, they can simply login to the parent member through the **Login** button posted beside the parent member on the Cluster Management screen.

IWSVA HA uses single sign-on technology to pass authentication credentials between cluster members so typing a password to access other members are not necessary.



Current Server: vahelen183 (parent) Synchronizing...

Cluster Management

Cluster Settings

Cluster Name : iwsva65sp2-test

HA Mode : Active/Passive

Deployment Mode : Bridge

Cluster IP Address : 10.204.171.184

Weighted Priority Election : Disabled

Description :

Cluster Member

Hostname	Role	IP address	Weight	Status	Last synchronized	Synchronized status
vahelen183	parent	10.168.240.77	128	✓	N/A	N/A
vahelen182	child	10.168.240.76	64	✓		Synchronizing...

FIGURE 3-2. Child node Cluster Management page with access to the parent node.

Note: CLI commands for centrally managed features are not available on the child node.

Cluster Management Web Console Page

From the Cluster Management page at **Administration > IWSVA Configuration > Cluster Management**, administrators can configure the following:

- Deleting a Child Member from a Cluster on page 3-15
- Dissolving a Cluster on page 3-15
- Performing a Manual Switchover on page 3-16
- Synchronizing Nodes Manually on page 3-7
- Modifying a Cluster on page 3-17

Deleting a Child Member from a Cluster

If you delete a child node from a cluster, the cluster still exists with the parent node as the only member. Another node can be added later as a child node.

To delete a child node:

1. Go to **Administration > IWSVA Configuration > Cluster Management** in the parent member Web console.
2. Go the **Cluster Member** section of the page.
3. Click the delete icon (🗑) in the child row to delete the child member.
4. Click **OK** to confirm the deletion. A progress bar displays.
5. If, after a few second, if the deletion has not completed, click your browser's **Refresh** button.

   The child member no longer displays in the Cluster Member list and the former child node will return to Forward Proxy mode.

Dissolving a Cluster

Dissolving an HA cluster breaks apart the HA cluster and occurs after the child member and parent member have been deleted. Dissolving an HA cluster returns the active HA member to a standalone IWSVA device operating in Transparent Bridge mode.

To dissolve a cluster:

1. Go to **Administration > IWSVA Configuration > Cluster Management** in the parent member Web console.
2. Delete the child member of the cluster as shown in Deleting a Child Member from a Cluster on page 3-15.
3. In the **Cluster Member** section of the page, click the delete icon (🗑) to delete the parent member.
4. Click **OK** to confirm the dissolution. A progress bar displays.

   a. If, after five minutes, if the dissolution has not completed, click your browser's **Refresh** button.

      The parent member become a standalone IWSVA unit in Transparent Bridge mode and the Cluster Management page no longer displays.

Performing a Manual Switchover

Administrators can manually switch the parent/child roles of the two members in an HA cluster. After a successful switchover, the original parent member becomes the child member and goes into passive mode. The original child member becomes the parent member and goes into active mode.

Note: Administrators can only perform a manual switchover if the Weighted Priority Election process is disabled. To perform a switchover with Weighted Priority Election mode enabled, administrators must modify the weight of each member to trigger an HA switchover. See Modifying a Cluster on page 3-17 for details on changing the weight value for a cluster member.

To perform a manual switchover with Weighted Priority Election mode disabled:

Note: If IWSVA is performing a synchronization, either a manually or a scheduled synchronization, the Synchronized Status shows “Syncing …”, and manual switchovers are prevented. This applies to switchovers when the Weight Priority Election mode is disabled (by switching roles) or if attempting to change the weight value of a node with the Weighted Priority Election mode enabled. Automatic failovers still occur even if synchronization is in progress, reverting to the policies and deployment settings that existed after the most recent successful synchronization.

1. Go to **Administration > IWSVA Configuration > Cluster Management** in the parent node Web console.
2. In the Cluster member section, click **Switch Roles**.
3. Click **OK** in the confirmation to switch roles and be re-logged into the new parent node.

Modifying a Cluster

The Cluster Management page allows administrators to view cluster settings, modify cluster settings, and to switch roles between parent and child servers.

Table 3-2 shows the Cluster Settings displayed on the Cluster Management page.

TABLE 3-2. Cluster Settings

VALUE	DESCRIPTION
Cluster Name	This is the name assigned to the cluster when it was first created in the Deployment Wizard. (Modifiable)
HA Mode	Active/Passive (Not modifiable)
Cluster IP Address	The floating IP address used to log into the cluster from the Web console or CLI. This IP address remains the same, even after a switchover occurs. (Modifiable)
Description	Displays the (optional) description entered when the cluster was added through the Deployment Wizard. (Modifiable)

TABLE 3-2. Cluster Settings (Continued)

VALUE	DESCRIPTION
Deployment Mode	Currently, this parameter always displays "Bridge" because IWSVA HA clusters are only supported in Transparent Bridge mode. (Not modifiable)
Weighted Priority Election	Displays either Enabled or Disabled. (Modifiable)
Switch Roles	Allows administrators to switch roles between parent and child members.
Refresh	Updates the status of cluster members

This Cluster Members section of the Cluster Management page displays the cluster members (parent and child members), gives status details, and allows login access to the child node.

Table 3-3 shows the parameters displayed for both parent and child nodes.

TABLE 3-3. Cluster Member Settings

PARAMETER	DESCRIPTION
Hostname	Displays the server name
Role	Displays either Parent or Child
IP Address	Displays the IP address of the device.
Weight	Displays the weight entered when the cluster was configured. (Default: parent 128/child 64- Modifiable. Configurable Value: 1-255, higher value = higher priority.)
Status	Displays the following icons: ✓● Up status ✗● Down status

TABLE 3-3. Cluster Member Settings (Continued)

PARAMETER	DESCRIPTION
Last Synchronized	Displays the date and time (hours: minutes: seconds) when the child server was last synchronized with the parent.
Synchronization Status	Displays the following: N/A ✓ Successful Success ✗ Failed ⓘ Failed. If failed, an information tool tip displays the reason why the synchronization failed.
Dissolve	Displays an icon (🗑) to delete the child member. The icon only displays for the parent member if the child member has been deleted. Deleting the parent member dissolves the whole cluster.

To modify cluster settings:

1. Go to **Administration > IWSVA Configuration > Cluster Management.**
2. Click the **Modify** link by the Cluster Settings heading.
3. In the Cluster Settings page, modify the following parameters as needed:
   - **Cluster Name**—Displays the name assigned to the cluster when it was first created in the Deployment Wizard. (Modifiable)
   - **Description**—Displays the (optional) description, if any, entered when the cluster was added through the Deployment Wizard. (Modifiable)
   - **Cluster IP Address**—Displays the floating management (or cluster) IP address used to log into the cluster from the Web console or CLI. The floating IP address is always associated with the active node in the cluster. (Modifiable)
   - **Weighted Priority Election**—Displays either Enabled or Disabled. If the Weighted Priority Election value is set to enable, the HA pair launches an election to choose the maximum weighted machine. If the Weighted Priority Election value is set to disable, the HA pair only launches an election when the current active (or primary) machine is not available. (Modifiable)

- **HA Mode**—Active/Passive (Display only)
- **Deployment Mode**—Currently, this parameter always displays **“**Bridge**”** because IWSVA HA clusters are only supported in Transparent Bridge mode. (Display only)

4. Click **Save**.

To change the weight value of a node:

Note: The Weighted Priority Election mode must be set to Enable to perform the following procedure. (To enable the Weight Priority Election mode, see To modify cluster settings: on page 3-19, Step 3.) Roles can be switched manually if the Weighted Priority Election is disabled. See Performing a Manual Switchover on page 3-16 for details.

1. Go to **Administration > IWSVA Configuration > Cluster Management.**
2. In the “Cluster Members” section, click the **weight value** to be changed.
3. In the Weight screen, change the weight value to reflect the appropriate value. (1-255, higher value = higher priority, same value for two nodes can't be saved.)
4. Click **Save**.

   If you change a child member’s weight value to be greater than the parent member’s weight value, and the Weighted Priority Election has been enabled, roles for the two members will be switched.

Chapter 4

Updates

Because new malicious programs and offensive Web sites are developed and launched daily, it is imperative to keep your software updated with the latest pattern files and engines, as listed on the **Updates > Manually** screen on the InterScan Web Security Virtual Appliance (IWSVA) Web console.

Topics in this chapter include the following:

Product Maintenance

From time to time, Trend Micro might release a patch for a reported known issue or an upgrade that applies to your product. To find out whether there are any patches available, visit the following URL:

`http://downloadcenter.trendmicro.com`

Clicking the link for IWSVA takes you to the Update Center page for IWSVA.

Enter the following search criteria:

- **Category:** Internet Gateway
- **Product:** InterScan Web Security Virtual Appliance
- **Version:** Current product version

Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the upgrade instructions in the readme.

Renewing Your Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If your Maintenance Agreement expires, scanning is still possible, but virus pattern and program updates stop. To prevent this, renew the Maintenance Agreement as soon as possible.

To purchase renewal maintenance, contact the same vendor from whom you purchased the product. A Maintenance Agreement, extending your protection for a year, is sent by post to the primary company contact listed in your company's Registration Profile.

To view or modify your company's Registration Profile, log into the account at the Trend Micro online registration Web site:

`https://olr.trendmicro.com/registration`

To view your Registration Profile, type the Logon ID and Password created when you first registered your product with Trend Micro (as a new customer), and click **Login**.

About ActiveUpdate

ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of the latest pattern files and engines.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. Updates are available on a regularly scheduled interval that you configure, or on demand.

Updating From the IWSVA Web Console

If you are not using Trend Micro Control Manager for centralized administration of your Trend Micro products, IWSVA polls the ActiveUpdate server directly. Updated components are deployed to IWSVA on a schedule you define, such as the following:

- Minutes (15, 30, 45, 60)

  These 15-minute interval updates only apply to the following patterns: Virus, spyware/grayware, bot, IntelliTrap, IntelliTrap Exception, Smart Scan Agent, Script Analyzer, and Protocol Information Extraction.
- Hourly
- Daily
- Weekly
- On demand (manually)

Note: Trend Micro recommends hourly updates of the pattern files and daily or weekly updates of engines. All updates include the following patterns: Virus, spyware/grayware, bot, IntelliTrap, IntelliTrap Exception, Smart Scan Agent, Script Analyzer, and Protocol Information Extraction.

Proxy Settings for Updates

If you use a proxy server to access the Internet, you must enter the proxy server information into the IWSVA Web console before attempting to update components. Any proxy information that you enter is used for the following:

- Updating components from Trend Micro's update servers
- Product registration and licensing
- Web reputation queries

To configure a proxy server for component and license updates:

1. Open the IWSVA Web console and click **Updates > Connection Settings**.
2. Select "**Use a proxy server for pattern, engine, license updates and Web Reputation queries**" to specify a proxy server or port. IWSVA supports both the IPv4 and IPv6 AU servers. The Update Proxy also supports the IPv6 proxy, or the IPv4 proxy by hostname or IPv4/IPv6 address.
3. If your proxy server requires authentication, type a user ID and password in the fields provided.

   Leave these fields blank if your proxy server does not require you to authenticate.
4. In the **Pattern File Setting** section, type the number of pattern files to keep on the IWSVA device after updating to a new pattern (default and recommended setting is three pattern files).

   Keeping old pattern files on your server allows you to roll back to a previous pattern file in the event of an incompatibility with your environment; such as excessive false positives. When the number of pattern files on the server exceeds your configuration, the oldest pattern file is automatically deleted.
5. Click **Save**.

Note: In transparent bridge mode, the IWSVA has an internal interface and an external interface. To ensure updates function properly, the configuration of the ActiveUpdate proxy and server settings must be done on the same side. If IWSVA is deployed with other proxy servers, the next hop proxy settings for the ActiveUpdate proxy and server should be the same server on the same side of the interface.

Updatable Program Components

To ensure up-to-date protection against the latest risks, there are several components you can update:

- **Pattern files and signatures**—These include the following patterns: Virus, spyware/grayware, bot, IntelliTrap, IntelliTrap Exception, Smart Scan Agent, Script Analyzer, and Protocol Information Extraction.. These files contain the binary "signatures" or patterns of known security risks. When used in conjunction with the scan engine, IWSVA is able to detect known risks as they pass through the Internet gateway. New virus pattern files are typically released at the rate of several per week, while the grayware/spyware pattern files are updated less frequently.
- **Protocol Information Extraction Pattern**—This file is used by application control and bandwidth control modules to update protocol or add a new application support.

  The Pattern file is stored in the following directory:

  /etc/iscan/libtmprotocols.so.########
- **Virus scan engine**—This module analyzes each file's binary patterns and compares them against the binary information in the pattern files. If there is a match, the file is determined to be malicious.
- **URL Filtering Engine**—IWSVA utilizes the Trend Micro URL Filtering Engine to perform URL categorization and reputation rating based on the URL data supplied from the cloud-based Smart Protection Network. Trend Micro recommends using the default setting of a weekly update check to ensure that your installation has the most current URL Filtering Engine.
- **Advance Threat Scan Engine (ATSE)**—ATSE is a new and innovative scan engine from Trend Micro with the latest heuristic rules to detect a wide range of less common risks, including document exploits, which are commonly used by attackers to exploit the document vulnerabilities to infect victims.

Virus Pattern File

The Trend Micro scan engine uses an external data file, called the virus pattern file, to keep current with the latest viruses and other Internet risks such as Trojans, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly pernicious risk is discovered.

All Trend Micro antivirus programs using the ActiveUpdate feature (see About ActiveUpdate starting on page 4-3 for details) can detect whenever a new virus pattern is available at the server, and can be scheduled to automatically poll the server every hour, day, week, and so on, to get the latest file. Virus pattern files can also be manually downloaded from the following Web site:

`http://www.trendmicro.com/download/pattern.asp`

There, you can find the current version, release date, and a list of the new virus definitions included in the file.

How it Works

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Because each virus contains a unique binary "signature" or string of tell-tale characters that distinguishes it from any other code, the virus experts at TrendLabs capture inert snippets of this code to include in the pattern file. The engine then compares certain parts of each scanned file to the data in the virus pattern file looking for a match.

Pattern files use the following naming format:

`lpt$vpn.###`

where ### represents the pattern version (for example, 400). To distinguish a given pattern file with the same pattern version and a different build number, and to accommodate pattern versions greater than 999, the IWSVA Web console displays the following format:

`roll number.pattern version.build number (format: xxxxx.###.xx)`

- `roll number`—This represents the number of rounds when the pattern version exceeds 999 and could be up to five digits.
- `pattern version`—This is the same as the pattern extension of `lpt$vpn.###` and contains three digits.
- `build number`—This represents the patch or special release number and contains two digits.

If multiple pattern files exist in the same directory, only the one with the highest number is used. Trend Micro publishes new virus pattern files on a regular basis (typically several times per week), and recommends configuring a hourly automatic update on the **Updates > Schedule** screen. Updates are available to all Trend Micro customers with valid maintenance contracts.

Note: There is no need to delete the old pattern file or take any special steps to "install" the new one.

Spyware/Grayware Pattern File

As new hidden programs (grayware) that secretly collect confidential information are written, released into the public, and discovered, Trend Micro collects their tell-tale signatures and incorporates the information into the spyware/grayware pattern file. The spyware/grayware pattern file is stored in the following directory:

```
/etc/iscan/ssaptn.###
```

where `###` represents the pattern version. This format distinguishes a given pattern file with the same pattern version and a different build number. It also accommodates pattern versions greater than 999. The IWSVA Web console displays the following format:

```
roll number.pattern version.build number (format: xxxxx.###.xx)
```

- `roll number`—This represents the number of rounds when the pattern version exceeded 999 and could be up to five digits.
- `pattern version`—This is the same as the pattern extension of `ssaptn.###` and contains three digits.
- `build number`—This represents the patch or special release number and contains two digits.

Bot Pattern File

A botnet refers to a collection of compromised machines running programs (usually referred to as worms, Trojan horses, or backdoors) under a common command and control infrastructure. Trend Micro collects botnet URLs and incorporates them into the Bot pattern file. The Bot pattern file contains an encrypted list of known botnet URLs and is saved in the following directory:

```
/etc/iscan/re###.ptn
```

IntelliTrap Pattern and IntelliTrap Exception Pattern Files

IntelliTrap detection uses a scan option in the Trend Micro's virus scanning engine with IntelliTrap pattern (for potentially malicious files) and IntelliTrap Exception pattern (as an allowed list). IWSVA uses the IntelliTrap option and patterns available for detecting malicious compressed files, such as bots in compressed files. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides a heuristic evaluation of compressed files to help reduce the risk that a bot or any other malicious compressed file might cause to a network.

Smart Scan Agent pattern

Smart Scan Agent pattern is used by the smart scan to perform local pattern match for accessed sample. If the sample is hit by local pattern, it will not query the sample hash from local cache or global smart scan server.

The smart scan agent pattern file is stored in the following directory:

```
/etc/iscan/icrc$oth.###
```

Script Analysis (SA) pattern

SA pattern is used by the script analysis module to analysis malicious script.

Pattern files use the following naming format:

```
ssaptn.###
```

Protocol Information Extraction Pattern

Protocol Information Extraction Pattern is used by application control and bandwidth control to identify protocols.

```
/etc/iscan/libtmprotocols.so.###
```

Scan Engine

At the heart of all Trend Micro antivirus products lies a proprietary scan engine. Originally developed in response to the first computer viruses the world had seen, the scan engine today is exceptionally sophisticated. It is capable of detecting Internet worms, mass-mailers, Trojan horse risks, network exploits and other risks, as well as viruses. The scan engine detects the following types of risks:

- "in the wild," or actively circulating
- "in the zoo," or controlled viruses that are not in circulation, but are developed and used for research and "proof of concept"

In addition to having perhaps the longest history in the industry, the Trend Micro scan engine has also proven in tests to be one of the fastest—whether checking a single file, scanning 100,000 files on a desktop machine, or scanning email traffic at the Internet gateway. Rather than scan every byte of every file, the engine and pattern files work together to identify not only tell-tale characteristics of the virus code, but the precise location within a file where the virus would hide. If a virus is detected, it can be removed and the integrity of the file restored.

To help manage disk space, the scan engine includes an automatic clean-up routine for old viruses, spyware, and IntelliTrap pattern files as well as incremental pattern file updates to help minimize bandwidth usage.

In addition, the scan engine is able to decode all major internet encoding formats (including MIME and BinHex). It also recognizes and scans common compression formats, including Zip, Arj, and Cab. Most Trend Micro products also allow administrators to determine how many layers of compression to scan (up to a maximum of 20), for compressed files contained within a compressed file.

About Scan Engine Updates

By storing the most time-sensitive virus information in the virus pattern file, Trend Micro is able to minimize the number of scan engine updates, while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- New scanning and detection technologies have been incorporated into the software
- A new, potentially harmful virus is discovered that cannot be handled by the current engine
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit:

`http://downloadcenter.trendmicro.com/engine.asp`

Web Reputation Database

The Web Reputation database resides in the cloud with rest of the Trend Smart Protection Network servers. When a user attempts to access a URL, IWSVA retrieves information about this URL from the Web Reputation database and stores it in the local cache. Having the Web Reputation database in the cloud and building the local cache with this database information reduces the overhead on IWSVA and improves performance.

The following are the information types the Web Reputation database can retrieve for a requested URL:

- Web category
- Pharming and phishing flags used by anti-pharming and anti-phishing detection
- Web Reputation scores used to block URL access, based on a specified sensitivity level (see Specifying Web Reputation Rules on page 9-44)

The Web Reputation database is updated with the latest categorization of Web pages.

If you believe the reputation of a URL is misclassified or you want to know the reputation of a URL, please use the link below to notify Trend Micro:

`http://global.sitesafety.trendmicro.com/`

Incremental Updates of the Pattern Files and Engines

ActiveUpdate supports incremental updates of the latest pattern and engine files. Rather than downloading the entire file each time, ActiveUpdate can download only the portion of the file that is new and append it to the existing file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software, deploy pattern, and engine files throughout your environment.

Component Version Information

To know which pattern file or scan engine build you are running, click **Updates** > **Manual** on the main menu. The version in use is displayed in the Current Version column on the **Manual Update** screen.

Manual Updates

The effectiveness of IWSVA depends upon using the latest pattern and engine files. Signature-based virus and spyware/grayware scanning works by comparing the binary patterns of scanned files against binary patterns of known risks in the pattern files. Trend Micro frequently releases new versions of the virus pattern and spyware pattern in response to newly identified risks. Similarly, new versions of the Phish pattern are released as new phishing URLs are identified.

New versions of the Trend Micro scan engine are updated as performance is improved and features added to address new risks.

Note: If Internet connections on your network pass through a proxy server, you need to configure your proxy information. Click **Updates > Connection Settings** from the main menu and enter your proxy server information.

To update the engines and pattern files:

1. Click **Updates > Manual**.
2. For all of the components listed on the Manual Update screen, click one of the following:
   - **Update All**—Updates all components
   - **Update**—Updates only the selected component

If IWSVA is already using the latest version of the component and no update is available, no component is updated. Forcing an update (by clicking **Update**) is not necessary unless the components on the IWSVA device are corrupt or unusable.

Forced Manual Updates

IWSVA provides an option to force an update to the pattern file and the scan engine when the version on IWSVA is greater than or equal to its counterpart on the remote download server (normally IWSVA would report that no updates are available). This feature is useful when a pattern file or scan engine is corrupt and you need to download the component again from the update server.

To force an update of a pattern file or scan engine:

1. Click **Updates > Manual** on the main menu to display the Manual Update screen.
2. For all of the components listed, click **Update** to update only the selected component(s)

   A message box appears if the version of the pattern file or scan engine on IWSVA is greater than or equal to the counterpart on the remote download server. If the pattern file on IWSVA is older than the one on the remote download server, the newer pattern file is downloaded.
3. Click **OK** in the message box to start the forced update.

Scheduled Updates

IWSVA can perform scheduled updates for the following pattern files:

- Virus (includes Trojan and worm signatures)
- Spyware/Grayware
- Bot
- IntelliTrap
- IntelliTrap Exception
- Smart Scan Agent
- Script Analyzer
- Protocol Information Extraction

Likewise, IWSVA can perform scheduled updates for the Scan and URL Filtering engines.

To schedule automatic pattern file and engine updates:

1. Click **Updates > Schedule** on the main menu.
2. For each type of updatable component, select the update interval.

   The following are your options:

   - Every *x* minutes (pattern files only; select the number of minutes between update interval)
   - Hourly (pattern files only)
   - Daily
   - Weekly (select a day from the drop-down menu; this is the recommended setting for the latest engine updates)

   Note: Scheduled updates for a given component can be disabled by selecting **Manual updates only** in each component section.

3. For each component, select a **Start time** for the update schedule to take effect.
4. Click **Save**.

Note: If your network configuration includes a cache server, Trend Micro recommends that you clear the cache and reboot the cache server after updating the pattern file. This forces all URL requests to be scanned, ensuring better network protection. Consult your cache server documentation for information on how to clear the cache and reboot the server.

Maintaining Updates

Update Notifications

IWSVA can issue notifications to proactively inform an administrator about the status of a pattern or engine update. For more information about configuring update-related notifications, see Enabling Pattern File Updates Notifications starting on page 14-34 and Enabling Notifications for URL Filtering Engine and Scan Engine Updates starting on page 14-39.

Rolling Back an Update

IWSVA checks the program directory and uses the latest pattern file and engine library file to scan inbound/outbound traffic. It can distinguish the latest pattern file by its file extension; for example, `lpt$vpn.401` is newer than `lpt$vpn.400`.

Occasionally, a new pattern file might incorrectly detect a non-infected file as a virus infection (known as a "false positive"). You can revert to the previous pattern file or engine library file.

Note: IWSVA does not support rollback for the URL filtering engine.

To roll back to a previous pattern file or scan engine:

1. Click **Updates > Manual** on the main menu.
2. Select the component to roll back and click **Rollback**.

   A progress bar indicates the rollback progress, and a message screen then displays the outcome of the rollback.

Deleting Old Pattern Files

After updating the pattern file, IWSVA keeps old pattern files (virus, spyware/grayware, bots, IntelliTrap, IntelliTrap Exception, Smart Scan Agent, Script Analyzer, and Protocol Information Extraction) on the server so they are available to accommodate a roll back. The number of pattern files kept on the server is controlled by the "**Number of pattern files to keep"** setting on the **Updates > Connection Settings** page.

If you need to manually delete pattern files, they can be found in the `/etc/iscan/` directory of IWSVA.

Controlled Virus Pattern Releases

There are two release versions of the Trend Micro virus pattern file:

- The Official Pattern Release (OPR) is Trend Micro's latest compilation of patterns for known viruses. It is guaranteed to have passed a series of critical tests to ensure that customers get optimum protection from the latest virus risks. Only OPRs are available when Trend Micro products poll the ActiveUpdate server.
- A Controlled Pattern Release (CPR) is a pre-release version of the Trend Micro virus pattern file. It is a fully tested, manually downloadable pattern file, designed to provide customers with advanced protection against the latest computer viruses and to serve as an emergency patch during a virus risk or outbreak.

Note: After you apply a CPR, incremental updates are not possible. This means that subsequent updates require downloading the entire pattern file rather than just the new patterns, resulting in a slightly longer pattern download time.

In order for IWSVA to access the new pattern file, ensure that it has the same permission and ownership as the previous pattern file.

To apply the latest CPR to IWSVA:

1. Open `http://www.trendmicro.com/download/pattern-cpr-disclaimer.asp` and click **Agree** to signify your agreement with the terms and conditions of using a Trend Micro CPR.
2. Download the CPR to a temporary folder on the IWSVA device. The filename is in the form `lptXXX.zip`.
3. Stop all IWSVA services.
4. Extract the contents of the files that you downloaded to the `/etc/iscan/`directory of IWSVA.
5. Restart all IWSVA services.

Chapter 5

Application Control

InterScan Web Security Virtual Appliance (IWSVA) provides a way to control application usage by protocol and displays useful traffic statistics about inbound and outbound application traffic.

Note: To use the Application Control feature, IWSVA must be deployed in Transparent Bridge Mode, Transparent Bridge Mode-High Availability, or Forward Proxy Modes. For more information, see Transparent Bridge Mode on page 2-3, Transparent Bridge Mode - High Availability on page 2-4, or Forward Proxy Mode on page 2-9.

Topics in this chapter include the following:

- Application Control Overview on page 5-2
- Application Control Policy List on page 5-2

Application Control Overview

Internet-based applications have grown in popularity over the last few years beyond using the browser to surf websites. Even with corporate usage policies, many companies are unable to curb and regulate the use of those applications. Recent findings show that 75% to 80% of corporate users ignore their company's computer usage policies. To avoid significant risk, the Application Control feature provides a security technology that automates the discovery of popular Internet applications and allows administrators to control them by using policies.

IWSVA provides both visibility and control for over 800 application types running across any port, including applications using custom clients (for example, Skype, bitTorrent, P2P) or leveraging Web 2.0 technologies within the browser (for example, social networking, webmail, and streaming media sites).

Note: Application Control is available in Transparent Bridge Mode, Transparent Bridge Mode - High Availability, and Forward Proxy Mode.

Enabling or disabling of the Application Control will not affect policies already created. They will be synchronized between HA nodes and are included in migration packages.

Change actions in Application Control policies and settings are recorded in the Audit Log.

Application Control Policy List

The Application Control feature allows more than a simple allow-or-block option for all examples of applications within a category. This flexibility is provided because many companies have found specific functions of these applications are effective for conducting business. Granular application control allows you to not only block and allow an application like Facebook, for example, but you could also allow the application, and still block newly posted messages.

Administrators may want to allow the two most popular IM applications, but block the rest. For P2P, administrators may want to allow the transfer of files between employees within the corporate network, but prohibit external use.

Creating Application Control policies allows granular control of the functionality within the supported Internet-based application categories.

The Application Control policy list shows all policies on the system (for IPv4 and IPv6 addresses)—enabled as well as disabled. Go to **Application Control > Policies**. Click **Add** to create a new policy, or click a policy name to edit an existing one.

- **Enable Application Control**—Globally controls the enabled status of all policies; overrides the status of an individual policy. Click **Save** after enabling or disabling Application Control. Enabling or disabling of the Application Control will not affect policies already created. They will be synchronized between HA noces and are included in migration packages.
- **Add**—Opens the Add Policy wizard that will take you through the steps of defining a new policy.
- **Priority**—Sets the order of precedence—if two conflicting policies overlap in their scope, the policy with the higher priority (closer to 1) will be applied and the other ignored.

Note: The Application Control Global Policy is the default policy. It automatically applies to all users, but also always takes the lowest priority. Any policy above it in the list will take precedence.

- **Deploy Policies**—Click this button after creating or modifying an Application Control policy to have it immediately take effect. This avoids waiting for the policy deployment interval.
- **Application Search**—Type an application protocol name to search.
- **Granular Action Search**—Select one or more granular actions to search for an application.
- **Action**—Set actions Allow, Block or Match Next Policy for selected applications.
- **Scheduling**—Select scheduled times for current policy by clicking the Choose scheduling drop-down list. For Scheduled Times, refer to **Administration** > **IWSVA Configuration** > **Scheduled Times**.
- **Collapse and expand category**—The Expand icon (⇊) allows you to see the contents of all the application category. The Collapse icon (⇈) allows you to close all application categories.

- **Search**—When creating policies, you can use the search field to find the applications you want to add to your policy rules.

To view Application Control policies:

1. Go to **Application Control > Policies**.
2. Click the name of an existing policy to see the details about that policy.

   The Global Application Control policy is the default policy.
3. To add a policy, see Adding an Application Control Policy on page 5-5.

Add Policies: Select Accounts

IWSVA has default global and guest policies for the following activities: HTTPS decryption, Advanced Thread Protection, HTTP Inspection, Data Loss Prevention, applets and Active X, and URL Filtering. Application Control and Bandwidth Control have only the default global policies.

- **Global Policy**—For all clients who access through IWSVA.
- **Guest Policy**—For those clients, typically temporary workers, contractors, and technicians who proxy through IWSVA using a special guest account.

The Global Application Control policy is the default policy.

- **Enable policy**—Enables or disables the individual policy; the global Application Control setting overrides the specifications of an individual policy.
- **IP Range**—Use to specify the range of IP addresses (IPv4 and/or IPv6) that will be affected by the Application Control policy.
- **IP Address**—Use to specify the single IP address (IPv4 or IPv6) that will be affected by the Application Control policy.
- **IP Subset**—Use to specify the subnet IP address that will be affected by Application control policy.
- **User or Group** (If User Identification is enabled)—Use to specify the user or group that will be affected by Application control policy.

Note: The options on this page depend upon the user identification method that you are using—either IP address or User/group name authentication, if you enable LDAP authentication. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method on page 8-6 and Configuring the Scope of a Policy on page 8-17.

- **Add**—Click to add a single or range of IP addresses to the list of addresses that will be affected by the Application Control policy.

Adding an Application Control Policy

To add an Application Control policy:

1. Go to **Application Control > Policies**.
2. Click the **Add** link at above the policy list.
3. Type a descriptive new policy name. This will help you remember the policy.
4. You can also create a new policy based on the settings of an existing policy by clicking the "Copy from existing policy" option and selecting a policy from the drop-down list.
5. Type a single IP address, a range of IP addresses, an IP subset, or a user/group name to signify the users affected. Alternatively, choose the user or group name if LDAP integration has been set up.
6. Click **Add** to move the newly entered IP address, range, or user/group name to the **Type & Identification** table.
7. Check the **Enable Policy** check box at the top of the screen to enable the policy after it is created.
8. Click **Next** to continue.
9. See Specifying Application Control Policy Rules on page 5-6 to set up the rules of the policy which apply to specified accounts.

Add or Edit Policies: Specify Rules for Application Control Policies

You add or edit policy rules in two locations:

- **Application Control > Policies | Add > Select Account > Specify Rules**
- **Application Control > Policies | Policy Name | Rule** (to edit an existing policy)

Adding an Application Control policy is a two-step procedure. First, create an account to specify the users to which the policy will apply, then assign Application Control rules to the policy.

Note: Use the search field to find a specific application on the Rules page. For more information about an application, click the name of the application to go to a separate page that contains information describing the supported applications, versions and other details.

Specifying Application Control Policy Rules

Editing an Application Control policy requires clicking on the policy name, then clicking the Rule tab.

- **Enable policy**—Enables or disables the individual policy; the global Application Control policy settings override the specifications of an individual policy.
- **Application Category**—Choose an action for the protocols to which you want to restrict access. There are over 1000 categories segmented in 25 logical groups. Use the search field to find specific application names.
    - Click on the "+" sign to expand a category and select specific protocols.
    - Click the protocol name to access a page with descriptions of the protocols.

Note: When you create a policy, current connections will not be blocked by the new policy. For example: If a user is logged on to Skype while an admin creates a policy to block Skype, the user can continue to use Skype. However, once the user logs off, he cannot log back on to Skype again because the policy will be in effect.

Use the following available filtering actions:

- Deny Send Mail
- Deny Upload File
- Deny Download File
- Deny Transfer File

- Deny Post Message
- Deny Video Voice Call
- Deny Play Media

Selecting the “allow”, “block” or “match next policy” action can be supported by all applications, and other actions can be supported by part of the applications; such as **File Transfer**. As a result, the policy setting process is:

- **Option 1**: Filtering Application Search
    - Enter application name at **Application Search** and click **Search** button, then the applications will be filtered out.
    - Select the applications that need actions set.
    - Go to **Action**, select the actions that apply to the selected application.
- **Option 2**: Filtering Granular Action search
    - Select any action from **Granular Action Search** and click **Search** button, then the action-selectable applications will be filtered out.
    - Select more than one action under **Granular Options** from the application action list, and apply it.
- **Allow**—User accounts can use the application normally. Application Control events are recorded if the administrator enables that setting. (See Application Control Settings for details.)
- **Block**—User accounts cannot use this application. The network packets identified as part of this application will not be delivered. Application Control events can be recorded if the settings is enabled. (See Application Control Settings on page 5-8 for details.) A log entry can also be created for this event.
- **Match Next Policy**—Use the next policy settings. This action does not exist in Global and Guest policy.
- **Scheduling**—Select the time object for the protocol for which you want to apply the action. (Restricted days and hours are defined at **Administration > IWSVA Configuration > Schedule Time**.) (See Scheduled Times on page 15-16 for details.) Click **Save** to apply the filtering action to the selected protocols.

Note: Settings will take effect after the HTTP service is reloaded.

- **Note**—Use to create policy notes, for example, to summarize the intent or justification for the policy. It can serve as a simple reminder or as a communication to others who could later administer this feature.
- Click **Save** at the end of the rules list to return to the policy list.
- In the policy list, click **Deploy Policies** when you are ready for the policy/policies to be deployed.

Application Control Settings

Administrators can configure the following setting:

- Enabling Log Application Control events for bandwidth statistic (Default: enabled)
- Setting the logging interval (Default: 300 seconds)

Note: If the Application Control feature is not enabled, no logs are recorded and the Dashboard's Application Bandwidth (**Application Control > Settings**) will not display data.

To configure the Application Control settings:

1. Go to **Application Control > Settings**.
2. Set the following configuration:
   - **Log Application Control events for bandwidth statistic**—Selecting this option allows you to monitor and report all application activity that is allowed by the Application Control polices. (Logging activity is normally turned off by default.)
   - **Logging interval XX seconds**—Changing this option defines when to write to an application log record. For example, the default interval is 300 seconds (five minutes). No matter how many times one client accesses the same application in that five-minute interval, there will be only one log entry.

     A user accessing the Internet using one of the tracked applications may create many sessions in a very short time. In order to prevent a flooding of events into the log database, this option can limit how often one event record is written for the activity. This limitation technique keeps the violation log from becoming too large and affecting performance. Admins may change the logging interval if they want to record to the violation log more frequently or less frequently.

3. Click **Save**.

Chapter 6

Bandwidth Control

This chapter introduces the bandwidth control feature in Trend Micro™ InterScan™ Web Security Virtual Appliance (IWSVA).

Topics in this chapter include the following:

- About Bandwidth Control starting on page 6-2
- Bandwidth Control Policy List starting on page 6-2
- Adding a Bandwidth Control Policy starting on page 6-5
- Specifying the Actual Internet Bandwidth starting on page 6-6

About Bandwidth Control

Peer-to-peer downloading, video streaming and instant message applications consume network bandwidth and can impact productivity. Bandwidth control reduces network congestion by controlling communications, reducing unwanted traffic and allowing critical traffic or services the appropriate bandwidth allocation. Bandwidth control gives all users fair access to resources and ensures better access to resources that are more central to the organization. Similar to policy rules, bandwidth control can limit traffic based on a source IP address, user or group, traffic type or service, and time of day.

Bandwidth control rules can be as general or specific as needed. The bandwidth control rules are compared against the incoming traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same. If the traffic does not match any of the rules, the traffic uses the remaining bandwidth.

Note: The maximum downstream or upstream bandwidth in a bandwidth control policy cannot exceed the actual Internet bandwidth settings.

The total guaranteed downstream or upstream bandwidth in all enabled bandwidth control policies cannot exceed the actual Internet bandwidth settings.

Bandwidth Control Policy List

The Bandwidth Control policy list shows all policies on the system (for IPv4 and IPv6 addresses)—enabled as well as disabled. Go to **Bandwidth Control > Policies**. Click **Add** to create a new policy, or click a policy name to edit an existing one.

- **Enable Bandwidth Control**—Globally controls the enabled status of all policies. Click **Save** after enabling or disabling Bandwidth Control policies.
- **Add**—Opens the Add Policy wizard that will take you through the steps of defining a new policy.
- **Priority**—Sets the order of precedence—if two conflicting policies overlap in their scope, the policy with the higher priority (closer to 1) will be applied and the other ignored.

Note: The Bandwidth Control Global Policy is the default policy. It automatically applies to all users, but also always takes the lowest priority. Any policy above it in the list will take precedence.

- **Deploy Policies**—Click this button after creating or modifying an Bandwidth Control policy to have it immediately take effect. This avoids waiting for the policy deployment interval.

To view Bandwidth Control policies:

1. Go to **Bandwidth Control > Policies**.
2. Click the name of an existing policy to see the details about that policy.

   The Global Bandwidth Control policy is the default policy.

To add a policy, see Adding a Bandwidth Control Policy on page 6-5.

Add Policies: Select Accounts

IWSVA has default global and guest policies for the following activities: HTTPS decryption, Advanced Thread Protection, HTTP Inspection, Data Loss Prevention, applets and Active X, and URL Filtering. Application Control has only the default global policy.

- **Global Policy**—For all clients (except for clients in "Guest Policy") who access through IWSVA.
- **Guest Policy**—For those clients, typically temporary workers, contractors, and technicians who proxy through IWSVA using a special guest account.

The Global Bandwidth Control policy is the default policy.

- **Enable policy**—Enables or disables the individual policy; the global Bandwidth Control setting overrides the specifications of an individual policy.
- **IP Range**—Use to specify the range of IP addresses (IPv4 and/or IPv6) that will be affected by the Bandwidth Control policy.
- **IP Address**—Use to specify the single IP address (IPv4 or IPv6) that will be affected by the Bandwidth Control policy.
- **IP Subset**—Use to specify the subnet IP address that will be affected by Bandwidth Control policy.

- **User or Group** (If User Identification is enabled)—Use to specify the user or group that will be affected by Bandwidth Control policy.

Note: The options on this page depend upon the user identification method that you are using—either IP address or User/group name authentication, if you enable LDAP authentication. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method on page 8-6 and Configuring the Scope of a Policy on page 8-17.

- **Add**—Click to add a single or range of IP addresses, user, or group to the list of addresses that will be affected by the Bandwidth Control policy.

Add Policies: Specify Rules

Editing a Bandwidth Control policy requires clicking on the policy name, then clicking the Rule tab.

- **Enable policy**—Enables or disables the individual policy; the global Bandwidth Control policy settings override the specifications of an individual policy when adding a new policy.
- **Application Category**—Choose an action for the protocols to which you want to restrict access. Use the search field to find specific application names.
  - Click on the “+” sign to expand a category and select specific protocols.
  - Click the protocol name to access a page with descriptions of the protocols.

Note: When you create a policy, current connections will not be controlled by the new policy. For example: If a user is logged on to Skype while an administrator creates a policy to control bandwidth usage for Skype, the user can continue to use Skype. However, once the user logs off and logs back on to Skype again, the bandwidth control policy will be in effect.

- **Action**—Select an action (**Control** or **No Control**) to apply on the selected protocol.

- **Schedule**—Select the time object for the protocol for which you want to apply the action. (Restricted days and hours are defined at **Administration > IWSVA Configuration > Schedule Time**.) (See Scheduled Times on page 15-16 for details.)

Note: Settings will take effect after the HTTP service is reloaded.

- **Bandwidth Throttle**—Configure bandwidth limits and service priority in this section.
- **Note**—Use to create policy notes, for example, to summarize the intent or justification for the policy. It can serve as a simple reminder or as a communication to others who could later administer this feature.
- Click **Save** at the end of the rules list to return to the policy list. In the policy list, click **Deploy Policies** when you are ready for the policy/policies to be deployed.

Adding a Bandwidth Control Policy

Note: Bandwidth Control is only supported in proxy mode.

Configure bandwidth control settings (**Bandwidth Control > Settings**) before you create bandwidth control policies. For more information, see Specifying the Actual Internet Bandwidth on page 6-6.

To add a bandwidth control policy:

1. Go to **Bandwidth Control > Policies**.
2. Click the **Add** link at above the policy list.
3. Type a descriptive new policy name. This will help you remember the policy.
4. You can also create a new policy based on the settings of an existing policy by clicking the “Copy from existing policy” option and selecting a policy from the drop-down list.
5. Type a single IP address, a range of IP addresses or an IP subset to signify the users affected. Alternatively, choose the user or group name if LDAP integration has been set up successfully.

6. Click **Add** to move the newly entered IP address, range, subnet, or user/group name to the Type & Identification table.
7. Click **Next** to continue.
8. In the **Rule** tab, choose an action (**No Control** or **Control**) for the application to which you want to control bandwidth.

   Use the search field to find specific application names.

   - Click on the "+" sign to expand a category and select specific applications.
   - Click the application name to access a page with descriptions of the applications.

   Note: When you create a policy, current connections will not be controlled by the new policy. For example: If a user is logged on to Skype while an administrator creates a policy to control bandwidth usage for Skype, the user can continue to use Skype. However, once the user logs off and logs back on to Skype again, the bandwidth control policy will be in effect.

9. Select an option from the **Schedule** drop-down list.
10. Configure bandwidth limits and service priority in the **Bandwidth Throttle** section.
11. Click **Save** to save the rule configuration and return to the policy list.
12. In the policy list, click **Deploy Policies** when you are ready for the policy/policies to be deployed.

Specifying the Actual Internet Bandwidth

Administrators can configure the actual upstream and downstream Internet bandwidth.

Note: If the Bandwidth Control feature is not enabled, no logs are recorded and the Dashboard's Bandwidth Control widgets will not display data.

To specify the actual Internet bandwidth:

1. Go to **Bandwidth Control > Settings**.
2. Set the **Upstream Bandwidth** and **Downstream Bandwidth**.

3. Click **Save**.

Note: The maximum downstream or upstream bandwidth in a bandwidth control policy cannot exceed the actual Internet bandwidth settings.

The total guaranteed downstream or upstream bandwidth in all enabled bandwidth control policies cannot exceed the actual Internet bandwidth settings.

Chapter 7

HTTP Configuration

Before you start using InterScan Web Security Virtual Appliance (IWSVA) to scan for malicious HTTP/HTTPS downloads, filter or block URLs, and apply access quotas for your clients, you need to configure some HTTP settings that control the HTTP traffic flow. IWSVA can be used in conjunction with another proxy server on your network; alternatively, you can configure IWSVA to use its native proxy.

Note: - To enable and configure WCCP, see Network Configuration and Load Handling on page 7-12 and your Cisco product documentation.
- To enable and configure Full Transparency (Transparent Bridge mode), see Network Configuration and Load Handling on page 7-12.

Topics in this chapter include the following:

Enabling the HTTP/HTTPS Traffic Flow

The deployment mode is originally configured with the IWSVA Deployment Wizard. If you would like to change the deployment mode after the installation, you can use the **Administration > Deployment Wizard** to make the changes.

To enable or disable the HTTP/HTTPS traffic flow through IWSVA:

1. Select **System Status** on the main menu.
2. Select one of the following:
   - If HTTP(S) traffic is turned off, click the **Turn On** link to enable it.
   - If HTTP(S) traffic is turned on, click the **Turn Off** link to disable it.

When HTTP/HTTPS traffic is turned off, your clients cannot access Web sites or any other services carried through HTTP/HTTPS.

Specifying a Proxy Configuration and Related Settings

If you would like to change the deployment mode after the installation, you can use the **Administration > Deployment Wizard** to make changes.

- **Transparent Bridge Mode**—IWSVA acts as a Layer 2 network bridge between the devices it is deployed between and transparently scans HTTP, HTTPS, and FTP traffic between the clients and external services. No configuration changes to the network devices are required. Transparent bridge settings apply to both HTTP and FTP traffic, and if selected, FTP proxy settings are disabled. By default, SSL (HTTPS) traffic is passed through IWSVA, but not scanned. To allow IWSVA to scan SSL-encrypted traffic, you can configure HTTPS decryption policies to decrypt the content before scanning.

  If the clients and IWSVA are in the same segment, no configuration is required. Otherwise, see the following list for mixed segment configuration considerations.

  If the network device and IWSVA device are on different network segments, use the IWSVA routing table to point IWSVA to the device. Requires two NICs.
- **Transparent Bridge Mode - High Availability** — Requires a minimum of four NICs.

- **Forward Proxy Mode**—This configuration is used to protect clients from receiving malicious HTTP/HTTPS/FTP-borne risks from a server. This is the most common configuration, and the typical use case is to protect Web users on your network from receiving malicious Internet downloads. IWSVA and the clients that it protects are typically in the same LAN.
- **Reverse Proxy Mode**—This configuration is used to protect Web servers from attacks or malware introduced by public or private users.
- **ICAP Mode**—Choose this topology if you have an ICAP client on the network and you want it to pass traffic to IWSVA for scanning. IWSVA acts as an ICAP server.
- **Simple Transparency Mode**—An L4 switch is set up to direct HTTP/FTP traffic to IWSVA. IPv6 support is not available with this option.
- **WCCP Mode**—The WCCP configuration allows customers that have WCCP enabled routers and switches to redirect Web and FTP traffic to IWSVA to create a high-performance scalable and redundant architecture.

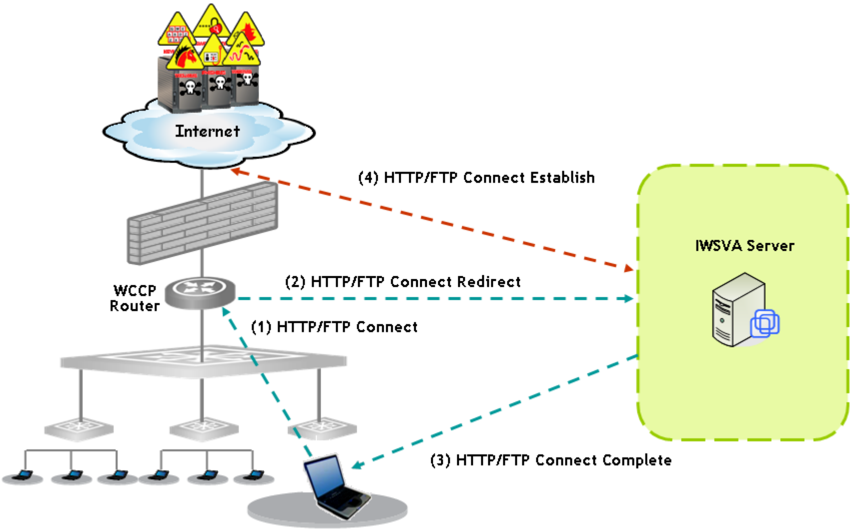

Internet
(4) HTTP/FTP Connect Establish
IWSVA Server
WCCP Router
(2) HTTP/FTP Connect Redirect
(1) HTTP/FTP Connect
(3) HTTP/FTP Connect Complete

FIGURE 7-1. WCCP configuration and Web and FTP traffic

Proxy Configurations

There are several types of proxy configurations:

- No upstream proxy (stand-alone mode)
- Upstream proxy (dependent mode)
- Simple transparency
- Reverse proxy
- ICAP
- WCCP

No Upstream Proxy (Stand-alone Mode)

The simplest configuration is to install IWSVA in stand-alone mode, with no upstream proxy. In this case, IWSVA acts as a proxy server for the clients. The advantages of this configuration are its relative simplicity and that there is no need for a separate proxy server. A drawback of a forward proxy in stand-alone mode is that each client must configure the IWSVA device as their proxy server in their browser's Internet connection settings. This requires cooperation from your network users, and also makes it possible for users to exempt themselves from your organization's security policies by reconfiguring their Internet connection settings.

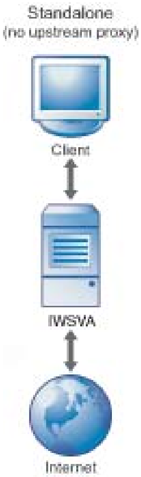


FIGURE 7-2. Forward, no upstream proxy

Note: If you configure IWSVA to work in stand-alone mode, each client on your network needs to configure Internet connection settings to use the IWSVA device and port (default 8080) as their proxy server.

To configure a stand-alone installation:

1. Click **Administration > Deployment Wizard** from the main menu.

   The Deployment Wizard displays.
2. Ensure that **Forward proxy mode** is selected. Click **Next**.
3. Verify that **Enable upstream proxy** is not selected.
4. Click **Next** until the Submit button displays. Click **Submit.** Click **Close**.

Upstream Proxy (Dependent Mode)

IWSVA can be configured to work in conjunction with another proxy server on your network. In this configuration, IWSVA passes requests from clients to another proxy server, which forwards the requests to the requested server.

Like the stand-alone mode, the dependent mode proxy configuration also requires client users to configure the IWSVA device as their proxy server in their Internet connection settings. One benefit of using an upstream proxy is improved performance through content caching on the upstream proxy server. IWSVA only performs content caching in forward proxy mode (if enabled.) When enabled, IWSVA performs content caching, or if another cache server is available, it could be configured for content caching. For other modes or if content caching is not enabled in Forward Proxy mode, every client request needs to contact the Internet server to retrieve the content. When using an upstream proxy, pages cached on the proxy server are served more quickly.

Note: If IWSVA is configured to operate in upstream proxy mode with a designated proxy server, Trend Micro recommends that the proxy settings for Updates also be configured to the same designated proxy server (see Proxy Settings for Updates on page 4-4). Certain types of update events utilize the Updates proxy settings to retrieve important information. If proxy settings are not configured properly, IWSVA will not be able to access the Internet for these services.

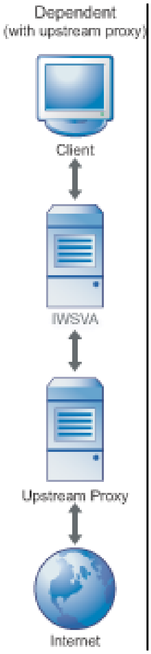


FIGURE 7-3. Forward, upstream proxy

Note: When IWSVA is configured in HTTP Forward Proxy mode with Upstream Proxy enabled, pharming sites cannot be effectively blocked.

When you configure IWSVA to work in Forward Proxy mode and enable Upstream Proxy, the approved server IP list configuration file will not take effect. Content from servers that you configure in the file still will be scanned or filtered.

To configure IWSVA to work with an upstream proxy:

1. Click **Administration > Deployment Wizard** from the main menu.

   The Deployment Wizard displays.
2. Ensure that **Forward proxy mode** is selected. Click **Next**.
3. Check **Enable upstream proxy** and enter the IP address or host name of the upstream **Proxy server**, and the **Port number**.
4. Click **Next** until the Submit button displays. Click **Submit.** Click **Close**.

Transparent Proxy

Transparency is the functionality whereby client users do not need to change their Internet connection's proxy settings to work in conjunction with IWSVA. Transparency is accomplished with a Layer 4 switch that redirects HTTP packets to a proxy server, which then forwards the packets to the requested server.

IWSVA supports a "simple" type transparency. Simple transparency is supported by most Layer 4 switches. While it is compatible with a wide variety of network hardware from different manufacturers, configuring simple transparency does impose several limitations:

- When using simple transparency, the User Identification method to define policies is limited to IP address and/or host name; configuring policies based on LDAP is not possible.
- FTP over HTTP is not available; thus, links to ftp:// URLs might not work if your firewall settings do not allow FTP connections. Alternatively, links to ftp:// URLs might work, but the files are not scanned.
- Simple transparency is not compatible with some older Web browsers when their HTTP requests do not include information about the host.
- Do not use any source NAT (IP masquerade) downstream of IWSVA, because IWSVA uses the IP address of the client to scan and clean the malicious traffic.

The benefit of enabling transparency is that the clients' HTTP requests can be processed and scanned by IWSVA without any client configuration changes. This is more convenient for your end users, and prevents clients from exempting themselves from security policies by simply changing their Internet connection settings.

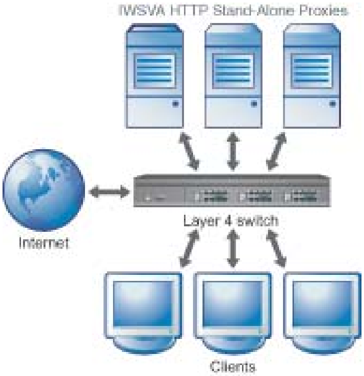


FIGURE 7-4. Forward proxy with transparency

Note: In simple transparency mode, IWSVA does not accept SSL (HTTPS) traffic. Configure the router not to redirect port 443 traffic to IWSVA.

If you configure IWSVA in simple transparency mode and the IWSVA server is connected to a layer-4 switch, you should set the HTTP listening port to 80 and enable PING on the data interface to allow users to access the Internet through IWSVA.

IWSVA does not support HTTPS decryption in simple transparency mode.

IPv6 is not supported in this deployment mode.

To configure simple transparency:

1. Click **Administration > Deployment Wizard** from the main menu.

   The Deployment Wizard displays.

2. Check **Simple Transparency mode** and click **Next**.

3. Change the **HTTP Listening port** to the same port that the Layer 4 switch is configured to use.
4. Click **Next** until the Submit button displays. Click **Submit.** Click **Close**.

Reverse Proxy

IWSVA can be used to scan content that clients upload to a Web server. When IWSVA is installed using either the forward or reverse proxy scan configuration, traffic in both directions is scanned (uploading and downloading).

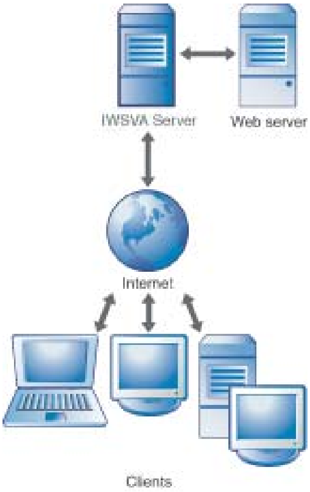


FIGURE 7-5. Reverse proxy protects Web server from clients

To configure IWSVA as a reverse proxy:

1. Click **Administration > Deployment Wizard** from the main menu.

   The Deployment Wizard displays.
2. Select **Reverse proxy** mode and click **Next**.
3. Enter the **HTTP Listening Port** number, the IP address and port number of the **Protected server.**
4. Check **Enable SSL Port**, if needed, type your **SSL Port number**, upload your certificate and private key, and then type your matching passphrase.

5. Click **Next** until the Submit button displays. Click **Submit.** Click **Close**.

Note: If you check **Enable SSL Port** in the Deployment Wizard, clients can communicate with IWSVA using SSL, but IWSVA communication with your internal web servers will not use SSL.

Note: In reverse proxy mode, HTTPS decryption is not supported. The DLP feature is not supported in this mode.

Proxy-related Settings

In addition to specifying the type of proxy configuration you want, you can also set the following parameters for the configuration:

- HTTP listening port
- Anonymous FTP logon over HTTP email address

HTTP Listening Port

If you enable HTTP scanning, be sure to specify the appropriate listening port number of a given HTTP handler so the traffic will go through.

Note: It is not necessary to configure an HTTP Listening Port in Transparent Bridge mode.

To configure the listening port number:

1. Open the IWSVA Web console and click **Administration > Deployment Wizard.**
2. Select your mode and click **Next**.
3. In the **HTTP Listening port** text box, type the port number (default values are 1344 for ICAP and 8080 for HTTP Proxy).
4. Click **Save**.

Note: IWSVA handles HTTPS connections differently from HTTP connections. Because the data is encrypted, you can configure HTTPS decryption policies to decrypt the content which can then traverse filtering and scanning policies as "normal" HTTP traffic. IWSVA examines the initial CONNECT request, and rejects it if it does not match the set parameters (such as the target URL is on the Block List or contained in the Phish pattern file, or the port number used is not defined in the `HttpsConnectACL.ini` file).

Anonymous FTP Logon Over HTTP Email Address

FTP over HTTP enables users to access hyper links to ftp:// URLs in Web pages and enter a URL starting with ftp:// in the address bar of their browser. If the user omits the user name when accessing this type of URL, anonymous login is used, and the user's email address is conventionally used as a password string that is passed to the FTP server.

To configure the email address to use for anonymous FTP logon over HTTP:

1. Select **Administration > Deployment Wizard** from the main menu.
2. Select **Simple Transparency mode.**
3. Type the **Email address to use** for an anonymous FTP log on.
4. Click **Save**.

Network Configuration and Load Handling

The number of users supported by each IWSVA instance depends on the hardware where IWSVA is installed, the average number of concurrent sessions used per user, the bandwidth used by each users' sessions, and the percentage of the user population that is using the Internet simultaneously. In general, the more powerful the IWSVA server platform, the larger IWSVA's capacity will be.

Note: For more information on capacity sizing, refer to the IWSVA Sizing Guide.

You can install IWSVA on the network in the following modes:

- **Transparent Bridge**—Run a cable from the external (Internet-facing) network device to an IWSVA external port, and from an IWSVA internal port, to an internal network device.
- **Forward Proxy**—Run a cable from the interface configured in the CLI to the internal network device.
- **ICAP**—Connect IWSVA to the ICAP client using the interface configured in the CLI.
- **WCCP**—Trend Micro recommends using the following Cisco IOS versions when configuring WCCP with IWSVA:
  - 12.2(0) to 12.2(22). Avoid using releases 23 and above within the 12.2 family
  - 12.3(10) and above. Avoid using releases 0-9 in the 12.3 family
  - IOS 12.4(15)T3 or later should be used

After setting up the IWSVA server, open the IWSVA Web console and click **Administration > Deployment Wizard** to set the corresponding IWSVA scan mode.

Configuring Internet Access Control Settings

IWSVA includes several configurations to control your clients' HTTP/HTTPS access. These settings are separate from any scanning or URL filtering policies that you might configure for your user base.

- HTTP access can be selectively enabled for client users with a given IP address, IP range, or IP mask.
- To improve performance when client users request content from "trusted" sites, scanning can be disabled for servers with a given IP address, or servers within a given IP range or IP mask.
- HTTP and HTTPS requests to ports or port ranges can be selectively allowed or denied for all users whose Internet access passes through IWSVA. This feature is convenient if you want to prevent certain types of Internet transfers.

Identifying Clients and Servers

For controlling client Web access or configuring servers as trusted, there are three ways to identify the client or server:

- IP address: a single IP address, for example, 123.123.123.12

- IP range: clients that fall within a contiguous range of IP addresses, for example, from 123.123.123.12 to 123.123.123.15
- IP mask: a single client within a specified subnet, for example, entering IP = 192.168.0.1 and Mask = 255.255.255.0 identifies all machines in the 192.168.0.x subnet. Alternatively, the Mask can be specified as a number of bits (0 to 32)

Client IP

In addition to the default setting that allows all clients on your network to access the IWSVA proxy, IWSVA can be configured to allow HTTP access only to those clients that you explicitly specify. If your organization does not allow everyone on your network to access the Internet, this is a convenient way to block HTTP access by default.

Client Access Control supports both IPv4 and IPv6 clients. When selecting policies, both IPv4 and IPv6 policies will appear. Client Access Control accepts a single IPv6 address, an IPv6 range, or an IPv6 mask similar to what has been supported with IPv4.

To allow HTTP access based on client IP:

1. Select **HTTP > Configuration > Access Control Settings** from the main menu.

   In transparent bridge mode, the destination and HTTPS ports are not available; therefore, when in this mode the **Destination Ports** and **HTTPS Ports** tabs are not present in the **Internet Access Control** screen.
2. Ensure that the **Client IP** tab is active.
3. Check **Enable HTTP Access Based On Client IP**.
4. Select the option that describes how clients are allowed HTTP access—either **IP Address**, **IP range**, or **IP Subset**.

   Note: If you specify a single IP address and then an IP address range containing the single IP address, the IP address range is negated if a user attempts to access a URL at the single IP address.

   For more information about identifying the clients, see Identifying Clients and Servers starting on page 7-13.

   To delete a client IP or IP range, click the corresponding **Delete** icon next to it.
5. Type a descriptive name in the **Description** field. (40 characters maximum)

6. Click **Add**.

   The client IP that you have configured is added to the list at the bottom of the **Client IP** tab. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Client IP** tab.

7. Click **Save**.

Approved Server IP List

To maximize the performance of your network, you can configure IWSVA to skip scanning and filtering content from specific servers. For example, if you are protecting your intranet server with IWSVA in a reverse proxy configuration, you can be reasonably assured that its content is safe and you might want to consider adding your intranet servers to the approved server IP list.

After configuring the IP addresses or ranges of trusted servers, the configurations are saved to the approved server IP list configuration file.

WARNING! **Content from servers that you configure in this configuration file is not scanned or filtered. Trend Micro recommends adding only those servers over which you have close control of the contents.**

In ICAP mode, the approved server IP list is only applied to RESPMOD requests. REQMOD activities (such as URL filtering, Webmail upload scanning, and URL blocking) cannot be bypassed by the approved server IP list for ICAP installations.

Server Access Control supports both IPv4 and IPv6 clients. When selecting policies, both IPv4 and IPv6 policies will appear. Server Access Control accepts a single IPv6 address, an IPv6 range, or an IPv6 mask similar to what has been supported with IPv4.

To add servers to the Approved Server IP List:

1. Select **HTTP > Configuration > Access Control Settings** from the main menu.
2. Ensure that **Approved Server IP List** tab is active.
3. Check the way you want to specify trusted servers whose content is not scanned or filtered—either **IP**, **IP range**, or **IP Subset**.

   For more information about identifying the clients, see Identifying Clients and Servers starting on page 7-13.

4. Type a descriptive name in the **Description** field. (40 characters maximum)
5. Click **Add**.

   The trusted servers that you have configured appears at the bottom of the **Approved Server IP List** tab.

   To delete a trusted server, range, or IP subset, click the corresponding **Delete** icon next to it.
6. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Approved Server IP List** tab.
7. Click **Save**.

Destination Port Restrictions

IWSVA can restrict the destination server ports to which clients can connect. HTTP requests to a denied port are not forwarded. This approach can lock down your server and prevent clients from using services such as streaming media applications that contravene your network's security policies by denying access to the ports used by these services.

The default post-install configuration is to deny all requests, except for those to ports 80 (HTTP), 70 (Gopher), 210 (TCP), 21 (FTP), 443 (SSL), 563 (NNTPS) and 1025 to 65535.

Note: To enable FTP over HTTP connections for clients to open FTP links in Web pages, IWSVA must be able to open a command connection to the FTP server on port 21. This requires allowing access to port 21 on the HTTP access control settings.

For a list of ports used by various applications and services, see `http://www.iana.org/assignments/port-numbers`.

To restrict the destination ports to which a client can connect:

1. Select **HTTP > Configuration > Access Control Settings** from the main menu.
2. Ensure that the **Destination Ports** tab is activated.
3. Choose the **Action** to perform. Choose **Deny** to prevent connections to a specific port or port range on a destination server, or **Allow** to permit connections to a specific port or port range.

4. Check either **Port** or **Port Range** and then enter the corresponding port(s).
5. Type a descriptive name in the **Description** field. (40 characters maximum)
6. Click **Add**. The destination port restrictions are added to the list at the bottom of the **Destination Ports** tab.

   To delete a destination port or port range to which you allow or deny access, click the **Delete** icon next to it.
7. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Destination Ports** tab.

   To change the order that ports appear in the list, click the up or down arrows in the **Evaluation Order** column.
8. Click **Save**.

HTTPS Ports

IWSVA can restrict which ports can be used for encrypted HTTP transactions. The default configuration is to allow only HTTPS connections on port 443 (the default HTTPS port), 563 (the default port for encrypted news groups), 8443(IWSVA secure console default port), and 1814 (the port for Captive Portal page used by Tomcat).

Note: If you need to access the Web console through HTTPS while connecting through IWSVA itself, allow access to the IWSVA secure console port number (8443 by default).

To restrict the ports that can be used to tunnel encrypted HTTP transactions:

1. Select **HTTP > Configuration > Access Control Settings** from the main menu.
2. Make the **HTTPS Ports** tab active.
3. Choose to either **Deny** or **Allow** the **HTTPS Ports.**
4. Check either **Port** or **Port Range** and then enter the corresponding port(s).
5. Type a descriptive name in the **Description** field (40 characters maximum.)
6. Click **Add**. The destination port restrictions appear at the bottom of the **HTTPS Ports** tab.

   To delete any HTTPS port access restrictions that you might have configured, click the **Delete** icon next to the port or port range to remove.

7. Access control settings are evaluated according to the order they appear in the list at the bottom of the **HTTPS Ports** tab. To change the order that ports are displayed in the list, click the up or down arrows in the **Evaluation Order** column.
8. Click **Save**.

Chapter 8

Policies and User Identification Method

InterScan Web Security Virtual Appliance (IWSVA) is able to apply different Application Control, Bandwidth Control, HTTPS decryption, HTTP virus scanning, HTTP Inspection, Data Loss Prevention, applets and ActiveX security, URL Filtering, and access quota policies to different individuals or groups on your network. In this way, security policies can be customized based on your business need to handle potentially malicious code, view certain categories of Web content or to prevent the consumption of excessive bandwidth for Web browsing.

Topics in this chapter include the following:

- How Policies Work on page 8-2
- Default Global and Guest Policies on page 8-4
- Deploying Policies on page 8-6
- Configuring the User Identification Method on page 8-6
- Configuring Policies Using LDAP on page 8-19

How Policies Work

Different security settings can be configured for different users or groups on your network, based on the type of files or Internet resources they need to access. IWSVA policies can be applied to IPv6 clients and servers, much like the HTTP(S) scan policies, URL filtering policies, and so on. All user identification methods function in the IPv6 environment (client IP address is IPv6) as well. Client and server access control should support IPv6 hosts. The following are some examples of the practical applications of different security policies:

- **Virus scanning:** Your organization's acceptable user policy might generally prohibit clients from downloading audio or video files. However, there might be some groups within your company who have a legitimate business purpose for receiving these types of files. By configuring several virus scanning policies, you can apply different file blocking rules in HTTP virus scanning policies for different groups within your company.
- **Applets and ActiveX security:** To prevent clients from running applets that could intercept sensitive information and transmit it over the Internet, you might want to configure a policy for most of your company that prevents applets from connecting to their originating servers. However, if there are users in your company who have a legitimate business purpose to run these sorts of applets (for example, to get quotations through a Java applet stock price ticker), another policy could be configured and applied to a sub-set of your client base.
- **URL filtering:** To discourage your employees from engaging in non-work-related Web surfing, you might want to configure a Global Policy that blocks access to Web sites in the "gambling" category. However, you might need to configure another policy that permits access to these types of sites so your sales organization can learn more about prospects in the gaming industry. In addition to selected pre-defined categories, you can also create new Web categories to apply to URL filtering policies.
- **HTTPS decryption:** To scan encrypted content over HTTPS connections, you can configure HTTPS decryption policies based on the type of sites accessed. Once decrypted, the content can traverse through filtering and scanning policies on IWSVA as "normal" HTTP traffic. HTTPS decryption policies prevent security risks embedded in HTTPS traffic.

  Account fields should support IPv6 addresses. You can define one rule for any IPv6 host, and this policy rule is triggered when the client accesses the HTTPS sites through IWSVA.

  - When selecting policies, both IPv4 and IPv6 policies will appear.
  - In the Account field, acceptable account entries include a single IPv6 address, an IPv6 range, or an IPv6 mask similar to what has been supported with IPv4.
- **Access quotas:** IWSVA allows you to configure access quota policies to limit the volume of files that clients can download during the course of a day, week, and month, to control the amount of bandwidth that your organization uses. For those employees who have a legitimate business need to browse the Internet extensively, you can configure another policy granting them unlimited Internet access.
- **Application Control:** Using a security technology that automates the discovery of popular Internet-based applications, Application Control policies allow administrators to control the use of those applications. Application Control policies allow granular control of the functionality within the supported Internet-based application categories. IWSVA allows more than a simple allow-or-block option, since many companies have found specific functions of these applications are effective for conducting business.
- **Bandwidth Control**: The Bandwidth Control feature allows administrators to configure policies to control communications, reduce unwanted traffic and allow critical traffic or services the appropriate bandwidth allocation.
- **HTTP Inspection:** HTTP Inspection allows administrators to identify behavior and filter web traffic according to HTTP methods, URLs, and headers. It also allows them to create filters or use default filters to identify web traffic, as well as import and export filters. After the traffic is identified, IWSVA can control it according to policy settings that determine the appropriate actions for specific traffic.
- **Data Loss Prevention:** Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data, referred to as digital assets, against accidental disclosure and intentional theft. IWSVA scans file content to check outgoing traffic for specific data.
- IWSVA provides the flexibility that allows you to configure and apply approved URL or file name lists on a per-policy bases.

In addition to being able to define custom policies that apply to specific users, IWSVA is pre-configured with two default policies, the “Global Policy” and the “Guest Policy,” to provide a baseline level of HTTPS decryption, HTTP virus scanning, HTTP Inspection, Data Loss Prevention, applets and ActiveX security, and URL Filtering.

Note: IWSVA supports the Guest Policy only with Captive Portal and LDAP enabled, or guest port enabled in Deploy Forward proxy mode.

Default Global and Guest Policies

IWSVA has default global and guest policies for the following activities: HTTPS decryption, Advanced Thread Protection, HTTP Inspection, Data Loss Prevention, applets and Active X, and URL Filtering. Application Control and Bandwidth Control have only the default global policy.

- **Global Policy**—For all clients, except those clients controlled by "Guest Policy", who access through IWSVA.
- **Guest Policy**—For those clients, typically temporary workers, contractors, and technicians who proxy through IWSVA using a special "guest access" option.

  Guest accounts are disabled by default; to enable a guest account go to **Administration > IWSVA Configuration > User Identification > Authentication Method > Captive Portal > Allow Guest Login** only after LDAP has been enabled. Go to *Enabling the Guest Account* starting on page 8-5.

Note: The guest policy is a feature that is available when the administrator has configured IWSVA to use the LDAP "User/Group name authentication" feature as the user identification method, or enabled guest port in Deploy Forward proxy mode. Administrators can opt to provide one "Guest Access" button to users who do not have accounts within the organization's directory servers, (such as contract personnel or visiting vendors) so they can still access the Web.

About the Guest Policy

The Guest Policy is the only policy applied to guest users.

For more information about enabling the "User/group name authentication" user identification method, see User/Group Name Authentication starting on page 8-9.

Enabling Guest Port

Use the Deploy wizard in Forward proxy mode to enable Guest port.

To enable Guest Port:

1. Select the Forward Proxy mode radio button on the Deployment Mode page.

   See Forward Proxy Mode on page 2-9 for details.
2. Click **Next**.
3. Select **Enable guest user login**, and use the port number 8081 (default value).
4. Click **Next**.
5. Without changing other default Forward proxy settings, click **Save**.

Enabling the Guest Account

To enable Internet connectivity to network users who are not in the LDAP directory and apply guest policies, enable the settings at **User Identification > Authentication Method**.

To enable the guest account:

1. From the **User Identification** page, select the Captive Portal (Custom Authentication page delivered by IWSVA to browser) option and the "Allow Guest Access" check boxes. (Unauthenticated users will always see the Captive Portal page)."
2. Click **Save**.

Policy Queries

When a new policy is added to the client, administrators might find that the policy is not functioning correctly. You might also like to determine which policy is currently functioning on the client server. The policy query feature is designed to help you discover how many policies are currently functioning on a client.

Using the policy queries is as simple as entering a client's IP address, or a username in the search box and clicking the Search icon.

After clicking the Search icon IWSVA provides the query result grouped by the policy type and sorted by the order. This feature is best suited for administrators who need an overview or summary of the policies used in IWSVA, and a list of those policies that can be found in the violation logs.

Every policy has a "notes" field, and administrators can use the field to store detailed information about the policy.

Deploying Policies

After configuring a policy, the settings are written to the database after you click **Save**. Clicking **Deploy Policies** applies the new policy configuration immediately. Otherwise, the policy changes go into effect when IWSVA reads the information from the database after the time intervals specified under **Policy Deployment Settings (in minutes)** on the **Administration > IWSVA Configuration > Policy Deployment** screen.

Configuring the User Identification Method

You need to configure how IWSVA identifies clients to define the scope of Application Control, Bandwidth Control, HTTPS decryption, HTTP virus scanning, HTTP Inspection, Data Loss Prevention, applets and ActiveX security, URL Filtering, and access quota policies. Your choice of user identification method also determines how security events are traced to the affected systems in the log files and reports.

IWSVA provides three user identification methods to identify clients and apply the appropriate policy:

- IP address (default option)
- User/Group name authentication (LDAP)

The following table lists the different user identification method IWSVA supports in various deployment modes:

TABLE 8-1. Supported User Identification Method in Different Deployment Modes

	IP ADDRESS	USER/GROUP NAME AUTHENTICATION
Transparent Bridge Mode	Yes	Yes
Forward Proxy Mode (Standalone, Dependent)	Yes	Yes
WCCP Mode	Yes	Yes
Simple Transparency Mode	Yes (if source NAT is disabled)	No **Note:** Standard Authentication and Captive Portal do work, but if an end-user inputs a user name and password, others will pass authentication and use the same IWSVA record for the same user. Enable Captive Portal and Cookie Mode work well.
Reverse Proxy Mode	Yes	No
ICAP Mode	Yes	Yes **Note:** Only standard authentication is supported. Captive portal authentication is not supported.

Note: For users connecting to an HTTP server with integrated Windows authentication through the IWSVA using Internet Explorer, make sure the **Use HTTP1.1 through proxy connections** option is selected in the **Tools > Internet Options >Advanced** screen for NTLM (NT LAN Manager) authentication to work properly.

IP Address

The IP address is the default identification option and requires the following:

- Client IP addresses are not dynamically assigned through DHCP as DHCP will make the IP address identification less accurate as DHCP leases expire.
- Network address translation (NAT) is not performed on the network path between the affected system and IWSVA.

If the local network meets these conditions, you can configure IWSVA to use the IP address user identification method.

When using the IP address identification method, the scope of scanning policies is defined by defining a range of IP addresses, or a specific IP address, when adding or editing a policy.

To enable the IP address user identification method:

1. Select **Administration > IWSVA Configuration > User Identification | User Identification** from the main menu.
2. From the **User Identification** screen, select **None**.
3. Click **Save**.

Client Registration Utility

The **Host name (modified HTTP headers)** user identification option requires that you run a Trend Micro-supplied program on each Windows client before clients connect to IWSVA and access the Internet. The program file is: `register_user_agent_header.exe` and is located in the /usr/iwss/bin (IWSVA machine). An effective way to deploy this program to your clients is to invoke it from a logon script for the local Windows domain.

The program works by modifying a registry entry:

32-bit Windows [`HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Internet Settings \User Agent \ Post Platform`]

64-bit Windows [`HKLM \ Software \ Wow6432Node \ Microsoft \ Windows \ CurrentVersion \Internet Settings \ User Agent \ Post Platform`]

Internet Explorer includes that registry entry in the User-Agent HTTP header. You can find the identifying information logged under the **User ID** column in various log files. It alters Windows configuration values to include the MAC address of the client system and the machine name that made the HTTP requests. The MAC address is a unique and traceable identification method and the machine name is an additional and helpful identifier.

After running the `register_user_agent_header.exe` utility, a new registry value is created under the following key:

32-bit Windows [`HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Internet Settings \User Agent \ Post Platform`]

64-bit Windows [`HKLM \ Software \ Wow6432Node \ Microsoft \ Windows \ CurrentVersion \Internet Settings \ User Agent \ Post Platform`]

The new registry value called `IWSS31:<host_name>/<MAC address>` is encrypted, where `<host_name>` and `<MAC address>` correspond to the client that ran the utility.

User/Group Name Authentication

IWSVA can integrate with the following LDAP servers, and supports both the LDAP v2 and v3 protocols:

- Microsoft™ Active Directory for Windows Servers 2003, 2008 and 2012
- Linux™ OpenLDAP Directory 2.2.16, 2.3.39, or 2.4.11
- Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)
- Novell eDirectory 8.8

LDAP Authentication Method

When you enable the "**User/group name authentication**" method, clients are required to enter their network logon credentials before accessing the Internet.

The following table shows which LDAP authentication methods can be used with each of the supported LDAP servers:

TABLE 8-2. Authentication Methods for Supported LDAP Servers

	KERBEROS	SIMPLE AUTHENTICATION	NTLM
Microsoft Active Directory for Windows Servers 2003, 2008 and 2012	yes	no	yes
Linux OpenLDAP 2.2.16, 2.3.39, 2.4.11	yes	yes	no
Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)	no	yes	no
Novell eDirectory 8.8	yes	yes	no

Note: To use the Digest-MD5 authentication method with the Sun Java System Directory Server 5.2, all passwords must be stored as clear text in the LDAP directory.

For increased security protection, IWSVA uses the advanced authentication method (Kerberos or Digest-MD5) for all subsequent user logon authentications from IWSVA to the LDAP server.

LDAP Communication Flows

When clients request Internet content, they are prompted to enter their network credentials. Advanced authentication uses a Kerberos server as a central secure password store. Therefore, the benefit of using Kerberos is that it provides a higher degree of security. After the client's credentials are authenticated with a Kerberos Server, a special encrypted "ticket" certified by the Kerberos server is used to access IWSVA and the Internet.

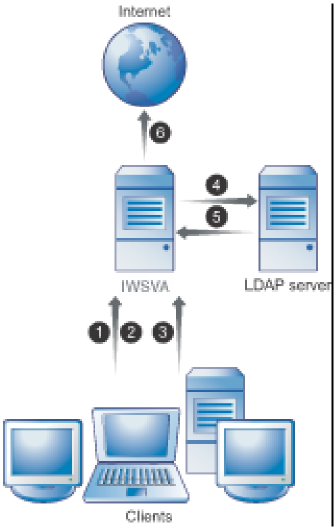


FIGURE 8-1. LDAP Communication Flow Using Kerberos Authentication

When User/group authentication is enabled in either forward proxy mode or transparent mode with Active Directory, you can take advantage of the automatic authentication feature provided in the Internet Explorer Web browser. With automatic authentication, clients already logged on the domain network can access the local Intranet without having to enter the logon information (such as the user name and password); that is, no password pop-up screen displays.

Note: You must configure IE settings to enable automatic authentication on each client computer. By default, automatic authentication is enabled in IE 7.0 or later.

IWSVA supports Internet Explorer automatic authentication for the following authentication method:

- Single domain (LAN or 802.11)
- Global catalog enabled in a multi-domain environment (LAN or 802.11)

To enable automatic authentication in IE:

1. Open Internet Explorer on a client computer, click **Tools > Internet Options** and then click the **Security** tab.
2. Click **Local intranet** and click **Custom level. . .**
3. Select **Automatic logon only in Intranet zone** and click **OK**.
4. Click **Sites**, select **Automatically detect intranet network**, and click **Advanced**.
5. In the Intranet Network screen, type the IWSVA hostname and click **Add**.
6. Save the settings.

To enable automatic authentication in Firefox:

1. Open Firefox on a client computer and type "about:config" in the address field.
2. Type "ntlm" in the **Search** field.
3. Double-click **network.automatic-ntlm-auth.trusted-uris**.
4. A pop-up screen displays. Type the hostname of the IWSVA server and click **OK**.

Note: For other supported Web browsers and authentication methods not listed above, users will need to type the logon information in a pop-up screen.

LDAP Authentication in Transparent Mode

Before configuring LDAP authentication on IWSVA deployed in transparent mode (bridge and WCCP), review the following criteria to ensure each item is fully met.

- A valid hostname must be assigned in the Deployment Wizard when configuring Transparent Bridge or WCCP modes. The same hostname must also be entered in the corporate DNS server.
- Ensure that the user ID cache is enabled, which is the default setting. This setting must be enabled before enabling transparent mode authentication. You can enable user ID cache using the `configure module ldap ipuser_cache enable` command in the CLI.
- By default, IWSVA keeps user ID cache information for up to 2 hours. To lower the cache timeout value, use the `configure module ldap ipuser_cache <interval>` command in the CLI to set a shorter cache interval.

- If authentication is enabled, IWSVA will block all non-browser applications trying to access the Internet. For example, the MSN application may try to access the Internet before the user has a chance to log in the IWSVA server. If this happens, the application will be blocked as the user has not successfully authenticated to IWSVA. You can perform one of the following:

    a. Enable the Domain Controller or Windows client query. After enabling either of these options, no authentication is required because IWSVA obtains the username and domain name through domain controller or client query.

    b. Bypass LDAP authentication for the application by adding the URLs that application accesses to "Global Trusted URLs." The URLs in this list will bypass both authentication and content scanning.

    c. Instruct users to open their Web browsers and get authenticated before starting up applications that need Internet access.

    d. Add the IP address of the client machine to "Approved LDAP Authentication List." IP address in this list will bypass LDAP authentication.

- When User/group authentication is enabled in either forward proxy mode or transparent mode with Active Directory, you can take advantage of the automatic authentication feature provided in the Internet Explorer (IE) Web browser. With automatic authentication, clients already logged on to the domain network can access the local Intranet without having to enter the logon information (such as the user name and password); that is, no password pop-up screen displays.

Note: You must configure your Internet Explorer (IE) settings to enable automatic authentication on each client computer. By default, automatic authentication is enabled in IE.

Configuring LDAP Settings

If you want to use LDAP user/group names for authentication and policy configuration purposes, you must set IWSVA's user identification feature to use your corporate LDAP server.

Note: If you want to apply the Guest Policy for those network users who are not in your LDAP directory, enable the guest account in the Authentication Method section. For more information about enabling the guest account see Enabling the Guest Account starting on page 8-5.

To configure IWSVA to use the user/group name authentication method:

1. Select **Administration > IWSVA Configuration > User Identification | User Identification tab** from the main menu.
2. Enter the Domain name, Service Account (AD User Principle Name (UPN)), and Password of the LDAP server and click **Test Connection** to validate the LDAP connection.
3. Click **Save** to preserve your settings.
4. If you have multiple LDAP domains or multiple LDAP server types, choose Advanced (other or multiple LDAP servers).
5. Enter the LDAP Domain Name.
6. When the LDAP server is a Microsoft Active Directory, "Auto Detect" will be available to detect and automatically fill the domain settings. Enter the "**Admin account**" and **Password** for a credential with at least read authority to the LDAP server. If the domain is *us.example.com*:
   - For Microsoft Active Directory, use the UserPrincipalName for the admin account, for example, *NT_Logon_ID@us.example.com*.
   - For OpenLDAP and the Sun Java System Directory Server 5.2, enter the Distinguished Name (DN) for the admin account (for example, `uid=LOGON_ID,ou=People,dc=us,dc=example,dc=com`).
7. When the LDAP server is a Microsoft Active Directory, configure LDAP encryption:
   - If you do not want to use the LDAP encryption, select **None** for **LDAP Encryption**.
   - If you want to use the LDAP encryption, select **LDAPv3 StartTLS extension** or **LDAP over SSL** for **LDAP Encryption**.

Note: If **StartTLS** is selected for LDAP encryption, the LDAP port number must be 389 or 3268.
If **LDAP over SSL** is selected, the used listening port number will be 636 or 3269.

8. Enter the **Listening port number** used by the LDAP server that you have chosen (default = 389). If your network has multiple Active Directory servers and you have enabled the Global Catalog (GC) port, change the listening port to 3268.

   Note: If you enable the Global Catalog in Active Directory, you might need to configure your firewall to allow communication through port 3268.

9. Enter the LDAP server's hostname using the Fully Qualified Domain Name (FQDN).
10. Enter the **Base distinguished name** to specify from which level of the directory tree you want IWSVA to begin LDAP searches.

    The base DN is derived from the company's DNS domain components; for example, LDAP server `us.example.com` would be entered as *DC=example, DC=com*.

    If you are using Active Directory servers with the Global Catalog (GC) port enabled, use the root domain of the Global Catalog-enabled Active Directory; for example, use *dc=example,dc=com*.
11. Select the LDAP authentication method to use—either **Simple, Digest-MD5,** or **Kerberos**.

    Additionally, configure the following parameters to use Advanced authentication:

    - Default Realm
    - Default Domain
    - **KDC and Admin Server:** The hostname of the Kerberos key distribution server. If you are using Active Directory, this is typically the same host name as your Active Directory server.
    - **KDC port number:** Default port = 88

When using NTLM to authenticate with KDC(s) on a different forest through Internet Explorer or using IWSVA to do referral chasing with Active Directory, Trend Micro recommends enabling "Use HTTP 1.1 through proxy connections." This setting can be found on the Internet Explorer **Tools** menu **> Internet Options > Advanced** tab. Enabling this setting prevents Internet Explorer from cutting off the "Keep-Alive connection" setting. Note that using NTLM is only supported with Microsoft Active Directory.

12. Configure the **Approved Authentication List** to exempt hosts from the LDAP authentication process.

    For example, if you have an application server that access the Internet and you want to permit its access without requiring the server to authenticate, you can include the server's IP address in the approved LDAP authentication list.

    IWSVA will only apply IP address-based policy settings and bypass user/group name checking.

    IWSVA supports LDAP queries from IPv6 with similar behavior to that of IPv4. The approved LDAP client list supports IPv6 addresses similar to that of IPv4 as well. The LDAP Authentication request dialog box supports IPv4 and IPv6 with port 9090, and IWSVA can automatically redirect the authentication dialog box to IWSVA's IPv4 or IPv6 address to a client based on the client's IP address version.

    - When the client uses an IPv4 address, IWSVA should send the redirect request with IWSVA's IPv4 address.
    - When the client uses an IPv6 address, IWSVA should send the redirect request with IWSVA's IPv6 address.

13. To verify the information has been entered correctly and IWSVA can communicate with the LDAP servers that you configured, click **Test LDAP Connection** on the **User Identification** page.

    A message appears, indicating that you have successfully contacted the LDAP server.

14. Click **Save**.

Note: After the LDAP server has successfully been added, a new button appears that reads "Sync with LDAP servers." Click this button to do a manual synchronization with your user group information.

Cross Domain Active Directory Object Queries

Trend Micro recommends using the Global Catalog port (3268) as the IWSVA LDAP communication port when using Microsoft Active Directory. Using port 3268 enables cross domain group nesting object queries. This applies when an object's attribute on one domain refers to another object residing on a different domain (for example, cross-domain user or group membership that resides on different domains in a forest).

For retrieving cross-domain group object attribute(s), you must create groups with the "Universal" Group Scope to ensure that cross-domain group memberships within an Active Directory forest are included in the Global Catalog. Using the Universal Group Scope to create groups also allows cross-domain queries. Avoid creating or using Global Group policies when the Global Catalog has been enabled.

Note: To configure IWSVA to listen on port 3268, the Microsoft Active Directory server that IWSVA uses should have the Global Catalog enabled.

Since the member attribute is not replicated to the Global Catalog for all group types, and because the *memberOf* attribute derives its value by referencing the member attribute (called back links and forward links, respectively), search results for members of groups, and groups in which a member belongs, can vary. Search results depend on whether you search the Global Catalog (port 3268) or the domain (port 389), the kind of groups that the user belongs to (global groups or domain local groups), and whether the user belongs to universal groups outside the local domain.

For more information, search for the article "How the Global Catalog Works" at http://www.microsoft.com.

Configuring the Scope of a Policy

Whether configuring Application Control, Bandwidth Control, HTTPS decryption, HTTP virus scanning, HTTP Inspection, Data Loss Prevention, applets and ActiveX security, URL Filtering, and access quota policies, the first step is the same—to configure the policy's scope by identifying the client users to which the policy applies. The following three procedures describe how to select the accounts using the IP address and the user/group name authentication user identification methods.

Those procedures are:

- Configuring Policies Using IP Addresses on page 8-18

- Configuring Policies Using LDAP on page 8-19

Note: Even if you configure IWSVA to use User/group name authentication user identification method, you can always specify clients by entering an IP address or IP address range.

Before adding a policy and configuring its scope, set the user identification method. See Configuring the User Identification Method starting on page 8-6 for more information.

Configuring Policies Using IP Addresses

Configuring policies using the clients' IP addresses is the simplest identification method and is always available, regardless of the user identification method you have configured to use.

To configure a policy's scope using the IP address user identification method:

1. From the main menu, click **HTTP** and choose the type of policy to create (**HTTPS Decryption policies**, **Advanced Threat Protection Policies**, **HTTP Inspection Policies**, **Data Loss Prevention Policies**, **Applets and ActiveX Policies**, **URL Filtering Policies**, or **Access Quota Policies**).

   Note: Access Application Control policies from the **Application Control > Policies** menu.
   Access Bandwidth Control policies from the **Bandwidth Control > Policies** menu.

2. In the screen that corresponds to the type of policy selected, click **Add**.
3. Type a descriptive **new policy name**.

   Policy names that include references to the users or groups to which they apply (for example, "Virus Policy for Engineers" or "URL Filtering Policy for Researchers") are easily recognizable.

4. Select the users to which this policy applies by typing the upper and lower bounds of a contiguous range of IP addresses in the **From** and **To** fields. Alternatively, type a single **IP address**. Click the corresponding **Add** button to add the addresses to the policy.

5. When you have named your new policy and defined the IP address(es) to which it applies, click **Next** to proceed with the other policy settings.

Configuring Policies Using LDAP

Before configuring a policy using users or groups from your LDAP server, set the user identification method and enter the details of your LDAP server. For more information, see Configuring LDAP Settings starting on page 8-13.

To configure a policy's scope using users and groups from an LDAP server:

1. From the main menu, click **HTTP** and then choose the type of policy to create (**HTTPS Decryption policies**, **Advanced Threat Protection Policies**, **HTTP Inspection Policies**, **Data Loss Prevention Policies**, **Applets and ActiveX Policies**, **URL Filtering Policies**, or **Access Quota Policies**).

> **Note:** Access Application Control policies from the **Application Control > Policies** menu.
> Access Bandwidth Control policies from the **Bandwidth Control > Policies** menu.

2. In the screen that corresponds to the type of policy that you selected, click **Add**.
3. Type a descriptive **new policy name**.
4. To query your LDAP directory for users or groups to add to your policy:
   a. Check either **User** or **Group**.
   b. Type the first part of the user or group name in the **Name** field and click **Search**.
   c. When the list box displays users or groups that match your search criteria, highlight the user or group to add to the policy and click **Add**.
5. Repeat adding users or groups until your policy's scope is complete.
6. When you have named your new policy and defined the account(s) to which it applies, click **Next** and proceed with configuring the rest of the policy.
7. Configure multiple domains when the user's credentials exist on a different directory server than the one configured.

Chapter 9

Configuring HTTP Scanning

This chapter describes how to configure HTTPS decryption, HTTP virus scanning, HTTP Inspection, Data Loss Prevention, and applets and ActiveX security policies in InterScan Web Security Virtual Appliance (IWSVA). Topics in this chapter include:

Enabling Advanced Threat Protection and Applets and ActiveX Security

You can enable or disable HTTP scanning from the HTTP Scan Policies page of the IWSVA Advanced Threat Protection page.

Note: In addition to enabling HTTP scanning and Applet/ActiveX security, ensure that HTTP traffic is turned on, otherwise clients cannot access the Internet. (See Enabling the HTTP/HTTPS Traffic Flow starting on page 7-2.)

To enable HTTP scanning and Applets and ActiveX Security:

1. Go to **HTTP > Advanced Threat Protection > Policies**.
2. At the top of the page, check **Enable virus scanning** and **Enable Web reputation**, then click **Save**.
3. Go to **HTTP > Applets and ActiveX** > **Policies**.
4. At the top of the page, check **Enable Applet/ActiveX security**, then click **Save**.

Advanced Threat Protection Performance Considerations

There are trade-offs between performance and security while scanning HTTP traffic for malicious content. When users click a link on a Web site, they expect a quick response. This response, however, might take longer as gateway antivirus software performs virus scanning. Some of the requested files might be large, and determining whether the file is safe requires downloading the entire file before it is relayed to the user. Content might also consist of many small files. In this case, the user's wait is the result of the cumulative time needed to scan the files.

One way to improve the user's experience is to skip scanning large files or files that are not likely to harbor viruses. For example, you can skip all files with an extension of `.gif`, or all files with a MIME type.

When configured to skip scanning a file because of its MIME content-type, IWSVA attempts to determine the file's true-file type (if you have enabled this feature) and match it to the claimed MIME type before skipping it. If the file's true-file type maps to a different MIME type than indicated in the Content-type header attached to the transaction, the file is scanned. Unfortunately, there is not always a clear mapping between file types and MIME types. If you disable the true file type option, IWSVA does not map the true-file type to a MIME type, it is skipped according to the Content-type header as configured.

You can exclude files from scanning based on the file extension. Trend Micro recommends that you minimize the list of MIME content-types to skip. In general, relying on the scan engine to determine whether a file should be scanned is safer than trying to pick out which file types you want to skip yourself. First, the content-type HTTP header might not accurately represent the true type of the content to download. Second, some types that you might think are safe to skip (for example, text) might not really be safe (because scripts are text, and might possibly be malicious). One more area where you might want to use MIME content-type skipping is where you are consciously making a trade-off in safety versus performance. For example, a lot of Web traffic is text, and the IWSVA scan engine scans all that traffic because the content might contain scripts, which are potentially malicious. But if you are confident that you are browsing an environment that cannot be exploited by Web scripts, you might choose to add text/* to your MIME content-type skip list so IWSVA does not scan Web pages.

Malicious code within a small file can quickly spread throughout a network. Malicious code that requires a large file for transport propagates more slowly, because the file containing malicious code takes longer to transmit. Therefore, it is important to screen small files efficiently and completely.

Note: System performance may be adversely affected if the main policy for ActiveX scanning directs all PE (windows executable) files to be scanned (not just COM objects, of which ActiveX controls are a subtype), or if all unsigned PE files are to be blocked. The performance impact occurs because the Javascan daemon—which enforces policy for these files—as well as Java Applets) is invoked more often.

HTTP Inspection Overview

The HTTP Inspection feature in IWSVA provides policy control based on HTTP methods, URLs, and HTTP headers.

Web behavior has become more complicated. IT managers face many challenges, like enforcing browser type policies, blocking large file transfers to save bandwidth, blocking Web file uploads and blocking Web Distributed Authoring and Versioning (WebDAV) traffic. These actions are used to protect company data from loss, block video uploads, filter on keywords in headers and take action, and prevent message posting on social networking service (SNS) sites.

HTTP Inspection allows admins to identify behavior and filter web traffic according to HTTP methods, URLs, and headers. It also allows admins to create filters or use default filters to identify web traffic. After the traffic is identified, IWSVA can control it according to policy settings that allow admins to determine the appropriate actions for specific traffic.

Note: HTTP Inspection filters cannot inspect the data payload of the HTTP packets. For example, it cannot look for pattern matching inside the text or file of a webmail or social networking site post. It can only identify that a POST action is happening to a defined site or set of sites and prevent that POST.

Information about HTTP Inspection is shown in corresponding logs and reports. HTTP Inspection notifications are also available to inform end-users why their actions on the Web are being blocked.

HTTP Inspection Policies

The HTTP Inspection Policy list at **HTTP > HTTP Inspection > Policies** shows all HTTP Inspection (IPv4 and/or IPv6) policies on the system—enabled as well as disabled. Click Add to create a new policy, or click a policy name to edit an existing one. See the following sections for details:

- HTTP Inspection: Select Accounts on page 9-5
- HTTP Inspection: Specify Rules on page 9-6
- HTTP Inspection: Specify Exception Lists on page 9-8

Editing an HTTP Inspection policy requires clicking on the policy name, then clicking the **Rule** tab.

HTTP Inspection: Select Accounts

Filters are required to add an HTTP Inspection policy. Several default filters are provided, but to create a policy using a custom filter, you must create the filters first at **HTTP > HTTP Inspection > Filters**. Acceptable accounts include a single IP address, an IP range, or an IP mask for both IPv4 and/or IPv6 accounts, User, or Group (if User Identification is enabled).

To enable HTTPS inspection:

1. Click **HTTP > HTTPS Decryption > Policies** from the main menu.
2. Select **Enable HTTPS Inspection**.
3. Click **Save**.

To select accounts for an HTTP Inspection policy:

1. Go to **HTTP > HTTP Inspection > Policies**.
2. Click **Add**.
3. Enter or determine the following information:
   - **Enable policy**—Enable or disable the individual policy.

   Note: If you have HTTP Inspection policies disabled at the global level (through **HTTP > HTTP Inspection > Policies**), the enabled status of an individual policy will be ignored.

   - **Create new policy**—Type a brief but descriptive name for the policy rule. Names must be unique, and will appear in the list of policies that appears when you click HTTP > HTTP Inspection > Policies.
   - **Select the users to which the policy applies**—The options on this page depend upon the user identification method that you are using—either IP address, Hostname (modified HTTP headers), or User/group name authentication. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method on page 8-6.

Note: Before choosing a Hostname, you need to prepare all clients on the LAN by running the following program on each client:

```
/usr/iwss/bin/register_user_agent_header.exe
```

This can be done by adding it to your Windows domain login script (or by creating one only for this purpose.)

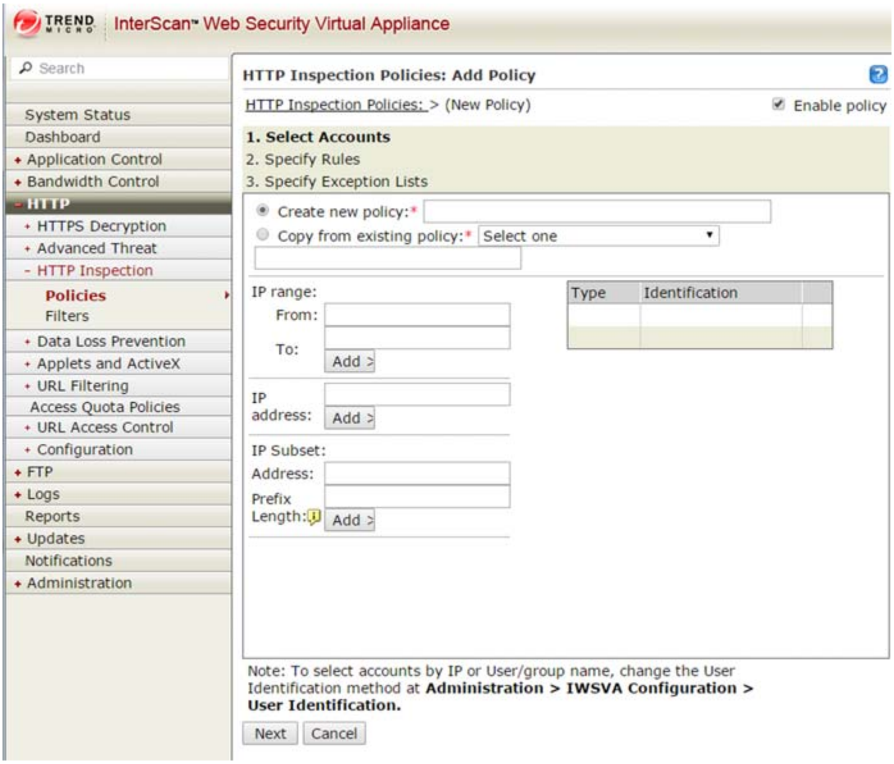
4. Click **Next** to specify the rules and exception, if any, for the new policy.

HTTP Inspection: Specify Rules

The Rules screen allows you to select the Inspection Filters for HTTP traffic. Adding an HTTP Inspection policy is a three-step procedure. First, create an account, then assign HTTP Inspection filtering rules to the new account, and then specify any exceptions.

To specify the rules in your HTTP Inspection policy:

1. Complete the steps in To select accounts for an HTTP Inspection policy: on page 9-5.



HTTP Inspection Policies: Add Policy

HTTP Inspection Policies: > (New Policy) ☑ Enable policy

1. Select Accounts
2. Specify Rules
3. Specify Exception Lists

● Create new policy:*
○ Copy from existing policy:* Select one ▾

IP range:
From:
To:
Add >

IP address: Add >

IP Subset:
Address:
Prefix Length: Add >

Type	Identification

Note: To select accounts by IP or User/group name, change the User Identification method at **Administration > IWSVA Configuration > User Identification.**

Next Cancel

FIGURE 9-1. Configuring HTTP Inspection policy blocking all content posting to defined social networking sites

2. Enter information or determine the following:
   - **Enable policy**—Enables or disables the individual policy; the global HTTP Inspection setting overrides the specifications of an individual policy.

- **Inspection Filter**—Choose the Inspection Filter to designate the type of traffic to which the policy will apply. The number of filters available is equal to the default filters plus any custom filters that have been created. *Table 9-1* describes the default filters.

Note: You can create custom filters at **HTTP > HTTP Inspection > Filters > Add**.

- The following describes the available filtering actions:
  - **Allow (scan)**—Connection to the target server is allowed and users can access the Web site, but the content is scanned for malware.
  - **Allow (no scan)**—Connection to the target server is allowed and users can access the Web site, but the content is not scanned for malware.
  - **Block**—Connection to the target server is not established and users are not allowed to access the Web site. A log entry is also created for this event.
  - **Monitor**—Connection to the target server is allowed and users can access the Web site. A log entry is also created for this event.

Note: For the next section, restricted days and hours are defined at **Administration > IWSVA Configuration > Scheduled Times**.

- **Scheduling**—Configure the schedule by going to **Administrator** > **IWSVA Configuration** > **Scheduled Times**. The default is **Always**.
- **Note**—Create policy notes, for example, to summarize the intent or justification for the policy. It can serve as a simple reminder or as a communication to others who could later administer HTTP Inspection.

3. Click **Next** to continue.

HTTP Inspection: Specify Exception Lists

There may be URLs or Web sites that you want to exempt from HTTP Inspection filtering (for example, the corporate intranet, business partner sites, and research tool sites). URLs in the exception list will not be blocked or monitored.

You can create exception lists in the **HTTP > Configuration > Approved Lists** page.

To specify exception to the HTTP Inspection policy:

1. Configure the accounts and rules.
2. On the HTTP Inspection Policies: Add Policy Exceptions page, select the name from the drop-down list of the Approved URL List to be exempted from a HTTP Inspection rule.

   Note: Approved lists are configured at **HTTP > Configuration > Approved Lists**.

3. Click **Save**. Your new policy will now appear in the list of policies at **HTTP > HTTP Inspection > Policies**.

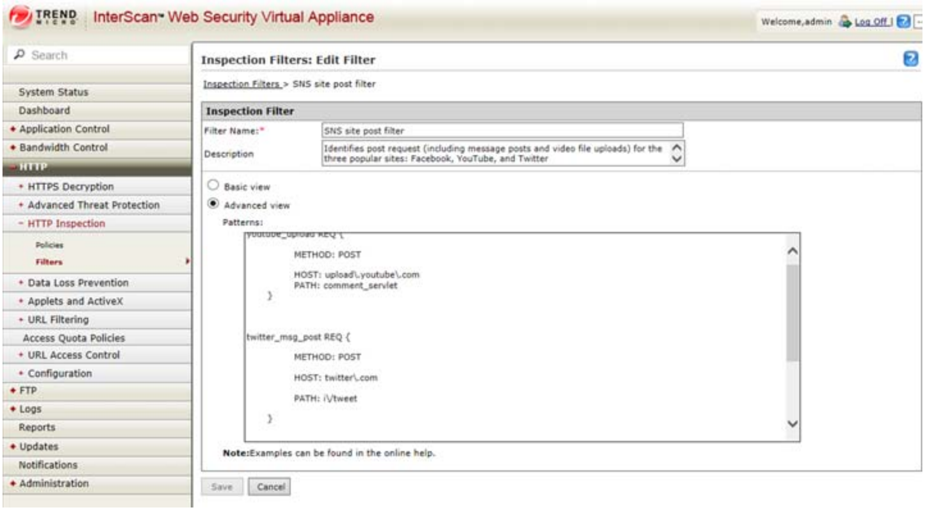
HTTP Inspection Filters

The HTTP Inspection filters provide a general way to identify Web traffic. It allows for the creation of filtering conditionals using the following components:

- URL Host
- URL Path
- URL Query
- HTTP Method
- HTTP Header

Default HTTP Inspection Filters

Default filters for HTTP Inspection provide filtering for common scenarios, such as blocking social networking services (SNS) uploads or regulating Web access through the use of certain types of browsers.



Inspection Filters: Edit Filter

Inspection Filters > SNS site post filter

Inspection Filter

Filter Name:* SNS site post filter

Description: Identifies post request (including message posts and video file uploads) for the three popular sites: Facebook, YouTube, and Twitter

○ Basic view

● Advanced view

Patterns:

```
youtube_upload REQ {
            METHOD: POST
            HOST: upload\.youtube\.com
            PATH: comment_servlet
      }


twitter_msg_post REQ {
            METHOD: POST
            HOST: twitter\.com
            PATH: i\/tweet
      }
```

Note: Examples can be found in the online help.

FIGURE 9-2. HTTP Inspection filter configuration for preventing POST actions to defined social networking sites

See *Table 9-1* for the default filter settings. Admins can make minor adjustments to the default or pre-defined filters to obtain the control capabilities needed.

- **Add**—Opens the Add Filter wizard that will take you through the steps of defining a new filter.
- **Delete**—Allows you to delete a filter.
- **Export**—Allows you to export existing filters.

- **Import**—Allows you to import custom filters created elsewhere or by technical support and import exported filters.

Table 9-1. Matrix of Default HTTP Inspection Filters

Default Filter Name	**Filtering Type**	**Request Method**	**URL Host**	**URL Path**	**URL Query**	**Header** (Name/ Operator/ Value)
Browser Type	REQ	None	None	None	None	User-Agent/ Contains/ MSIE || Firefox || Chrome || Opera
Large data download	RESP	N/A	None	None	None	Content-length/ ≥/ 1048576
Large data upload	REQ	None	None	None	None	Content-length/ ≥/ 1048576
Query Keyword	REQ	None	None		<keyword>	None/None/ None

TABLE 9-1. Matrix of Default HTTP Inspection Filters (Continued)

DEFAULT FILTER NAME	FILTERING TYPE	REQUEST METHOD	URL HOST	URL PATH	URL QUERY	HEADER (NAME/ OPERATOR/ VALUE)

SNS SITE POST	REQ	POST	(Added in Advanced View)
			`youtube_upload` `REQ {`
			`METHOD: POST`
			`HOST: upload\.youtube\.com }`
			`twitter_msg_post` `REQ {`
			`METHOD: POST`
			`HOST: twitter\.com`
			`PATH: status`
			`}`
			`facebook_upload` `REQ {`
			`METHOD: POST`
			`HOST: upload\.facebook\.com }`
				None	None	None/
						None/
						None

WEB FILE UPLOAD	REQ	POST	None	None	None	Content-Type/ Contains/ multipart/form-data

TABLE 9-1. Matrix of Default HTTP Inspection Filters (Continued)

DEFAULT FILTER NAME	FILTERING TYPE	REQUEST METHOD	URL HOST	URL PATH	URL QUERY	HEADER (NAME/ OPERATOR/ VALUE)
WEBDAV	REQ	PROPFIND PROPMATCH MKCOL COPY MOVE	None	None	None	None/ None/ None

Add an HTTP Inspection Filter

There are two ways to add HTTP Inspection filters:

- **Basic view**—Common component of a filter are provided, offering options for the filtering type (HTTP request or response), URL host, URL path, URL query, and request or response header.
- **Advanced view**—Allows you to enter patterns

Note: New filters can also be added by clicking on the name of an existing filter, then modifying it as needed and saving it under a different name.

Adding a Filter in Basic View

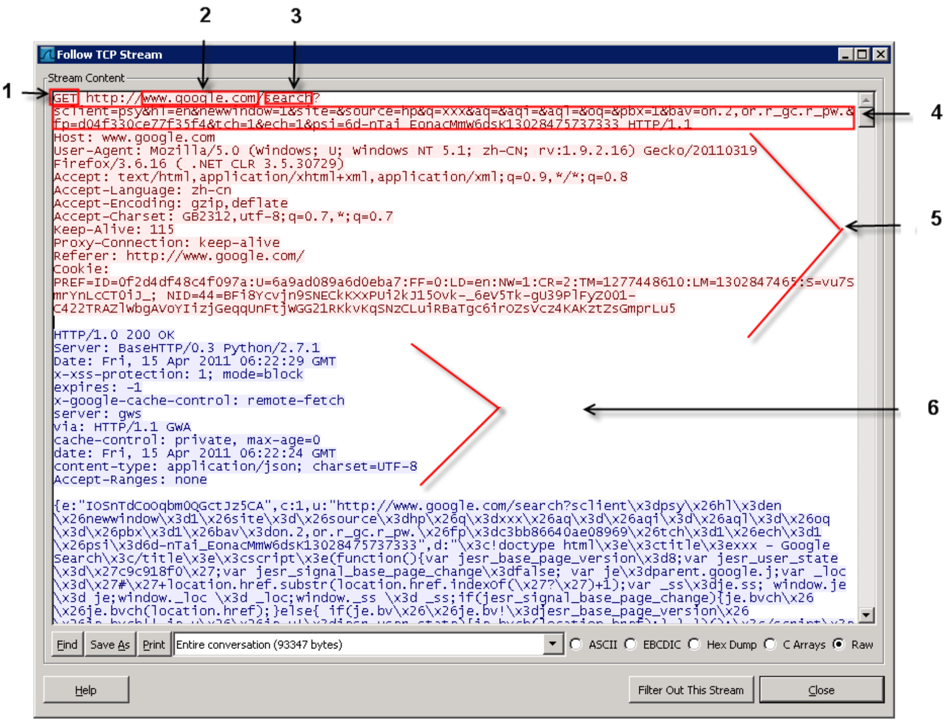
The filter configured in the Basic View defines the following:

- **Filter name and description**—Name and description assigned to the new filter by the user.
- **HTTP request or response**—Denotes the traffic direction
- **Filter scope**—Includes the HTTP method (HTTP request only), path, query, and/or header

- **Keyword matching**—For the HOST, PATH, QUERY and METHOD options, matching means the value contains the input keywords (using simple string comparison.) For the HEADER option, matching supports both string-value matching and integer-value comparison.

Using a Packet Capture

To determine some of the components for your filter, it helps to run a packet capture on the HTTP request or response. See the sample capture in *Figure 9-3* and the explanation in *Table 9-2*. See more about the Network Packet Capturing tool at Network Packet Capturing on page 15-39.



```
GET http://www.google.com/search?
sclient=psy&hl=en&newwindow=1&site=&source=hp&q=xxx&aq=&aqi=&aql=&oq=&pbx=1&bav=on.2,or.r_gc.r_pw.&
fp=d04f330ce77f35f4&tch=1&ech=1&psi=6d-nTai_EonacMmw6dsK13028475737333 HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.16) Gecko/20110319
Firefox/3.6.16 ( .NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn
Accept-Encoding: gzip,deflate
Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://www.google.com/
Cookie:
PREF=ID=0f2d4df48c4f097a:U=6a9ad089a6d0eba7:FF=0:LD=en:NW=1:CR=2:TM=1277448610:LM=1302847465:S=vu7S
mrYnLcCT0iJ_; NID=44=BFi8Ycvjn9SNECkKXxPUi2kJ15Ovk-_6eV5Tk-gU39PlFyZ001-
C422TRAZlWbgAVoYIizjGeqqUnFtjWGG21RKkvKqSNzCLuiRBaTgc6irOZsVcz4KAKztZsGmprLu5

HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.1
Date: Fri, 15 Apr 2011 06:22:29 GMT
x-xss-protection: 1; mode=block
expires: -1
x-google-cache-control: remote-fetch
server: gws
via: HTTP/1.1 GWA
cache-control: private, max-age=0
date: Fri, 15 Apr 2011 06:22:24 GMT
content-type: application/json; charset=UTF-8
Accept-Ranges: none

{e:"IOSnTdCoOqbm0QGctJz5CA",c:1,u:"http://www.google.com/search?sclient\x3dpsy\x26hl\x3den
\x26newwindow\x3d1\x26site\x3d\x26source\x3dhp\x26q\x3dxxx\x26aq\x3d\x26aqi\x3d\x26aql\x3d\x26oq
\x3d\x26pbx\x3d1\x26bav\x3don.2,or.r_gc.r_pw.\x26fp\x3dc3bb86640ae08969\x26tch\x3d1\x26ech\x3d1
\x26psi\x3d6d-nTai_EonacMmw6dsK13028475737333",d:"\x3c!doctype html\x3e\x3ctitle\x3exxx - Google
Search\x3c/title\x3e\x3cscript\x3e(function(){var jesr_base_page_version\x3d8;var jesr_user_state
\x3d\x27c9c918f0\x27;var jesr_signal_base_page_change\x3dfalse; var je\x3dparent.google.j;var _loc
\x3d\x27#\x27+location.href.substr(location.href.indexOf(\x27?\x27)+1);var _ss\x3dje.ss; window.je
\x3d je;window._loc \x3d _loc;window._ss \x3d _ss;if(jesr_signal_base_page_change){je.bvch\x26
\x26je.bvch(location.href);}else{ if(je.bv\x26\x26je.bv!\x3djesr_base_page_version\x26
```

FIGURE 9-3. Packet capture for Google search

TABLE 9-2. Components shown in the Packet Capture

NUMBER	COMPONENT
1	Request method
2	URL host
3	URL path
4	URL query
5	Request header
6	Response header

To add a new HTTP Inspection filter in the basic view:

1. Go to **HTTP > HTTP Inspection > Filters**.
2. Click **Add**.
3. Enter a filter name and description.
4. Select the **Basic view** radio button. See *Figure 9-2*.
5. Select the filtering type, either HTTP Request or HTTP Response, depending on the direction for which you want to create a filter:
    - **HTTP Request**—Creates a filter used when clients send a request to the Web server to retrieve an HTML page. Request filters include the following scope: request method, URL host, URL path, URL query, and HTTP header.
    - **HTTP Response**—Creates a filter used when the Web server returns a response message to the client. Response filters include the following scope: URL host*, URL path*, URL query*, and HTTP response header.

Note: Information for the items above with an asterisk (*) are obtained from the HTTP request. The response does not contain this information.

6. Enter values to define the filter by configuring one or more of the following options:
   - (HTTP Request Filtering type only) Check the **Request Method** check box. To limit the scope of the filter, provide the HTTP request method. The value can be those show in *Table 9-3* or any other extension method value.

TABLE 9-3. Method Values for HTTP Request Filters

METHOD	DESCRIPTION
DELETE	Deletes the specified resource.
GET	Requests the specified resource.
HEAD	Asks for the response identical to the one that would correspond to a GET request, but without the response body. This is useful for retrieving meta-information written in response headers, without having to transport the entire content.
OPTIONS	Returns the HTTP methods that the server supports for specified URL. This can be used to check the functionality of a web server by requesting '*' instead of a specific resource.
POST	Submits data to be processed (e.g., from an HTML form) to the identified resource. The data is included in the body of the request. This may result in the creation of a new resource or the updates of existing resources or both.
PUT	Uploads a representation of the specified resource.
TRACE	Echoes back the received request, so that a client can see what (if any) changes or additions have been made by intermediate servers.

Note: Users can define multiple keywords with an OR relation, separated by the '|' character or on a new line for the URL Query, URL Path, Header, or HTTP Method options.

- Check the **URL Host** check box. Type the host name or IPv4/IPv6 address (including port number, if any) as part of the URL.
- Check the **URL Path** check box. Type the path part of the URL (if any) after, but not including, the final "/" of the host part, and up to, but not including, the "?" of the query, if any.
- Check the **URL Query** check box. Type the query part of the URL (if any), after, but not including, the "?" and up to the end of the URL string in the field below the translation wizard.
  - If you need to translate a UTF-8 string, check the **Need a translator** check box.

  Note: Keyword queries are only supported in UTF-8 encoding. Use URL-encoded hex code to match multiple-byte characters with other character sets.

  - Type the UTF-8 string to translate.
  - Select the appropriate character set:
    - Chinese Simplified (GB2312)
    - Chinese Traditional (Big5)
    - Japanese (EUC)
    - Japanese (Shift-JIS)
  - Click **Translate** and the translated value appears in the Translated string field.
- Check the **Header** check box. To select the Name and Value heading to be used, click the "+" sign in the last column. This supports both string-value matching and integer-value comparison:
  - **Contains | Not Contain** means the value contains or does not contain the input keywords using a simple string comparison.

- Add multiple keywords with an OR relation, separated by the "|" character.
- =, ≠, ≥, ≤ —Means integer-value comparison
- **Exist/Not exist**—Means the header includes or does not include the defined header
- The web traffic is matched by one filter only if all the defined scopes are matched, which means there is an AND relation in METHOD, HOST, PATH, QUERY, and multiple HEADERs.
- Type the values to be used and select the appropriate operation (Contains, Not Contain, equals, does not equal, greater than or equal to, or less than or equal to) from the drop-down list.

7. Click **Save**.

   Your new filter name now appears in the list of filters at the HTTP > HTTP Inspection > Filters.

Adding a Filter in the Advanced View

You can edit filter definitions in text mode with defined syntax. (HTTP BODY is not supported.) Regular expressions are supported. All regular expressions are applied (see `http://www.pcre.org/pcre.txt`). See *Table 9-4* for the active Perl-Compatible Regular Expressions (PCRE) flags.

TABLE 9-4. Active PCRE Flags for Use in Configuring Patterns

REGULAR EXPRESSION	DESCRIPTION
PCRE_DOTALL	The '.' (period) character matches any byte, including the EOL characters CR ('\r') and LF ('\n').
PCRE_DOLLAR _ENDONLY	The '$' (dollar sign) character matches only the absolute "end of source" (the end of the data), and does not match EOL.

TABLE 9-4. Active PCRE Flags for Use in Configuring Patterns (Continued)

REGULAR EXPRESSION	DESCRIPTION
PCRE_EXTENDED	The main effect of this is that the following characters (as literals) are ignored in regular expression definitions: ‘ ’ (space), tab, carriage return, line feed, form feed, ‘#’ However, the escaped forms of these characters are obeyed: ‘\ ’, ‘\t’, ‘\r’, ‘\n’, ‘\f’, ‘\#’. The main reason for this behavior is to allow regular expression definitions to be formatted in a more readable manner (with white space emphasizing structure and branches), and to allow them to be easily split across line boundaries.

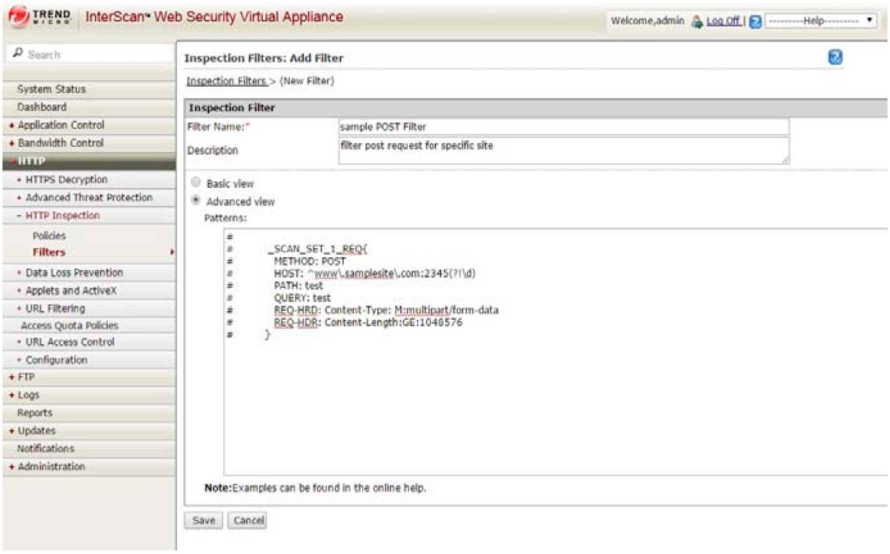
Note: Note: PCRE_DOTALL and PCRE_EXTENDED may be turned off by including ‘(?-s)’ and ‘(?-x)’, respectively, in an expression.

Other rules include:
-The PCRE runtime flag PCRE_UTF8 (“UTF-8 mode”) is never used. This means that the ‘.’ character will always match only one byte.
- In signature definitions, EOL may be escaped by using ‘\’ (backslash) at the end of the line (in the Unix shell manner). Note that this is not part of the PCRE regular expression language and, to be safe, the line continuation backslash should be preceded by at least one space. When assembling a multi-line regular expression for use, the line-end backslashes are stripped, and then all leading and trailing white space is stripped from each line before the lines are concatenated.

To add a new HTTP Inspection filter in the advanced view:

1. Go to **HTTP > HTTP Inspection > Filters**.
2. Click **Add**.
3. Enter a filter name and description.

4. Select the **Advanced view** radio button. See *Figure 9-4*.



Inspection Filters: Add Filter

Inspection Filters > (New Filter)

Inspection Filter

Filter Name:* sample POST Filter

Description filter post request for specific site

○ Basic view

● Advanced view

Patterns:

```
#
#       _SCAN_SET_1_REQ{
#         METHOD: POST
#         HOST: ^www\.samplesite\.com:2345(?!\d)
#         PATH: test
#         QUERY: test
#         REQ-HRD: Content-Type: M:multipart/form-data
#         REQ-HDR: Content-Length:GE:1048576
#       }
```

Note: Examples can be found in the online help.

FIGURE 9-4. Sample Request mode POST filter in Advanced view

5. Do one of the following:

   - To do pattern matching, enter a pattern in the **Patterns** field. Use the following syntax:

   Note: The [Filter Type] must be replaced with REQ (for request mode) or RESP (for response mode.)

   ```
   [ScanSetName] [Filter Type] {
   [TAG]:RegularEx
   [HDR-TAG]:[HDR-NAME]:[HDR-OP]:RegularEx
   [TAG]
   METHOD, HOST, PATH, QUERY
   [HDR-TAG]
   ```

```
REQ-HDR, RESP-HDR}
[HEADER_OP]:
-----------------------------------
EQ : =
NE : !=
GE : >=
LE : <=
M : Contain
NM : Not Contain
X  : Exist
NX : Not exist
```

i. Here is a sample pattern for Request mode:

```
#
#        _SCAN_SET_1_ REQ {
#              METHOD: POST
#              HOST: ^www\.samplesite\.com:2345(?!\d)
#              PATH: test
#              QUERY: test
#
REQ-HDR:Content-Type:M:multipart/form-data
#              REQ-HDR:Content-Length:GE:1048576
#       }
#
```

ii. Here is a sample pattern for the Response mode:

```
#
#        _SCAN_SET_2_ RESP {
#             HOST: ^www\.samplesite\.com:2345(?!\d)
#             PATH: test
#             QUERY: test
#
RESP-HDR:Content-Type:M:multipart/form-data
#                RESP-HDR:Content-Length:GE:1048576
#         }
#
```

Note: Other considerations:
1. For integer value comparisons, IWSVA converts the string value part. The string may include a '0x' prefix, and the number will be read in base 16; otherwise, it is interpreted as 10 (decimal) unless the next character is '0', in which case it is interpreted as 8 (octal).

2. If the first non-space character is not a sign or a digital number, then it is not a number.

3. Do not include RESP-HDR in a request header check rule. You cannot add headers which only appear in response headers to a request type filter.

4. Do not include METHOD and REQ-HDR in a response header check rule. You cannot add headers which only appear in request headers to a response type filter. When using the advanced view to create new filters, do not use METHOD in the response type filter.

5. IWSVA does not verify if filters comply with the HTTP protocol. Filters written incorrectly do not work.

- To change HTTP header, enter a pattern in the **Patterns** field. Use the following syntax:
  - To add HTTP header

    ```
    EVENT: {
    OP: HEADER_ADD
    HEADER: X-GoogApps-Allowed-Domains
    VALUE: unixlabs.net, unix.com
    }
    ```

  - To remove HTTP header

    ```
    EVENT: {
    OP: HEADER_REMOVE
    ```

```
HEADER: X-GoogApps-Allowed-Domains
}
```

- To modify HTTP header value

```
EVENT: {
        OP: HEADER_MODIFY
        HEADER: cookie
        ORIGINAL_VALUE: [text1]
        FINAL_VALUE: [text2]
}
```

Note: This function only enables HTTP inspection filter action to monitor or Allow (scan).

6. Click **Save**.

Editing an HTTP Inspection Filter

You can modify existing filters or use them as a basis for creating new filters.

If you are editing an HTTP Inspection filter, you may edit:

- Filter name
- Filter description
- Filter methods (Basic view)
- Filter patterns (Advanced view)

You can modify a filter in the basic or advanced view.

To modify a filter:

1. Got to **HTTP > HTTP Inspection > Filters**.
2. Click on the name of the filter to be modified.
3. Change parameters as shown in:
    - To add a new HTTP Inspection filter in the basic view: on page 9-15
    - To add a new HTTP Inspection filter in the advanced view: on page 9-19
4. Click **Save**.

Importing an HTTP Inspection Filter

Two types of HTTP Inspection filters can be imported:

- New filters created by the users in a text file outside of IWSVA
- Custom filters created by Trend Micro support

Filter files are XML files. Imported filter files must conform to a defined standard shown in To create a filter to import: on page 9-24.

To create a filter to import:

1. Imported filter XML files can be created in several ways:
   - Exported from IWSVA
   - Created as a new file
2. If you are creating a new file, use the following sample format:

```
<?xml version="1.0" encoding="UTF-8"?>
<SDF>
    <Filter Mode="Basic" Name="Browser type filter" ID="1">
        <Note>Identifies requests sent from the FireFox browser
according to the
user-agent header</Note>
        <Basic Type="REQ">
            <Headers Enable="true">
                <Header Value="Firefox" Op="M"
Name="User-Agent"/>
            </Headers>
        </Basic>
    </Filter>
    <Filter Mode="Basic" Name="Large data upload filter" ID="3">
        <Note>Identifies large file uploads according to the
content-length header</Note>
        <Basic Type="REQ">
```

```
            <Headers Enable="true">

                <Header Value="1048576" Op="GE"
Name="Content-Length"/>

            </Headers>

        </Basic>

    </Filter>

    <Filter Mode="Basic" Name="Query keyword filter" ID="4">

        <Note>Identifies query keyword for search engine
website, etc.</Note>

        <Basic Type="REQ">

            <Query Enable="true">

                <Value><![CDATA[[put query keywords
here]]]></Value>

            </Query>

        </Basic>

    </Filter>

</SDF>
```

To import a filter:

1. Go to **HTTP > HTTP Inspection > Filters**.
2. Click the **Import** link.
3. Click **Browse** and specify the path and filter to be imported.
4. Click **Import**.
5. View the name of the imported filters in the list of filter names.

Exporting an HTTP Inspection Filter

Existing filters can be exported for several reasons:

- Filters can be used elsewhere
- Custom filters created by Trend Micro support services that can be exported, sent to a customer, and then imported by an IWSVA administrator.

Note: Do not manually edit exported filter files. Changes might prevent them from importing successfully.

To export a filter:

1. Go to **HTTP > HTTP Inspection > Filters**.
2. Check the box of the name or names of files to be exported.
3. Click the **Export** link. (An error message appears if no filter name was selected.)
4. In the **Save As** dialog box, select the location for the file to be save. Use the default file name or change it.
5. Click **Save**.

Data Loss Prevention

Data Loss Prevention (DLP) has been added to IWSVA to provide users the ability to:

- scan outbound traffic for content that includes sensitive corporate data.
- create and modify policies using predefined templates to better meet regulatory privacy requirements in various countries by filtering for personally identifiable information.
- create and modify custom policies using keywords and regular expressions to help filter on intellectual property - as defined by the customer.
- provide reports on which DLP policies have been violated by which users.
- provide auditing functions for administrators to measure the effectiveness (catch rate and false positive rate) of the DLP policies in the product.

Tip: As a best practice, it is strongly recommended to first create a policy that imposes the strictest rules for as many targets (users or endpoints) as possible (such as All

Endpoints or All users), and then create policies for a few endpoints or users as the exception from "All Endpoints" or "All users."

Policies

Use the DLP Policies page to create these across-the-board company rules and criteria that your company's files should meet.

From the DLP Policies page, you can add, edit, delete, or save your company's Data Loss Prevention policy. You can also control whether or not the feature is enabled by clicking the **Enable DLP** checkbox. IWSVA includes the DLP Scan Default Policy that can be modified, but not deleted.

To access the DLP Policies page:

1. Go to **HTTP > Data Loss Prevention > Policies**.

   The Data Loss Prevention Policies page appears.

2. Choose a policy to edit, delete, or if desired, add a new policy. The sections that follow describe the steps necessary.

To modify an Existing DLP Policy:

1. Go to **HTTP > Data Loss Prevention > Policies** and click the name of the desired policy you would like to modify.

   The DLP Policies: Policy page appears.

2. Each policy template is categorized by particular regions or industries that you can choose to Allow, Block, or Monitor.
3. Click the Plus icon to the left of the rule template you would like to enforce.
4. Modify as desired by selecting the rule's checkbox and by using the pull-down, change to the desired behavior and click **Apply**.

   The Action icon will change to the requested status.

To add a new DLP policy:

1. Go to **HTTP > Data Loss Prevention > Policies** and click **Add**.

   The Data Loss Prevention Policies: (New Policy) page appears.

2. Enter the policy name.

3. Enter any useful account information by defining the targets to be protected or monitored. On this page, you can select targets from an IP range or a specific IP address.

Note: These account fields support IPv6 addresses. You can define one rule for any IPv6 host, and this policy rule is triggered when the client sends data violating the company's security policies through IWSVA.

4. Select to target a specific user or an entire group of users. Name the user or group and click **Search**.
5. Click **Next**.

   The Specify Rules page appears.
6. Similar to Editing an Existing Policy, use a defined DLP Template, or modify a policy template categorized by particular regions or industries where you can scan content by selecting target templates that enable you to Allow, Block, or Monitor particular rules.

   The default scan traffic is set for HTTP/HTTPS.
7. Click the Plus icon to the left of the rule template you would like to enforce.
8. Modify as desired by selecting the rule's checkbox and by using the pull-down, change to the desired behavior and click **Apply**.
9. The Action icon will change to the requested status.
10. Fill the remaining page elements.
11. Click **Next**.

    The Specify Exception Lists page appears.
12. Specify the settings for the Approved URL list, the approved file name list, and if you would like to limit the sizes of files, enter the size limitation and click the checkbox.
13. Click **Save**.

Templates

The template page shows all the template defaults as well as any templates customized by the administrators. These templates are displayed by their associated industry or region and include descriptions of each. You can Add, Copy, Delete, Import, or Export templates through this page.

To add a new compliance template:

1. Go to **HTTP > Data Loss Prevention > Templates** and click **Add**.

   The Add Compliance Template page appears.
2. Enter a name and description for the compliance template you are adding.
3. Define each digital asset as either an expression or a keyword.
4. Select predefined expressions or keyword items as "Digital Asset Definition" with a fixed number occurrence or combined with the logic expressions "And"/"Or" in a new Compliance template.
5. Additional digital assets can be added by clicking the plus symbol at the left of the page.
6. Click **Add** to create the new digital asset.
7. Click **Save** to complete.

iDLP

IWSVA 6.5 includes a TMCM 6.0 DLP widget in which company administrators can deploy DLP policies/templates to IWSVA from TMCM 6.0. Administrators can use TMCM 6.0 to manage organization-wide DLP policies for Trend products including IWSVA 6.5.

HTTPS Security

HTTPS (Hypertext Transfer Protocol with Security) is a combination of HTTP with a network security protocol (such as SSL, Secured Sockets Layer). HTTPS connection is used for Web applications (such as online banking) that require secured connections to protect sensitive content. Since traditional security devices are unable to decrypt and inspect this content, virus/malware and other threats embedded in HTTPS traffic can pass unobstructed through your security defenses and on to your enterprise network.

IWSVA closes the HTTPS security loophole by decrypting and inspecting encrypted content. You can define policies to decrypt HTTPS traffic from selected Web categories. While decrypted, data is treated the same way as HTTP traffic to which URL filtering and scanning rules can be applied. In addition, decrypted data is completely secure since it is still in the IWSVA server's memory. Before leaving the IWSVA server, the data is encrypted for secure passage to the client's browser.

IWSVA supports HTTPS decryption and scanning in the following modes:

- Forward proxy
- WCCP
- Transparent bridge
- Reverse proxy

Dangers of Unchecked HTTPS Content

The following lists some major concerns about HTTPS connections:

- Virus scanning and content filtering policies cannot be applied to encrypted data
- Digital certificates can be forged, expired or revoked since clients rarely check the certificate revocation list
- Legitimate certificates can be easily obtained by a malicious third-party, causing users to assume that the information they provide is secure
- Web browsers are vulnerable to certificate insertion attacks that allows a malicious intruder to gain access to a corporate intranet
- Users may not have the required knowledge to decide if a certificate is to be trusted
- Monitoring HTTPS traffic is difficult since the URL path and other information are concealed

SSL Handshake Overview

To use the SSL protocol to establish an HTTPS connection, a Web server needs to install an SSL certificate. Certificates are supplied by a Certificate Authority (CA) and helps determine that a Web site is trustworthy, sensitive information (such as credit card numbers) is encrypted, and data transmitted cannot be tampered with and forged.

When a client initiates an SSL session by typing a URL that starts with https:// instead of http://, an SSL handshake is performed to verify identification (such as certificate exchange and validation) and process encryption methods required for the session. The IWSVA server acts as an intermediary between a client and a secure Web server to validate server certificates. The following describes a simplified SSL handshake process:

1. The client Web browser sends a connection request and its encryption data to the Web server. IWSVA forwards the request to the Web server.
2. The Web server returns its SSL information (including the server certificate). IWSVA checks the server certificate.
3. If the server certificate passes validation tests, the HTTPS connection is allowed between the Web server and the client. IWSVA applies HTTPS decryption policies to scan encrypted content.

   If the Web server requests a client certificate, IWSVA either blocks or tunnels the encrypted traffic.

For more information on server certificate management, refer to Managing Digital Certificates on page 9-93.

HTTPS Decryption and Process Flow in IWSVA

After an HTTPS connection is allowed between the Web server and the client, IWSVA closes the HTTPS security loophole by decrypting and inspecting encrypted content. You can define policies to decrypt HTTPS traffic from selected Web categories. While decrypted, data is treated the same way as HTTP traffic to which URL filtering and scanning rules can be applied.

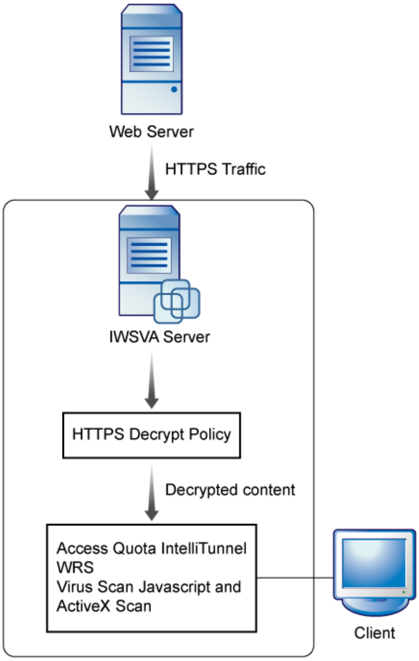


FIGURE 9-5. Decrypted HTTPS traffic flow in IWSVA

The HTTPS decryption feature offers the following benefits:

- Decryption at the gateway—IWSVA is able to decrypt HTTPS traffic and apply existing security policies.
- Data privacy is preserved—Decrypted data is completely secure since it is still in the IWSVA server's memory. Before leaving the IWSVA server, the data is encrypted for secure passage to the client's browser.

- Central certificate handling—IWSVA verifies certificates issued by remote servers and manage certificates to relieve clients of the critical tasks.

Configuring HTTPS Decryption Policies

Before IWSVA can apply scanning and filtering policies on encrypted content, you must configure HTTPS decryption policies to decrypt the content. Similar to the way you configure URL filtering policies, you configure HTTPS encryption policies to decrypt content based on selected Web categories. For example, you can configure an HTTPS decryption policy to decrypt encrypted content from Web sites in the Business categories.

HTTPS decryption and URL filtering policies use the same Web category grouping and naming. You can also configure custom categories to meet the needs of your company or users.

Note: IWSVA only matches the first custom category regardless of whether zero or more than one custom category is selected.

In bridge mode, if a proxy server is located between IWSVA and the Web server and client browsers are configured to access the Internet through the proxy server, IWSVA tunnels or decrypts and scans HTTPS connections based on the policy settings.

HTTPS Accelerator Card Support

For customers that have more than 20-25 percent of their total traffic as HTTPS, IWSVA has drivers that support HTTPS accelerator cards, which can be used for the demanding computational calculations needed for HTTPS and save the general purpose CPU cycles for other IWSVA functions, such as content inspection. The accelerator card is designed to off-load the CPU intensive operations of SSL key pair negotiation, decryption of the HTTPS stream for content inspection, and re-encryption of the content for secure delivery to the client workstation.

IWSVA supports several Silicom cards:

- PCI-E 61
- PCI-X 51
- PESC62

Using the accelerator card allows systems to off-load high-level SSL or IPsec protocol commands that reduce the host I/O traffic and system processor to increase the total system throughput. This also frees system processor resources for other functions, increasing overall system performance.

Enabling HTTPS Decryption

To enable HTTPS Decryption:

1. Click **HTTP** > **HTTPS Decryption** > **Policies**.
2. Select **Enable HTTPS Decryption**.
3. Click **Save**.
4. Click **Deploy Policies**.

Creating a New HTTPS Decryption Policy

Creating a new HTTPS decryption policy is a three-step process:

- Select the accounts to which the policy applies
- Specify the Web site categories whose traffic you want to decrypt
- Select an exception list

To enable HTTPS decryption:

1. Click **HTTP > HTTPS Decryption > Policies** from the main menu.
2. Select **Enable HTTPS Decryption**.
3. Click **Save**.

To create a new HTTPS decryption policy:

1. Open the IWSVA Web console and click **HTTP > HTTPS Decryption > Policies** from the main menu.

   Click **Add**. The **HTTPS Decryption Policy: Add Policy** screen appears.
2. Type a descriptive policy name in the "Create new policy" box.

Policy names that include references to the users or groups to which they apply, for example, "HTTPS decryption policy for Web Mail," are easier to remember.

3. Select the users to which the policy applies.

   The options on this page depend upon the user identification method that you are using—either *IP address*, *Host name (modified HTTP headers),* or *User/group name authentication (LDAP)*. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method starting on page 8-6.

4. Click **Next**.

5. On the **Specify Categories** screen, ensure that **Enable policy** is selected.

6. Select the URL categories to decrypt.

   To select all the categories of a group, click **Select All** for the group. The group does not need to be expanded for you to select all categories in a group.

7. Type an optional **Note** to include useful information about this policy for future reference.

8. Click **Next**.

9. If you want to apply an exception list, in the **Specify Exception Lists** screen, select an approved HTTPS URL list name from the drop down list box. IWSVA tunnels HTTPS traffic from a URL in the exception list; that is, the encrypted content will not be decrypted for inspection.

10. Click **Save**.

11. In the **HTTPS Decryption Policies** screen, set the priority of the new policy (under the **Priority** column) by clicking the up or down arrow.

    The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies.

12. Click **Save**.

13. To immediately apply the policy, click **Deploy Policies**; otherwise, the policy is applied after the database cache expires.

WARNING! **In proxy mode, IWSVA applies HTTPS decryption policies based on the client's browser domain. However in transparency mode, since IWSVA is unable to obtain client domain information, IWSVA applies HTTPS decryption policies to the CommonName in the server certificate.**

HTTPS Decryption Settings

Click **HTTP > HTTPS Decryption > Settings** to configure the following:

- Server certificate validation
- Client certificate handling
- Certificate authority

Server Certificate Validation

In the Server Certificate Validation screen, enable server certificate validation and configure validation settings to automate certificate tests such as querying certificate revocation list and establishing certificate validity.

Note: If you disable certificate validation, clients can access any HTTPS Web sites without checking server certificates.

If a certificate does not pass a certificate validation test, clients can still choose to access a Web site through HTTPS connection. A warning screen displays on the client's browser.

To configure server certificate validation:

1. From the main menu, click **HTTP > HTTPS Decryption > Settings**. The Server Certificate Validation screen displays.
2. Select **Enable Certificate Verification** to check server certificates.
3. Select one or more of the following options:
   - **Deny Certificates where the CommonName does not match the URL**—Select this option to deny a certificate if the CommonName does match the accessed URL. IWSVA treats the certificate as invalid.
     - **Allow Wildcard-Certificates**—Select this option to allow and verify certificates whose CommonName is represented by a wildcard. Disable this option to deny any certificate with a CommonName expressed using wildcards.
   - **Deny expired or wrong purpose certificates**—Select this option to deny certificates that are expired or certificates that cannot be used for the intended purpose.

- **Verify entire certificate chain**—Select this option to ensure that a given certificate chain (from the supplied certificate to the root Certificate Authority's certificate) is valid and trustworthy.
- **Certificate revocation check by CRL**—Select this option to check whether a certificate is revoked (becomes invalid) by looking up the Certificate Revocation List (CRL).

4. Click **Save**.

Certificate Verification Exception

You can add exceptions to server certificates to let IWSVA take certain pre-defined action when the certificate of the target Web site fails to pass the verification.

There are two types of exception items:

- CERT type: when certificate verify fails in HTTPS traffic, (for example: the certificate of the web sites expires); IWSVA will add a CERT type exception item automatically for this certificate with "Warning" action.

  You can just change and action and description for this type of exception item.
- URL type: you can add a URL type exception item by clicking Add button on this screen.

Client Certificate Handling

For many high-security applications, such as online banking, the Web server may require client certificates to authenticate the clients. Since IWSVA does not support Web sites that require client certificates, you can select to tunnel or block the connection in the Client Certificate Handling screen.

- **Tunnel**—Select this option to bypass HTTPS traffic. IWSVA will not decrypt the content for inspection.
- **Block**—Select this option to deny access to the remote server.

Certificate Authority

By default, IWSVA acts as a private Certificate Authority (CA) and dynamically generates digital certificates that are sent to client browsers to complete a secure session for HTTPS connections. However, the default CA is not signed by a trusted CA on the

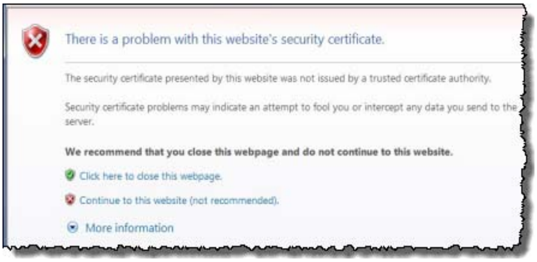
Internet and the client browsers will display a certificate warning each time users access an HTTPS Web site. Although users can safely ignore the certificate warning, Trend Micro recommends using your own certificate for IWSVA.

To import a CA certificate:

1. From the main menu, click **HTTP > HTTPS Decryption > Settings | Certificate Authority**.
2. Click **Browse** next to **Certificate** to select a certificate file. IWSVA supports certificates using Base64-encoded certificate and RSA-based encrypted private key in PEM file format.
3. Click **Browse** next to **Private Key** to select the private key associated with the CA certificate.
4. Type the **Passphrase** for the private key.
5. Type the passphrase again the **Confirm passphrase** field.
6. Click **Import CA.**

Note: IWSVA supports certificates using Base64-encoded certificate and RSA-based encrypted private key in PEM file format only.

After importing a CA certificate, a certificate warning screen (*Figure 9-6*) may display on the end users machines, if they attempt to access a secured Web site. To avoid this behavior, add the related certificates to the Trusted Root Certificates Authorities list in the appropriate Web browser. See *Figure 9-7* for details.



There is a problem with this website's security certificate.

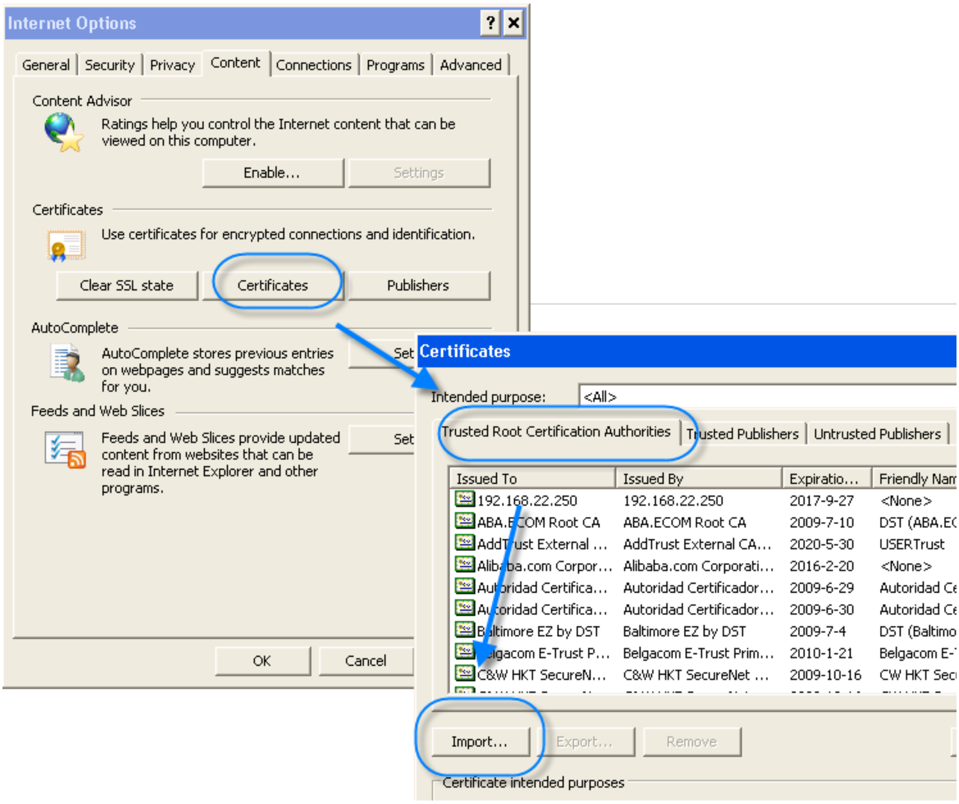
The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

FIGURE 9-6. Certificate Warning Screen



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

Issued To	Issued By	Expiratio...	Friendly Nam
192.168.22.250	192.168.22.250	2017-9-27	<None>
ABA.ECOM Root CA	ABA.ECOM Root CA	2009-7-10	DST (ABA.EC
AddTrust External ...	AddTrust External CA...	2020-5-30	USERTrust
Alibaba.com Corpor...	Alibaba.com Corporati...	2016-2-20	<None>
Autoridad Certifica...	Autoridad Certificador...	2009-6-29	Autoridad Ce
Autoridad Certifica...	Autoridad Certificador...	2009-6-30	Autoridad Ce
Baltimore EZ by DST	Baltimore EZ by DST	2009-7-4	DST (Baltimo
Belgacom E-Trust P...	Belgacom E-Trust Prim...	2010-1-21	Belgacom E-
C&W HKT SecureN...	C&W HKT SecureNet ...	2009-10-16	CW HKT Sec

FIGURE 9-7. Add a certificate to Trusted Root Certificate Authorities

To export a CA certificate (public key):

1. From the main menu, click **HTTP > HTTPS Decryption > Settings | Certificate Authority**.
2. Click **Export Public CA Key**.
3. Follow the on-screen prompt to save the certificate file on your computer.

To export CA private key:

1. From the main menu, click **HTTP > HTTPS Decryption > Settings | Certificate Authority**.
2. Click **Export Private CA Key**.
3. Follow the on-screen prompt to save the key file on your computer.

TLS/SSL Protocols

About TLS/SSL

IWSVA can use Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to help ensure secure communication between the web console and the server.

TLS and its predecessor, SSL, are cryptographic protocols. These protocols help to secure communication between a web console and a server by using long-term, asymmetric public keys to authenticate each side. Once authenticated, these protocols allow the sides to create short-term, symmetric secret keys used to encrypt communication between the sides during the session. It is not possible to use the public keys to reverse-engineer the secret keys.

To perform authentication, TLS and SSL protocols use X.509 certificates and asymmetric cryptography. Supporting X.509 certificates requires a certificate authority (CA) and public key infrastructure to do the following:

- Generate, sign, and validate certificates
- Verify the relationship between certificates and sides

Specifying TLS/SSL Methods

To specify TLS/SSL methods:

1. Go to **HTTP > HTTPS Decryption > Settings > SSL Method**.
2. Select one or more options under the **Client SSL Method** and the **Server SSL Method** sections.

Domain Tunneling

HTTPS Tunnels can be used to communicate between network locations with restricted connectivity – usually being locations behind NATs, firewalls, or proxy servers. Restricted connectivity is usually the result of blocked TCP/IP ports, blocked traffic initiated from outside the network, or from the blocking of most network protocols is how a network can be locked down to secure it against internal and external threats.

Similar to a global trusted list, domain tunneling allows administrators to maintain a list of trusted sites.

To set up domain tunneling:

1. Go to **HTTPS** > **HTTPS Decryption** > **Tunneling**.
2. Enter the domain name match to be added.
3. Select to match by a string (exact name) or to match by an entire domain. (An asterisk will appear next to tunnels made through entire domains.)
4. If you have a previously created file with approved entries already included, click **Choose File**, select the file you want to add, then click **Import**.

   The Tunneled Domains you add will appear in the Tunneled Domains box.
5. Click Save.

Tunneled Domains

Obsolete tunnels can be deleted by highlighting the tunnelled domain and clicking **Remove**, or clear the entire list by clicking **Remove all**. You can also save your list of tunnelled domains by clicking **Export** and saving the list to a secure location.

Exceptions to the Tunneled Domains

Exceptions can be listed as well. All domains in the exception list will be decrypted.

Failed HTTPS Accesses

Failed HTTPS access attempts can be tracked and recorded. Administrators can add a tunneled domain into a tunnel list for site surfing. Logs can be queried based on time, user name and domain.

In the Action column, a button is provided to add the domain name into the tunneling list. If the domain is already in the list, the column space will read "Tunneled."

To search for failed HTTPS Access attempts:

1. Go to **HTTPS > HTTPS Decryption > Tunneling - Failed HTTPS Accesses**.
2. Select the option to Enable Auto Tunneling for Fatal Failures if you would like to initiate auto-tunneling.
3. Choose the number of failed HTTPS accesses you would to review, 20, 50 or 100 entries.
4. To search for a specific user's attempted access, enter the user name in the Search box as well as the user's Domain.

For each entry, the following information is shown:

- Date
- User Name (user or IP)
- Domain Name
- Failure Reason
- Action

The Action column will reveal a button for you to add the domain name into your tunneling list. If the domain is already in the list, the Action will show "tunneled" instead.

Creating and Modifying Advanced Threat Protection Policies

In addition to the default global and guest policies, you can create customized HTTP scanning policies for specified members of your organization.

To create a new virus scan policy:

1. Choose **HTTP > Advanced Threat Protection > Policies** from the main menu.
2. Select **Enable virus scanning** to enable virus scanning.
3. Select **Enable Advanced Threat Scan Engine** to enable the Advanced Threat scan engine.
4. Select **Enable Web Reputation** to enable Web Reputation.

Note: Web Reputation must be enabled at the global level to be used at the policy level.

5. Select **Enable Bot Detection** to enable Bot Detection.
6. Click **Add**.
7. Type a descriptive **policy name** in the "Create new policy" field.

   Policy names that include references to the users or groups to which they apply (for example, "Virus Policy for Engineers" or "URL Filtering Policy for Researchers") are easy to remember.

   Account fields should support IPv6 addresses. You can define one rule for any IPv6 host, and this policy rule is triggered when the client accesses the HTTP sites through IWSVA.

   When selecting available policies, both IPv4 and IPv6 policies will appear. In the Account field, acceptable account entries include a single IPv6 address, an IPv6 range, or an IPv6 mask similar to what has been supported with IPv4.

   IWSVA supports the "Scan before delivering" feature with IPv6, and can automatically redirect the progress of IWSVA IPv6 or IPv4 addresses to the client based on the version of the client's IP address.

   - When a client uses an IPv4 address, IWSVA sends a redirect request with IWSVA's IPv4 address.
   - When a client uses an IPv6 address, IWSVA sends a redirect request with IWSVA's IPv6 address.
8. Select the users to which this policy applies.

   The options on this page depend upon the user identification method that you are using—either **IP address**, **Host name (modified HTTP headers)**, **IP Subsets**, or **User/group name authentication**. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method starting on page 8-6.

   Note: Regardless of the user identification method you have configured, you can always enter IP addresses of the clients to which the policy applies.

9. When you have named your new policy and defined the account(s) to which it applies, click **Next** to proceed with defining HTTP virus scanning rules.

To modify an existing Advanced Threat Protection policy:

1. Click **HTTP > Advanced Threat Protection > Policies** from the main menu.
2. Click the name of the policy to modify.
3. Modify the Web Reputation rule, virus scanning rule, bot detection rule, the spyware scanning rule, policy exceptions, and the scanning action.

   The specified scanning action applies to all specified rules.

To add or remove users from an existing Advanced Threat Protection policy:

1. Click **HTTP > Advanced Threat Protection > Policies** from the main menu.
2. Click the desired scan policy account.
3. From the **HTTP Scan Policies: Edit** screen, on the **Account** tab, either add or remove a user.
   - To add a user, specify an IP address, a range of IP addresses, an IP subset, or a user/group name to signify the users affected.
   - To remove a user, click the trash can icon next to the user.

To enable a HTTP scanning policy:

- To enable a HTTP scanning policy at the global level
  Click **HTTP > HTTP Malware Scan > Policies** and select **Enable virus scanning**.
- To enable a HTTP scanning policy at the policy level
  Click **HTTP > HTTP Malware Scan > Policies**, click a policy that you added, and select **Enable policy**.

Specifying Web Reputation Rules

Web Reputation rules are created at the policy level.

To specify Web Reputation rules:

1. Ensure that Web Reputation is enabled at the global level.

   Web Reputation must be enabled at the global level to use it at the policy level (**HTTP > Advanced Threat Protection > Policies | Enable Web Reputation** checkbox).
2. Ensure that Web Reputation is enabled at the policy level.

Using the **Add** or **Edit** option for the **HTTP > Advanced Threat Protection > Policies | Web Reputation Rules** page, ensure that the **Use Web Reputation rule in this policy** check box is selected. This check box is selected by default.

3. Specify the URL blocking sensitivity level.

Upon receiving the Web Reputation score, IWSVA determines whether the score is above or below the threshold. The threshold is defined by sensitivity level as configured by the user. Medium is the default sensitivity setting. This setting is recommended because it blocks most Web threats while not creating many false positives.

4. Either accept or disable the anti-pharming, anti-phishing, and C&C contact detections.

By default, all detections are enabled. See Anti-phishing, Anti-pharming, and C&C Callback Attempt Detection on page 9-45.

Anti-phishing, Anti-pharming, and C&C Callback Attempt Detection

Phishing attacks are emails designed to steal private information from you. These emails contain URLs which direct you to imposter Web sites where you are prompted to update private information, such as passwords and credit card numbers, social security number, and bank account numbers.

Pharming attacks are attempts to redirect you to imposter Web sites with the intention of stealing private information, which is usually financially related. Pharming compromises a DNS server by planting false information into the server, which causes a user's request to be redirected to an unintended location. Unfortunately, the Web browser displays what appears to be the correct Web site.

Note: Because the source of anti-phishing/pharming detection is Web Reputation and it is part of the Web Reputation Rule for a policy, anti-phishing/pharming is also disabled when Web Reputation is disabled globally.

In ICAP mode, IWSVA does not support anti-pharming.

Command and control callback attempt detection (C&C Callback) attacks are systems attempting to detect botnets by examining traffic content for IRC commands or by setting up honeynets.

Custom Defense Settings

You can integrate IWSVA with the Deep Discovery Advisor/Deep Discovery Analyzer (DDA/DDAN) sandbox to defend against offline custom-defense APT attacks from malicious programs through HTTP/HTTPs traffic.

ATSE engines can be used to scan for viruses and suspicious files. This engine is more aggressive than VSAPI engines. It can apply APT custom defense rules that can be configured in Custom Defense to identify APT detection. You can configure Custom Defense Settings at **HTTP** > **Advanced Threat Protection** > **Custom Defense** on the Web console.

Enable Custom Defense

Click this check box to enable or disable IWSVA integration with the DDA/DDAN server. If the DDA/DDAN server is not recognized, IWSVA cannot save the settings.

Virtual Analyzer Server

Enter the IP address, port, and API key of the Virtual Analyzer server. Click **Test Connection** to confirm proper integration.

Sample Submission

Select the threat or file types that you want to submit to Deep Discovery Advisor (DDA)/Deep Discovery Analyzer (DDAN) to scan for threats.

Actions

Select based on the types of threats you would like to block or monitor. Save your changes.

Web Reputation Settings

Web Reputation settings involve specifying the following:

- Whether to provide feedback on infected URLs to Trend Micro
- Whether to evaluate Web Reputation in a monitoring only mode (no URLs are blocked)

Enabling and Disabling Web Reputation

IWSVA allows you to enable or disable Web Reputation at the global level and at the policy level. If you disable Web Reputation at the global level, then it is automatically disabled at the policy level.

To enable and disable Web Reputation at the global level:

1. Click **HTTP > Advanced Threat Protection > Policies > Virus Scan Global Policy** and click the Web Reputation Rule tab.
2. From the Web Reputation Rules screen, select **Use Web Reputation rule in this policy** to enable Web Reputation. Clear the checkbox to disable it.

To enable and disable Web Reputation at the policy level:

1. Click **HTTP > Advanced Threat Protection > Policies > policy name** and click the **Web Reputation Rule** tab.
2. Select **Use Web Reputation rule in this policy** to enable Web Reputation or clear the check box to disable it for this policy.

Managing Web Reputation Results

IWSVA provides two options for managing Web Reputation results:

- **Feedback Option**: to provide feedback on infected URLs to help improve the Web Reputation database.
- **Monitor Only Option**: to monitor the effectiveness of Web Reputation without affecting existing Web-access policies.

You can configure one or all of the options available.

To set this option, click **HTTP > Advanced Threat Protection > Settings** in the web console.

To configure Managing Web Reputation, navigate to **HTTP** > **Advanced Threat Protection** > **Settings** on the Web console.

Feedback Option

In addition to the current dynamic URL Blocking List, virus scan results can be fed back to the URL Local Cache and an external backend Rating Server. The Trend Micro Feedback Engine (TMFBE) provides a feedback mechanism for IWSVA to send back virus scan results to the backend Rating Server. The Feedback option is enabled by default. To disable it go to **HTTP** > **Advanced Threat Protection** > **Settings** and uncheck **Send feedback on infected URLs to Trend Micro** under **Feedback Option**.

Note: When using Upstream Proxy mode, you might need to configure the proxy server to explicitly allow the IWSVA IP address to access www.trendmicro.com.

Negative Results

If the scan result from the Trend Micro virus scanning engine is negative, the infected URL is sent back to the following locations:

- Dynamic URL Blocking List
- URL Local Cache with an adjusted Web Reputation score
- TMFBE feedback buffer with VirusName and IntelliTrap Flag. When this buffer reaches ten entries or five minutes have passed from the last feedback, these URLs are sent to the backend Rating Server in a batch (each URL is sent sequentially).

Positive Results

If the scan result from Trend Micro's virus scanning engine is positive, the URL in question is saved in the URL local cache. This prevents the same URL from getting scanned by Trend Micro's virus scanning engine twice.

Monitor Only Option

The Monitor Only option gives you the opportunity to evaluate Web Reputation results. With this option selected, you are able to monitor Web Reputation results from the URL Blocking Log or Security Risk Report. The results only include the URLs filtered by Web Reputation, anti-phishing and anti-pharming. Because you are only monitoring Web Reputation results, no URL blocking occurs and URLs are passed to clients.

By default, the Monitor Only option is disabled.

Clearing the WRS/URL Cache

When a user attempts to access a URL, IWSVA retrieves information about this URL from a remote database—the Web Reputation database—and stores the retrieved information in a local WRS/URL cache. Having the Web Reputation database on a remote server and building the local WRS/URL cache with this database information reduces the overhead on IWSVA and improves performance.

The following are the information types the WRS/URL cache can receive from the Web Reputation database for a requested URL:

- Web category
- Pharming and phishing flags used by anti-pharming and anti-phishing detection
- Web Reputation rating results used to determine whether or not to block a URL (see Specifying Web Reputation Rules on page 9-44)

The URL cache keeps frequently accessed URLs in cache for quick retrieval. Clear the cache only if a new URL query is necessary or if the cache size is affecting performance.

Note: Clearing the cache stops and restarts the HTTP scanning daemon, which may interrupt IWSVA service.

To clear the WRS/URL cache:

1. From the main menu, click **HTTP > Configuration > WRS/URL Cache**.
2. Click **Clear Cache**.

Using the Content Cache

Note: The Content Cache feature is not available in a Cluster Configuration Replication (CCR) cluster where content cache is disabled on the CCR receiver, even if the CCR receiver obtains the content cache configuration from the CCR source.

Web content caching is the caching of Web objects (such as HTML pages and images) to reduce bandwidth usage, server load, and perceived lag. A Web cache stores copies of objects passing through it. Subsequent duplicate requests may be satisfied from the cache if certain conditions are met. Cached objects will be re-scanned by IWSVA.

The Content Cache capability provides users who access the Web through IWSVA with a quicker experience while saving bandwidth.

Note: This feature is available in Forward Proxy and WCCP modes. The Content Cache feature is grayed out and will not function in other modes.

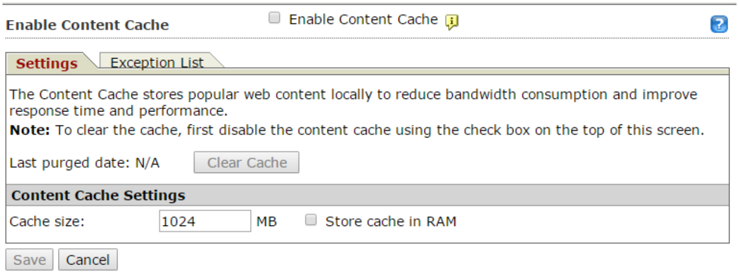
With the Content Cache feature, administrators enable or disable the IWSVA in-box cache and manage caching through the Web console.

Note: The Content Cache feature cannot be disabled from the CLI.

Enabling/Disabling the Content Cache

To enable/disable the Content Cache feature:

1. Go to **HTTP > Configuration > Content Cache**.
2. Select the **Enable Content Cache** check box at the top of the page to enable the Content Cache feature. (See *Figure 9-8*.)
3. Click **Save**.
4. Clear the **Enable Content Cache** check box to disable the Content Cache feature.
5. Click **Save**.



Enable Content Cache □ Enable Content Cache

The Content Cache stores popular web content locally to reduce bandwidth consumption and improve response time and performance.

Note: To clear the cache, first disable the content cache using the check box on the top of this screen.

Last purged date: N/A

Content Cache Settings

Cache size: 1024 MB □ Store cache in RAM

FIGURE 9-8. Content Cache screen

Clearing the Content Cache

To clear the Content Cache:

1. Click **Clear Cache**. You receive the following warning:

   "It could take a significant amount of time to clear a large cache.

   Are you sure you want to clear the cache?"

2. Click **OK**. A progress bar displays during the cache clearing process.

   The Clear Cache button and the Enable Content Cache checkbox are both disabled until the clearing process ends. After the cache clears, the "Last purged date" updates.

Managing the Content Cache

Administrators can configure the following content cache areas:

- Hard disk usage for the Content Cache
- RAM usage for the Content Cache

To manage the Content Cache:

1. Go to the **Content Cache Settings** section of the Content Cache Settings tab.
2. Set the **Cache size** field. (See *Figure 9-8*.)

   Administrators can adjust the amount of disk space or RAM used to store the cached content. A larger cache volume will allow more Web objects to be cached. A smaller cache partition will reduce the number of cacheable objects. If you set the cache volume too small and run out of disk space for caching, the hit ratio may decrease as IWSVA will rely more on real-time content retrieval and less on locally cached content.

   Enter the available cache size based on your IWSVA settings.
3. Enable cache to be stored in RAM by checking the **Store cache in RAM** checkbox.

Note: If the **Store cache in RAM** checkbox is not selected, content cache is stored in the `/var/cache/trafficserver/` folder.

4. Click **Save**.

Content Cache Exception List

When administrators do not want to cache a specific URL, they can add the URL to the cache exceptions list. The behavior here is the same as the URL blocking list. Administrators can add a web site, URL keyword, or string to exceptions list. URLs that match the list will not be cached by IWSVA.

You can have IWSVA block certain Web pages, domains, and URLs from being stored in the content cache. URLs blocked from the Content Cache are not policy based—it affects everyone in the organization.

Note: Content caching is supported in Forward Proxy and WCCP modes.

Blocking URLs from the Content Cache combats large Web sites from being cached and taking up cache space that is more efficiently used for other common Web sites.

- **Enable Content Cache**—Enable or disable Content Cache (click Save after enabling or disabling content caching).
- **Match**—Enter an exact Web site, a keyword or phrase, or a string of characters in the field, and then configure IWSVA with how to apply the match.
- **Web site**—Limits the search to the string as a whole. This type of blocking can be especially useful for preventing entire Web sites from being cached. There is no need to include http:// or https:// in the URL (as it is automatically stripped).
- **URL keyword**—Looks for any occurrence of the letters or numbers within a URL, and will match regardless of where the string is found (the string "sex" would be considered a match for "http://www.encyclopedia/content/sexton.htm") and the page blocked.
- **String**—Limits the search to the string as a whole; for example, to target a specific site, page, file, or other particular item.
- **Import Blocked Content Cache List and Exception**s—You can import an existing list of URLs that you want to block or exempt from content caching. For example, if you have a list of URLs from a third-party vendor, Web Manager, or related software program, or a list of sites you have compiled using a text editor, you can import the list rather than enter them one-by-one in the Match field. Imported lists must conform to a defined standard.

Content Cache Exceptions List Format

The Content Cache exception list uses the following format to import exception lists.

```
[no_cache]
@www.example1.com*
www.example2.com/c.jgp
*example3*
```

HTTP Virus Scanning Rules

IWSVA administrators can configure which file types to block and scan, and how compressed and large files are handled.

See **HTTP > Advanced Threat Protection > Policies | policy name** on the **Virus/Malware Scan Rule** tab.

Advanced Threat Scan

Select to monitor or block threats during scans.

Specifying File Types to Block

You can identify the types of files to block for security, monitoring, or performance purposes. Blocked files are not received by the requesting client or scanned—requests to retrieve a blocked file type are not executed. You have the option of blocking file types such as Microsoft Office documents, images, executables, audio/video files, Java applets, archives, or other files types that you specify.

To specify which file types to block:

1. While adding or editing a policy, under **Virus/Malware Scan Rule** > **Block These File Types**, check the box of the file types to block. This will block all files in that category.
2. To choose to unblock file types within a selected category, click the Show Details link.
3. Uncheck the files that should not be blocked.

Specifying File Types to Scan

IWSVA is equipped with the following HTTP scanning capabilities:

- All scannable files
- IntelliScan
- Specified file extensions
- IntelliTrap

Note: For the highest level of security, Trend Micro recommends scanning *all* files.

About IntelliScan

Most antivirus solutions today offer you two options to determine which files to scan for potential risks. Either all files are scanned (the safest approach), or only those files with certain file extensions considered the most vulnerable to infection are scanned. However, recent developments that disguise files by changing their extensions renders this latter option less effective. *IntelliScan* is a Trend Micro technology that identifies a file's "true-file type," regardless of the file name extension.

Note: IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible to virus infection.

About True-file Type

When set to scan *true*-file type, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named `family.gif`, it will not accept that the file is a graphic file and skip scanning. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that has been deceptively named to avoid detection.

True-file type scanning works in conjunction with Trend Micro IntelliScan, to scan only those file types known to be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but it comes at the cost of potentially higher risk.

For example, .GIF and .JPG files make up a large volume of all Web traffic. It is possible for a malicious hacker to give a harmful file a "safe" file name to smuggle it past the scan engine and onto the network. The file could not run until it was renamed, but IntelliScan would not stop the code from entering the network.

To select which file types to scan:

IWSVA can scan all files that pass through it, or just a subset of those files as determined by true-file type checking (IntelliScan) or the file extension. In addition, individual files contained within a compressed file can also be scanned.

1. Select the files to scan:
   - To scan all file types, regardless of file name extension, select **All scannable files**. IWSVA opens compressed files and scans all files within. This is the most secure, and recommended, configuration.
   - To use true-file type identification, select **IntelliScan**. This configuration scans file types that are known to harbor viruses by checking the file's true-file type. Because checking the true-file type is independent of the filename's extension, it prevents a potentially harmful file from having its extension changed to obscure its true-file type.
   - You can explicitly configure the types of files to scan or skip, based on their extensions, to work around possible performance issues with scanning all HTTP traffic. However, this configuration is not recommended because the file extension is not a reliable means of determining its content.

     To scan only selected file types, select **Specified file extensions** and then click the list. (Trend Micro does not recommend this setting.) The **Scan Specified Files by Extension** screen opens. The default extensions list shows all file types that are known to potentially harbor viruses. This list is updated with each virus pattern file release. On the **Scan Specified Files by Extension** screen, add or exclude additional extensions in the **Additional Extensions** and **Extensions to Include** fields.

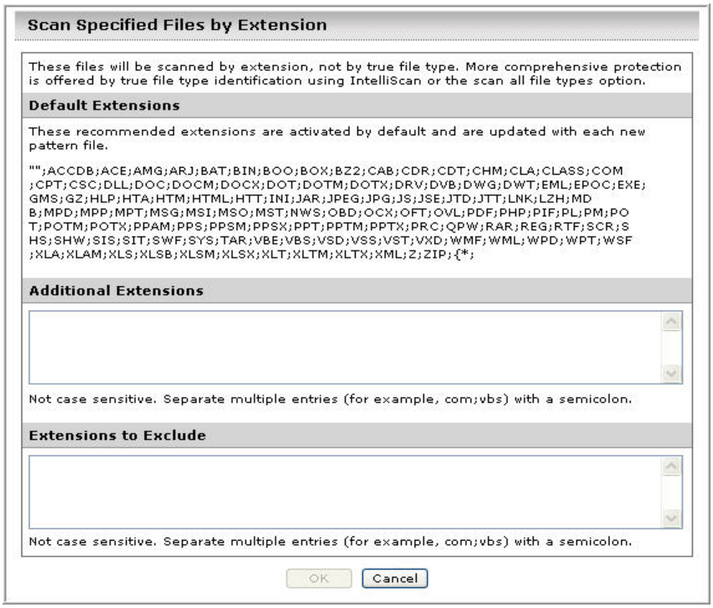
     Enter the extension to scan or exclude from scanning (typically three characters), without the period character. Do not precede an extension with a wildcard (*) character, and separate multiple entries with a semicolon.

     Click **OK** when you are finished. The screen closes.
2. You can configure IWSVA to selectively bypass certain MIME content-types. Some file types, such as RealAudio or other streaming content, begin playing as soon as the first part of the file reaches the client machine and does not work properly with

the resulting delay. You can have IWSVA omit these file types from scanning by adding the appropriate MIME types to the **MIME content-types to skip** list on the **Virus Scan Rule** tab. Type the MIME content-type to bypass in the **MIME content-type to skip** field (for example, image, audio, application/x-director video, and application/pdf). See Appendix B, *Mapping File Types to MIME Content-types* for more information.

You can also enable the **Enable MIME type validation** check box to allow true file type scanning. This option enables a true file type check on the MIME stream. However, not all MIME types can be accurately detected. If false positives occur, disable Mime Type Validation and Content Type will be used instead.

Note: Trend Micro recommends minimizing the list of MIME content-types to skip to reduce the risk of virus infection. Also, Trend Micro does not recommend skipping any MIME content-types when large file handling is enabled, because it's possible for a MIME content-type to be forged.



Scan Specified Files by Extension

These files will be scanned by extension, not by true file type. More comprehensive protection is offered by true file type identification using IntelliScan or the scan all file types option.

Default Extensions

These recommended extensions are activated by default and are updated with each new pattern file.

""";ACCDB;ACE;AMG;ARJ;BAT;BIN;BOO;BOX;BZ2;CAB;CDR;CDT;CHM;CLA;CLASS;COM
;CPT;CSC;DLL;DOC;DOCM;DOCX;DOT;DOTM;DOTX;DRV;DVB;DWG;DWT;EML;EPOC;EXE;
GMS;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;JPG;JS;JSE;JTD;JTT;LNK;LZH;MD
B;MPD;MPP;MPT;MSG;MSI;MSO;MST;NWS;OBD;OCX;OFT;OVL;PDF;PHP;PIF;PL;PM;PO
T;POTM;POTX;PPAM;PPS;PPSM;PPSX;PPT;PPTM;PPTX;PRC;QPW;RAR;REG;RTF;SCR;S
HS;SHW;SIS;SIT;SWF;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WMF;WML;WPD;WPT;WSF
;XLA;XLAM;XLS;XLSB;XLSM;XLSX;XLT;XLTM;XLTX;XML;Z;ZIP;{*;

Additional Extensions

Not case sensitive. Separate multiple entries (for example, com;vbs) with a semicolon.

Extensions to Exclude

Not case sensitive. Separate multiple entries (for example, com;vbs) with a semicolon.

FIGURE 9-9. **The Recommended Extensions to Scan are Updated with Each New Pattern File**

About IntelliTrap

IntelliTrap detects potentially malicious code in real-time, compressed executable files that arrive with HTTP data. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus compressed using these methods enters a network through the Web.

IntelliTrap has the following options:

- Can be enabled or disabled in the **Virus Scan Rule** tab for each scan policy. (IntelliTrap is enabled by default.)
- Malicious, compressed executable files receive the actions specified in the Action tab.

To enable / disable IntelliTrap:

- Click **HTTP > Advanced Threat Protection > Policies | <policy name>| Virus/Malware Scan Rule tab** and select the **Enable IntelliTrap** check box in the IntelliTrap section.

For more IntelliTrap information, see IntelliTrap Pattern and IntelliTrap Exception Pattern Files on page 4-8.

Priority for Virus/Malware Scan Configuration

IWSVA scans according to the following priority:

1. File types to block
2. MIME content-types to skip
3. File types to scan

Configuring Compressed File Scanning Limits

Compressed file scanning limits can be configured for each policy (click **HTTP > Advanced Threat Protection > Policies > policy** and click the **Virus/Malware Scan Rule** tab). IWSVA opens and examines the contents of compressed files according to the criteria specified in the HTTP virus scanning configuration screen. IWSVA decompresses the files according to the configurable limits (number of files in the compressed archive, size of the compressed file, number of compressed layers, and the compression ratio).

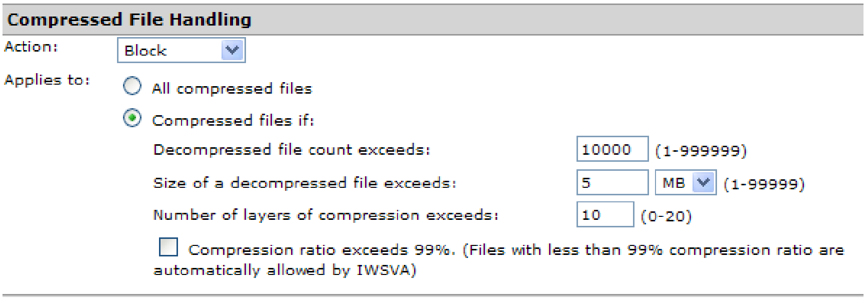
To configure the compressed file scanning limits:

Under **Compressed File Handling**, configure the following settings:

- **Action**: Select an action (**Pass**, **Block**, or **Quarantine**) you want IWSVA to take when it detects a compressed file violation.
- **Applies to**: Select one of the following options.
    - **All compressed files**: Match all requests to download compressed files.

- **Compressed files if...**: Match only requests to download compressed files that exceed the configured criteria. Type values for the following parameters:
    - Decompressed file count exceeds (default is 50000)
    - Size of a decompressed file exceeds (default is 200MB)
    - Number of layers of compression exceeds (range is 0-20; default is 10). If you type "0" in this field, the system uses the maximum of 20 compression layers.
    - Enable/disable when compression ratio exceeds 99% (default is disabled)

IWSVA applies the selected action on a compressed file that meets the specified conditions at the gateway and the file is not scanned. For example, suppose your settings appear as shown in *Figure 9-10*:



Compressed File Handling

Action: Block

Applies to:

○ All compressed files

● Compressed files if:

Decompressed file count exceeds: 10000 (1-999999)

Size of a decompressed file exceeds: 5 MB (1-99999)

Number of layers of compression exceeds: 10 (0-20)

□ Compression ratio exceeds 99%. (Files with less than 99% compression ratio are automatically allowed by IWSVA)

FIGURE 9-10. "Decompression percent" can be used to prevent a denial-of-service (DoS) attack against the IWSVA device

A compressed file that has more than 10 layers of compression or contains more than 10000 files that will not pass through the gateway.

Handling Large Files

For larger files, a trade-off must be made between the user's experience and expectations, and maintaining security. The nature of virus scanning requires doubling the download time (that is, the time transferring the entire file to IWSVA, scanning the file, and then transferring the entire file to the client) for large files. In some environments, the doubling of download time might not be acceptable. There are other factors such as network speed, and server capability that must be considered. If the file is not big enough to trigger large-file handling, the file is scanned as a normal file.

Consider configuring large file handling if your users experience browser time-outs when trying to download files. There are two large file scanning options:

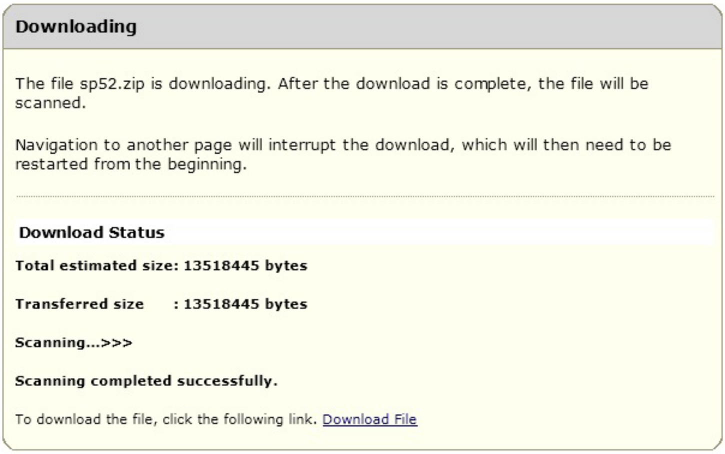
- Scan Before Delivering (Progress Page) on page 9-60
- Deferred Scanning on page 9-62

Scan Before Delivering (Progress Page)

When IWSVA is configured to use the **Scan before delivering** scanning option, requested files are not passed to the client until scanning is finished. A progress page is generated during the scan process to prevent the browser from timing out and to inform the user that scanning is in progress.

Note: For large file handling, IWSVA uses the progress page. The progress page uses JavaScript and a pop-up window to display the download progress. If your desktop security policy has pop-up blocking enabled or JavaScript disabled, then the progress page does not function and scanning is prevented.

For the progress page to work, IWSVA needs to determine to which externally visible IP address the clients connect. Using 127.0.0.1 causes a problem. If a message about the progress page appears, add the machine IP address to `iscan_web_server` so that the host name does not resolve to 127.0.0.1 (for example, `iscan_web_server=1.2.3.4:1812`) or modify the `/etc/hosts` file.



Downloading

The file sp52.zip is downloading. After the download is complete, the file will be scanned.

Navigation to another page will interrupt the download, which will then need to be restarted from the beginning.

Download Status

Total estimated size: 13518445 bytes

Transferred size : 13518445 bytes

Scanning...>>>

Scanning completed successfully.

To download the file, click the following link. Download File

Trend Micro InterScan Web Security Virtual Appliance 5.5: IWSVA126

FIGURE 9-11. "Scan before delivering" Large File Handling Progress Window

Note: Some Internet applications (YouTube, Windows Update, streaming, and others) are programmed to receive a certain amount of data on the client side within a certain time frame (for example, 20 percent of data or 1MB of data in 90 seconds). When IWSVA is configured to use the Scan feature before delivering the scanning option, some requested files will not be passed to the client until the scanning is completed. In this case, it is likely that the Internet application could detect a transmission failure because the client side does not receive enough data in time. Then, the client side will not be able to complete the video file or streaming file.

Deferred Scanning

When IWSVA is configured to use the **Deferred scanning** option, part of the file is passed to the requesting client while IWSVA scans the remainder of the file. However, the Web page is not entirely delivered if the scan process is interrupted because of virus detection. If you set the percent of received data will be unscanned and sent to client periodically value to 100%, the last 4Kb will not be sent to the client until the scanning is complete.

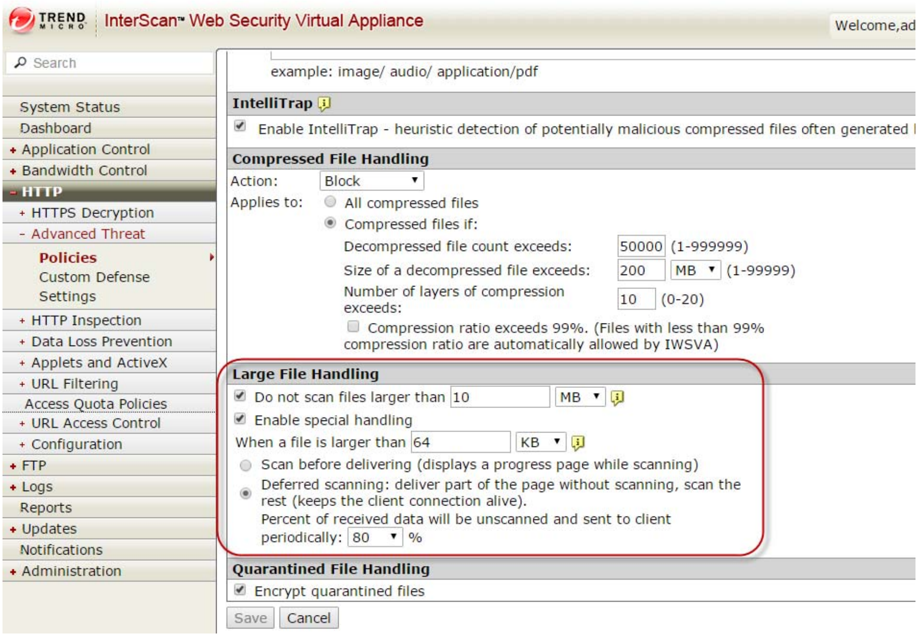
Instead of using a specified data size, IWSVA uses a percentage to define how much data is downloaded at a time. At most every two seconds, IWSVA sends a specified percentage of received data to the browser. The last chunk of data is not larger than 4KB and is sent to the browser before the scan is finished.

For the data download percentage, you can specify either 20, 40, 60, 80, or 100. The default percentage is 60. The actual percentage of data sent to the browser can be much smaller than the percentage specified.

Note: Large file handling does not work when using the Blue Coat Port 80 Security Appliance in ICAP mode. In addition, when using the Blue Coat security appliance in ICAP mode, when the client downloads a large virus-infected file, the client browser may not show the virus blocking notification page. Instead, the client browser will show "Page cannot be displayed." If IWSVA is configured as an HTTP proxy in-line with the Blue Coat appliance, however, large file handling functions.

External data received by IWSVA is sent to the browser in smaller chunks without scanning. The last chunk is sent to the browser to complete the download only after the entire set of data is received and scanned. Sending smaller chunks not only maintains the IWSVA-Web browser connection, but also keeps end-users posted of the download progress.

Large file handling can be set for each policy (click **HTTP > Advanced Threat Protection > Policies > policy** and click the **Virus/Malware Scan Rule** tab).



example: image/ audio/ application/pdf

IntelliTrap

☑ Enable IntelliTrap - heuristic detection of potentially malicious compressed files often generated

Compressed File Handling

Action: Block

Applies to:
○ All compressed files
● Compressed files if:
Decompressed file count exceeds: 50000 (1-999999)
Size of a decompressed file exceeds: 200 MB (1-99999)
Number of layers of compression exceeds: 10 (0-20)
□ Compression ratio exceeds 99%. (Files with less than 99% compression ratio are automatically allowed by IWSVA)

Large File Handling

☑ Do not scan files larger than 10 MB
☑ Enable special handling
When a file is larger than 64 KB
○ Scan before delivering (displays a progress page while scanning)
● Deferred scanning: deliver part of the page without scanning, scan the rest (keeps the client connection alive).
Percent of received data will be unscanned and sent to client periodically: 80 %

Quarantined File Handling

☑ Encrypt quarantined files

FIGURE 9-12. For special handling of large files, there are two options to choose from: (1) scan before delivering and (2) deferred scanning

Disable large file scanning by choosing the **Do not scan files larger than** option to reduce performance issues when downloading very large files. This allows you control over their integrity.

To disable scanning large files:

- Under **Large File Handling**, select the **Do not scan files larger than** check box and then configure the file size over which files are not scanned.

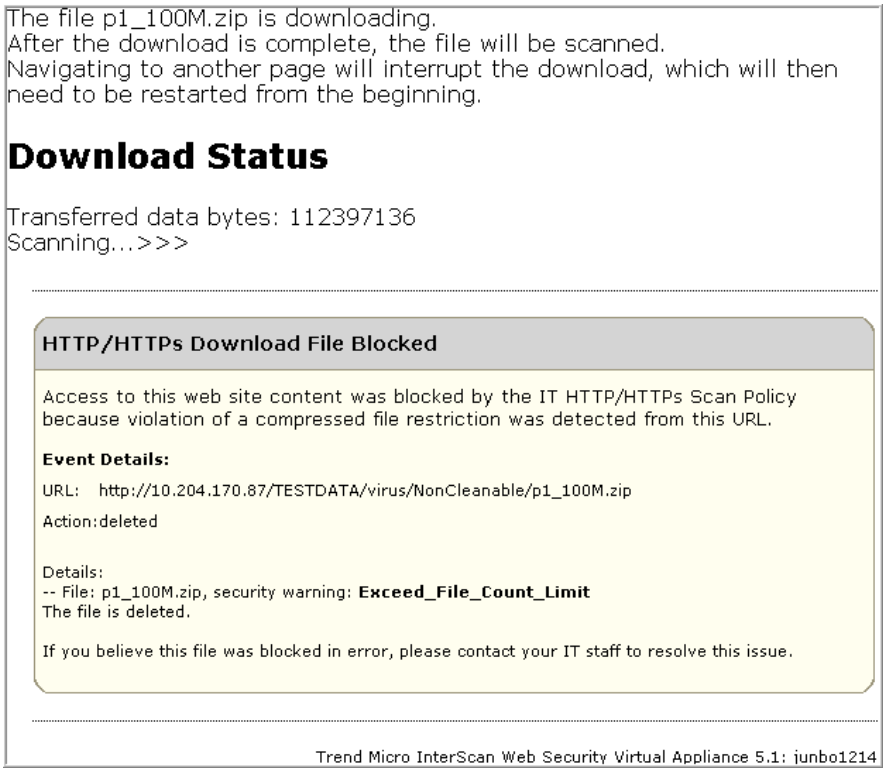
  Trend Micro does not recommend disabling the scanning of any files, even large ones, because it introduces a security vulnerability into your network.

To use large file handling for HTTP scanning:

1. In the **Large File Handling** section, select **Enable special handling**, and then type the file size (in KB or MB) to be considered a large file.
2. Select the type of large file-handling to use:
   - **Scan before delivering**: Shows progress while scanning, and then loads the page afterwards (default setting)
   - **Deferred scanning**: Loads part of the page while scanning; stops the connection if a virus is found
3. Click **Save**.

Important Notes for Large File Handling

- Violations of the large file handling policy displays a user notification in the requesting client's browser. See the example in *Figure 9-13*.



The file p1_100M.zip is downloading.
After the download is complete, the file will be scanned.
Navigating to another page will interrupt the download, which will then need to be restarted from the beginning.

Download Status

Transferred data bytes: 112397136
Scanning...>>>

HTTP/HTTPs Download File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPs Scan Policy because violation of a compressed file restriction was detected from this URL.

Event Details:

URL: http://10.204.170.87/TESTDATA/virus/NonCleanable/p1_100M.zip

Action:deleted

Details:
-- File: p1_100M.zip, security warning: **Exceed_File_Count_Limit**
The file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

Trend Micro InterScan Web Security Virtual Appliance 5.1: junbo1214

FIGURE 9-13. Notification after Completing Scanning and Downloading the File

- Large file special handling only applies to HTTP scanning, FTP scanning, and FTP over HTTP through the HTTP proxy. It does not apply to FTP over HTTP for ICAP traffic. Time-out issues may occur while downloading large files using FTP over HTTP.
- When using the deferred scanning method, IWSVA does not delete files subsequently found to be infected in the first affected client.

Quarantined File Handling

If you choose to quarantine files that IWSVA detects as malicious, you can optionally choose to encrypt the files before moving them to the quarantine folder by selecting the **Encrypt quarantined files** check box.This prevents the files from being inadvertently executed or opened. Note that encrypted files can only be decrypted by a Trend Micro Support engineer.

After configuring the HTTP virus scanning rules in the **HTTP > Advanced Threat Protection > Policies > Add Policy/Edit Policy** screen, click **Next** to move on to the Spyware/Grayware scanning rules.

Spyware and Grayware Scanning Rules

In addition to computer viruses, the IWSVA pattern files include signatures for many other potential risks. These additional risks are not viruses, because they do not replicate and spread. However, they can perform unwanted or unexpected actions, such as collecting and transmitting personal information without the user's explicit knowledge, displaying pop-up windows, or changing the browser's home page.

IWSVA can be configured to scan for the following additional risks:

- **Spyware—**Software that secretly collects and transmits information without the user's explicit knowledge or consent
- **Dialers—**Software that secretly dials a telephone number, typically an international or pay-per call number, through the user's modem.
- **Hacking tools—**Software that can be used for malicious hacking purposes.
- **Password cracking applications—**Software designed to defeat computer passwords and other authentication schemes.
- **Adware—**Software that monitors and collects information about a user's browsing activities to display targeted advertisements in the user's browser or through pop-up windows.
- **Joke programs—**Programs that mock computer users or generate some other sort of humorous display.
- **Remote access tools—**Programs designed to allow access to a computer, often without the user's consent.

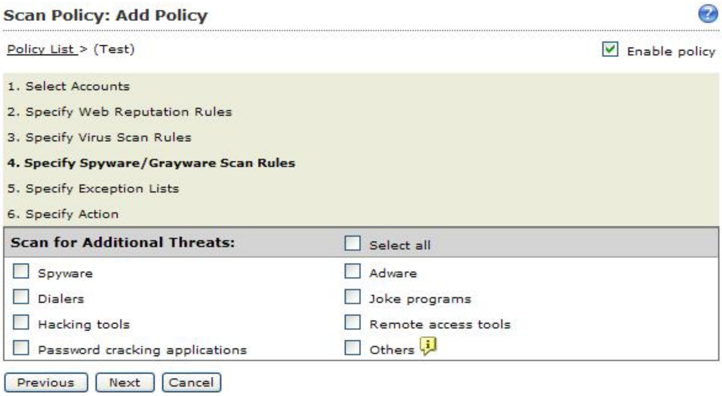
- **Others—**Files that do not fit into the other additional risks classifications. Some of these might be tools or commercial software that have legitimate purposes, in addition to having the potential for malicious actions.

To scan for spyware, grayware, and other non-virus additional risks:

1. Click **HTTP > Advanced Threat Protection > Policies > policy** and click the **Spyware/Grayware Scan Rule** tab. Under **Scan for Additional Threats**, select the types of additional risks to be detected.

   To scan for all additional risks that have signatures in the pattern file, check **Select all**.

2. Click **Next** to configure the actions against security risks.



Scan Policy: Add Policy

Policy List > (Test) ☑ Enable policy

1. Select Accounts
2. Specify Web Reputation Rules
3. Specify Virus Scan Rules
4. **Specify Spyware/Grayware Scan Rules**
5. Specify Exception Lists
6. Specify Action

Scan for Additional Threats: □ Select all

□ Spyware	□ Adware
□ Dialers	□ Joke programs
□ Hacking tools	□ Remote access tools
□ Password cracking applications	□ Others

FIGURE 9-14. Spyware, grayware and additional threat scan configuration

X-Forwarded-For HTTP Headers

The X-Forwarded-For (XFF) HTTP header is a de facto standard for identifying the originating IP address of a client connecting to a Web server through an HTTP proxy or load balancer. X-Forwarded-For header are supported by most proxy servers, and IPv6 X-Forward-For headers are supported in IWSVA. The headers can be parsed to access the client's IPv6 addresses similar to the behavior of IPv4 addresses.

IWSVA also handles three actions for IPv6 access similar to IPv4, including the "Keep X-Forwarded-For header intact" feature, and the "strip X-Forwarded-For header" feature.

- When IWSVA receives an HTTP request with an XFF header, it parses the XFF header to get the original client IP address and use the IP address to do a policy match.
- When IWSVA forwards an HTTP request, it takes the action configured by the administrator on the XFF HTTP header. (See *Table 9-5*.)

Note: IWSVA does not support parsing XFF headers for HTTPS traffic.

TABLE 9-5. Available actions for XFF HTTP headers

ACTION	DESCRIPTION
Keep X-Forwarded-For header intact	IWSVA does not make any changes to the XFF HTTP header.
Append the IP address where IWSVA receives the request	IWSVA adds the IP address of the last hop into the XFF HTTP header. If the XFF HTTP header does not exist, IWSVA creates one.
Strip X-Forwarded-For header	(Default) IWSVA removes the XFF HTTP header from the HTTP request and prevents the privacy information of client from leaking upstream.

See *Table 9-6* to verify that your deployment scenario works with the XFF HTTP headers.

TABLE 9-6. Deployment scenarios using X-Forwarded For HTTP headers

DEPLOYMENT MODE	PARSES XFF	ACTION: KEEP	ACTION: ADD IP ADDRESS	ACTION: REMOVE	NOTES
Forward Proxy Mode	Yes	Yes	Yes	Yes	
Transparent Bridge Mode	Yes	Yes	N/A	Yes	This mode is transparent and does not need to add and IP address in the header.
WCCP Mode	Yes	Yes	Yes	Yes	
Simple Transparency Mode	Yes	Yes	Yes	Yes	
ICAP Mode	N/A	N/A	N/A	N/A	IWSVA acts as an ICAP server. It does not communicate with the client and server. The IP address is provided by the ICAP client with an X-Client-IP header
Reverse Proxy Mode	N/A	N/A	N/A	N/A	XFF HTTP headers are not supported in this mode.

Configuring X-Forwarded-For HTTP Headers

In IWSVA, there are mainly two scenarios to configure:

- Enabling or disabling the parsing of XFF HTTP headers
- Configuring the action taken on the XFF HTTP header (if enabled.)

To configure the XFF HTTP header module settings:

1. Go the **HTTP > Configuration > X-Forwarded-For Header.**
2. Enable or disable parsing of the XFF HTTP.
   - To enable, select **Enable** from the drop-down list.
   - To disable, select **Disable** from the drop-down list.
3. If parsing is enabled, set the action to **Keep** (default) the X-Forwarded-For header intact, **Append** the IP address where the IWSVA receives the request**,** or **Strip** the X-Forwarded-For header. (See *Table 9-5*.)
4. Click **Save**.

Specifying Bot and C&C Contact Detection Rules

In order for you to monitor and analyze possible bot behavior within your network environment, you can specify an action when a bot detection rule has been matched. Navigate to **HTTP > Advanced Threat Protection > Policies | policy | Bot Detection Rule** tab. You can select or clear **Use Bot/C&C Detection rule in this policy** to enable or disable using Bot/C&C Detection rule. You can also select action for bot detection.

Specifying the Exceptions List

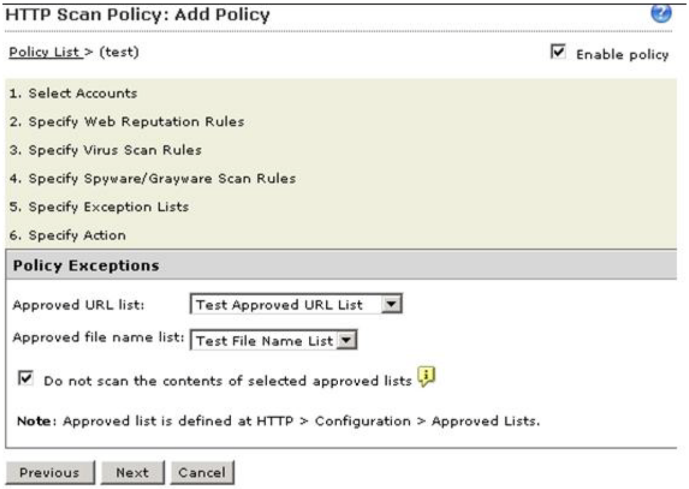
See **HTTP > Advanced Threat Protection > Policies | policy | Exceptions** tab.

You can configure IWSVA to bypass virus/spyware scanning and compressed file handling action on an approved list. This could cause security holes when this approved Web site has been hacked to inject malicious code into the Web site. IWSVA addresses this issue by enabling the virus/spyware scan feature as the default. As such, the Web page is always scanned even when a security policy determines that the Web site is within its approved list.

You can apply an exception list in the Exceptions screen. For HTTP and FTP scanning policies, you can also apply a filename exception list. You can create new exception lists in the Approved Lists screen (see *Creating Exception Lists* on page 9-72 for more information).

The following describes the options in the Exceptions screen:

- **Approved URL list**—Select the name of the approved URL list to be exempted from a URL filtering policy, HTTPS decryption policy, HTTP Inspection policy, Data Loss Prevention policy, applet and ActiveX security policy, or the WRS rule and file type blocking in an HTTP scanning policy.
- **Approved file name list**—Select a file name list to be exempted from file type blocking. You can apply a file name exception list to an HTTP scanning policy, Data Loss Prevention policy, or an FTP scanning policy. This option is not available for HTTPS decryption policies, HTTP Inspection policies, applets and ActiveX policies, and URL Filtering policies.
- **Do not scan the contents of selected approved lists**—Select this option if you do not want to scan the contents of the URLs or files in the approved lists for viruses. Compressed file handling is not available when this option is selected.



HTTP Scan Policy: Add Policy

Policy List > (test)

☑ Enable policy

1. Select Accounts
2. Specify Web Reputation Rules
3. Specify Virus Scan Rules
4. Specify Spyware/Grayware Scan Rules
5. Specify Exception Lists
6. Specify Action

Policy Exceptions

Approved URL list: Test Approved URL List

Approved file name list: Test File Name List

☑ Do not scan the contents of selected approved lists

Note: Approved list is defined at HTTP > Configuration > Approved Lists.

FIGURE 9-15. Configuring policy exceptions

Creating Exception Lists

You can create a new URL and file name exception list in the Approved Lists screen.

To configure a URL exception list:

1. Select **HTTP > Configuration > Approved Lists** from the main menu and click the **URL Lists** tab.
2. Click **Add** and specify a name, the match type or, if preferred, import the URL exception list.
   - **List Name**—Type a brief but descriptive name for the approved list.
   - **Match**—Type a Web site, a keyword or phrase, or a string of characters in the field. This field supports both the ? and * wildcards. Entries in this field are added one-by-one to the Approved List.
3. Select the option that corresponds to what you typed in the Match field:
   - **Web site**—Limits the search to the string as a whole; used with one or more wildcards, this type of exemption rule can be especially useful for allowing access to an entire Web site. There is no need to include http:// or https:// in the URL (it is automatically stripped). IWSVA allows using the internationalized domain names for Web pages. IWSVA also adds the "@" character before the Web site domain name.
   - **URL keyword**—Looks for any occurrence of the letters and/or numbers within a URL, and will match regardless of where the string is found (the string "partner" would be considered a match for "http://www.playboy.com/partner.htm" and the URL exempted). Using wildcards in this field greatly increases the chance of false positives and unexpected results.
   - **String**—Limits the search to the string as a whole; for example to target a specific site, page, file, or other particular item.

Note: - For HTTPS decryption policies, the strings to match vary depending on whether you set IWSVA in the proxy or transparency modes.

- In the proxy mode, IWSVA matches the domain names, not the full URL. Thus, you only need to specify the domain names.

- In the transparency mode (WCCP or bridge mode), IWSVA matches the `CommonName` in the server certificates received.

- For HTTPS standard ports, IWSVA matches the `CommonName`.

- For HTTPS non-standard ports, IWSVA matches `CommonName:Port`

- **Import approved list**—You can import an existing list of URLs that you want exempt from virus scanning or filtering (done by the URL Filtering module). For example if you have a list of URLs from the Trend Micro WebManager, or URLs you have compiled using a text editor, you can import the list rather than enter them one-by-one. Import lists must conform to a defined standard. See *Approved List Formats* on page 9-74.

4. Click **Save**.

To configure a file name exception list:

1. Select **HTTP > Configuration > Approved Lists** from the main menu and click the **File Name Lists** tab.
2. Click **Add** or **Edit** and specify the match type or import the exception list.
   - **List Name**—Type a brief but descriptive name for the approved list.
   - **Match**—Enter a file name with the file extension or a file extension in the field. This field supports the * wildcard. Entries in this field are added one-by-one to the Approved List.
   - **Import approved list**—You can import an existing list of file names that you want exempt from virus scanning. For example if you have a list of file names from Trend Micro's Web site, or file names that you have compiled using a text editor, you can import the list rather than enter them one-by-one. Import lists must conform to a defined standard. See *Approved List Formats* on page 9-74.
3. Click **Save**.

Approved List Formats

IWSVA supports two types of approved lists: URL and file name. The list formats for each type is described below.

Approved lists using the [approved] format can be imported. Blocked and allowed lists using the [blocked] and [allowed] formats can be imported.

Approved URL List Format

An approved URL list can be any ASCII text file containing the header:

[approved]

There is no limit to the number of URLs you can include in an approved list. Delimit separate Web addresses, URLs, and/or strings using a line break. Approved-lists support the following * and ? wildcards.

Sample file:

```
[approved]

www.good-job-habits.com/*

www.business-productivity.com/*
```

File Name List Format

A file name approved List can be any ASCII text file containing the header:

[approved]

There is no limit to the number of file names you can include in an approved list. Delimit separate file names and/or strings using a line break. Approved-lists support the * wildcard.

Sample file:

```
[approved]

abcfile.doc

*.sc
```

Setting the Scan Action for Viruses

After configuring the HTTP virus scanning rules, configure the actions that IWSVA takes if an infected file, uncleanable file, password-protected or macro-containing file is detected.

Scan Actions

In **HTTP > Advanced Threat Protection > Policies | policy | Action** there are four actions that IWSVA can take in response to the outcome of virus scanning:

- Choose **Delete** to delete an infected file. The requesting client will not receive the file. This action can be applied to the *Infected files*, *Uncleanable files*, and *Password-protected files* scan events.
- Choose **Quarantine** to move a file (without cleaning) to the quarantine directory.

  ```
  /var/iwss/quarantine
  ```

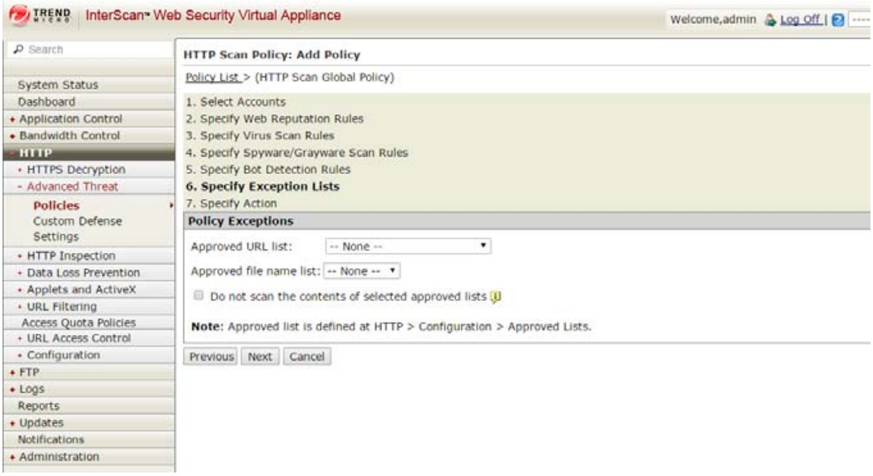
  The requesting client will not receive the file. This scan action can be applied to all four of the scan events. You can optionally choose to encrypt files before sending them to the quarantine directory. For more information, see Quarantined File Handling starting on page 9-66.
- Choose **Clean** to have IWSVA automatically clean and process infected files. The requesting client receives the cleaned file if it is cleanable, otherwise the uncleanable action is taken. This action can be applied to the *Infected files* and *Macros* scan events. For macro-containing files, the Clean action strips the macro from the file, whether the macro is a virus or benign, to protect your network before an updated virus pattern is released and deployed.
- Choose **Pass** to send the file to the requesting user. This action can be applied to the *Uncleanable files*, *Password-protected files*, and *Macros* events. The Pass action should always be used for Macros events, unless you want to strip or quarantine all macro-containing files during a virus outbreak.

Note: Trend Micro does not recommend choosing the *Pass* scan action for uncleanable files.

Scan Events

After scanning, you can configure actions for the four possible scanning outcomes:

- **Infected files**—Files determined to be infected with a virus or other malicious code. Available actions are **Delete**, **Quarantine** or **Clean** (recommended and default action).
- **Uncleanable files**—Depending on the type of virus or malicious code infecting a file, the scan engine might not be able to clean some files. Available actions are **Delete** (recommended and default action), **Quarantine**, and **Pass**.
- **Password-protected files**—Files that cannot be scanned because they are either password-protected or encrypted. The infection status of these types of files cannot be determined. Available actions are **Delete**, **Quarantine**, and **Pass** (recommended and default action).
- **Outside of scan restriction criteria files**—Files that cannot be scanned because the virus scan engine is unable to scan these files due to unknown reasons. Available actions are **Delete**, **Quarantine**, and **Pass** (recommended and default action).
- **Macros**—Microsoft Office files that contain macro program code. Because many of the fastest spreading viruses are macro viruses, you can quarantine all macro-containing files during the early stages of a virus outbreak to block all files before the new virus pattern is added to the pattern file and deployed to your environment. Available actions are **Quarantine**, **Clean**, and **Pass**. Unless there is a need to quarantine or strip macros during a virus outbreak before an updated pattern file is released, the action for Macro should always be set to **Pass**.



HTTP Scan Policy: Add Policy

Policy List > (HTTP Scan Global Policy)

1. Select Accounts
2. Specify Web Reputation Rules
3. Specify Virus Scan Rules
4. Specify Spyware/Grayware Scan Rules
5. Specify Bot Detection Rules
6. **Specify Exception Lists**
7. Specify Action

Policy Exceptions

Approved URL list: -- None --

Approved file name list: -- None --

□ Do not scan the contents of selected approved lists

Note: Approved list is defined at HTTP > Configuration > Approved Lists.

Previous | Next | Cancel

FIGURE 9-16. HTTP Virus Scanning Policy Action Configuration

Adding Notes to Your Policy

To record notes about your policy, type them into the **Note** field at the bottom after configuring the actions taken against files detected by IWSVA. See **HTTP > Advanced Threat Protection > Policies | policy | Action.**

When you have completed configuring the scan actions to apply to your policy, click **Save**. Click **Deploy Policies** to immediately apply the policy; otherwise, the policy is applied after the database cache expires.

Java Applet and ActiveX Security

IWSVA Applets and ActiveX scanning blocks malicious Java applets and unsecured ActiveX controls at the Internet gateway, preventing them from infiltrating your network and performing malicious acts on client workstations.

IWSVA employs a tiered technology approach that operates on both the Internet gateway server and on desktops.

- On the server, IWSVA prefilters Java applets and ActiveX controls based on whether they are digitally signed, the validity of the signature, and the status of the certificates used to do the signing.
- On client workstations, IWSVA code, inserted into Java applets, monitors the behavior of the applets in real time and determines whether their behavior is malicious according to a pre-configured security policy.

Figure 9-17 illustrates how IWSVA scans and blocks malicious applets and ActiveX objects.

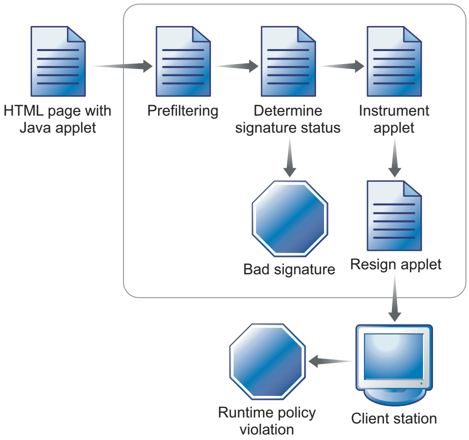


FIGURE 9-17. How Java applet security works

How Applets and ActiveX Security Works

As applets and ActiveX objects pass through the gateway, the validity of their digital signatures are checked. In addition, IWSVA monitors applets in real-time on the client workstations and issues an alert if any prohibited operations are attempted.

Step 1. Filtering Applets & ActiveX at the Server

As Java applets and ActiveX controls are downloaded to the proxy server, IWSVA filters them according to the following criteria:

For ActiveX Objects

If ActiveX security is enabled, IWSVA checks the signatures of CAB files and executable COM objects (of which ActiveX controls are a type) that are digitally signed. It then examines the digital certificates contained in the signature and compare them with those in the IWSVA-specific certificate database. ActiveX objects not signed, invalidly signed, or signed using an unknown root Certification Authority (CA) certificate can be blocked. In their place, the system creates a new HTML page containing a warning message. This new page is then delivered to client workstations.

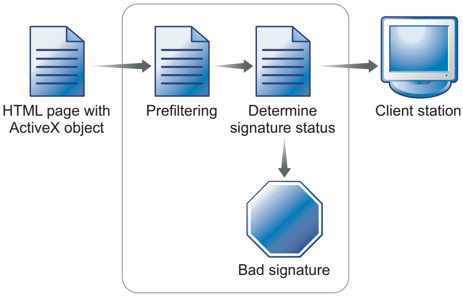


FIGURE 9-18. How ActiveX Security Works

For Java Applets

IWSVA filters Java applets based on whether they are digitally signed, the validity of the signature, and the status of the certificates used to do the signing.

If signature verification is enabled, IWSVA verifies the signatures of digitally signed applets. Those not signed, signed using an unknown or inactive root Certification Authority (CA) certificate, signed using a flagged certificate, or invalidly signed can be blocked. They are then replaced with a new applet that displays a warning message. If certificate checking is disabled, the system accepts all Java applets regardless of the certificates they carry.

IWSVA keeps a database of recognized certificates, which is used in the filtering process. This database is automatically updated to include any unrecognized certificate the system encounters. You can delete entries from the database and enable or disable entries on the **HTTP > Configuration > Digital Certificates** (see Managing Digital Certificates starting on page 9-93).

For Java Applets, IWSVA first performs Steps 2 and 3 below before sending the applets to the clients.

Step 2. Instrumenting Applets

IWSVA analyzes the applet code to determine any potentially dangerous actions that it might perform. It then adds instrumentation code (that is, instructions that notify the user of certain programming operations) to monitor and control these actions.

During instrumentation, IWSVA inserts monitoring code around suspicious instructions and then attaches the security policy assigned to the intended recipients. Depending on how IWSVA is configured, this security policy might vary from one client to another, based on the domain they belong to or their IP addresses. IWSVA supports creating multiple policies that can be mapped to different groups of users in your network. IWSVA uses the inserted monitoring codes and the attached security policy to monitor the applet's behavior in real-time and to determine whether or not this behavior is malicious.

Note: The process of instrumenting a signed applet renders the signature invalid. Therefore, the signature is stripped, leaving it unsigned. IWSVA can optionally re-sign the applet if required by the client browser.

Step 3. Optionally Re-signing Instrumented Applets

If configured to do so, IWSVA re-signs the instrumented applets using an imported "private key" before sending them to client workstations. Because applets lose their original signatures during the instrumentation process (due to modifications to their original code), you might want to use this feature to ensure that the clients' Web browsers run the instrumented applets with the permissions they might require to run correctly.

IWSVA supports the import of a "private key", along with the associated certificate that contains the corresponding "public key," for use in the re-signing process. You can purchase this key from any of the well-known Certifying Authorities (CAs). Only one re-signing key may be configured for use at any given time.

Note: Re-signing applies only to validly signed applets. If the system is configured to accept unsigned applets, these applets bypass this process and are delivered to client workstations immediately after instrumentation.

Step 4. Monitoring Instrumented Applet Behavior

When the applet executes in the browser, the instrumentation is automatically invoked before any potentially dangerous operation is performed. The instrumentation determines whether an action is permitted by comparing it with the attached security policy. If the action is permitted, IWSVA then allows the action to take place; otherwise, IWSVA notifies the users and gives them the option to allow the behavior, terminate the behavior, or stop the applet.

Enabling Applet/ActiveX Security

To start scanning your HTTP traffic for malicious applets and ActiveX objects, enable this scanning from the Applets and ActiveX policy page.

To enable malicious Applets and ActiveX scanning in HTTP traffic:

1. Select **HTTP > Applets and ActiveX > Policies** from the main menu.
2. Check **Enable Applet/ActiveX security**.
3. Click **Save**.

Adding and Modifying Applet/ActiveX Scanning Policies

See Configuring the Scope of a Policy starting on page 8-17 for more information and procedures for setting a policy’s scope using the three different user identification methods.

All configured policies are listed on the **Applets and ActiveX Policies** screen available from **HTTP > Applets and ActiveX > Policies**.

To modify the scope of a policy:

1. Open the **Applets and ActiveX Policy** screen (**HTTP > Applets and ActiveX > Policies** from the main menu).
2. Do one of the following:

- To remove accounts from a policy's scope, select the users, click **Delete** and then **Save**.
- To add accounts to a policy's scope, click the **Policy Name**, switch to the **Account** tab, add or delete the accounts to which the policy applies, and click **Save**.

Account fields should support IPv6 addresses. You can define one rule for any IPv6 host, and this policy rule is triggered when the client accesses Applets or ActiveX through IWSVA.

- When selecting available policies, both IPv4 and IPv6 policies will appear.
- In the Account field, acceptable account entries include a single IPv6 address, an IPv6 range, or an IPv6 mask similar to what has been supported with IPv4.

3. Click **Deploy Policies**. Changes to a policy's scope do not take effect until the modified policies are deployed.

After configuring the scope of your policies, configure the applet and ActiveX scanning rules.

Configuring Java Applet Security Rules

On the **HTTP > Applets and ActiveX > Policies** screen, add a new policy or select an existing policy. On the **Java Applets Security Rules** tab, IWSVA can be configured to either block all applets, or to accept and process applets using the security settings you specify.

Signature Status

A digital signature is a way to verify the genuine publisher of an applet. It also allows you to verify that the applet has not been tampered with or otherwise changed because it was published. After analyzing the applet's signature, IWSVA makes one of the following determinations:

- **Valid signature**
- **No signature:** The applet is unsigned.
- **Invalid signature:** The applet's signature is corrupt or cannot be verified for some reason; for example, no trusted root certificate is found

Checking the signature of an applet is done in two steps. The first verifies the integrity of the applet code against data in the signature. The second verifies the integrity of the certificates, the "certificate chain," used to create the signature. For the signature to be considered valid, the certificate chain must end with a trusted certificate recognized by IWSVA. The set of these certificates can be viewed and managed by opening the Web console to **HTTP > Configuration > Digital Certificates > Active Certificates**.

Certificate Status

Java applet security rules can apply different actions to applets that have valid signatures, based on their certificate status.

By default, IWSVA trusts its active certificates. However, an active certificate can be "flagged" if you no longer want to trust applets that have a flagged certificate in their certificate chain. Flagged certificates continue to be listed as active certificates, though the flagged status is noted.

Instrumentation and Re-signing

Instrumentation is the process through which IWSVA adds monitoring and control code to the applet. Because the instrumentation process breaks the applet's signature, if any, you can alternatively choose to re-sign an applet after instrumentation. This ensures the instrumented applets executes in the browser and perform operations as expected.

Applet Instrumentation Settings

The purpose of instrumenting applets is to prevent applets from executing prohibited operations on client machines. By default, Java applets processed by IWSVA are not allowed to perform the following types of operations:

- **Destructive operations:** Deleting and renaming files
- **Non-destructive operations:** Listing files in a directory or retrieving file attribute information
- **Write:** Writing new or modifying existing files
- **Read:** Reading file contents

Configuring Exceptions

For each of the types of operations that can be selectively allowed or prohibited, you can configure file or folder exceptions where the security policies do not apply.

- To allow a given type of file operation, except when performed by a subset of files, check the **Enable** button next to the file operation. Click the **Exceptions** link. The **Exceptions to File Operations** screen opens. Configure the files and folders where the operation is not allowed.
- To disallow a given type of file operation, except for a subset of files, check the **Disable** button next to the file operation. Click the **Exceptions** link and then configure the files and folders where the operation is allowed.

To configure Java applet processing settings:

1. After setting the scope of your policy, do one of the following:
   - Select **Process Java applets using the following settings** for IWSVA to pass, block or instrument the applet based on its signature and certificate status.
   - Select **Block all Java applets** for IWSVA to not allow any applets to pass to the clients. If you choose this setting, proceed to step Step 3.
2. For each of the following signature and certificate status, choose the processing action to use (* denotes the default Trend Micro-recommended settings):
   - **Valid signature, trusted certificate**: Pass*, Instrument applet (re-sign), Instrument applet (strip signature), Block
   - **Valid signature, flagged certificate**: Pass, Instrument applet (re-sign), Instrument applet (strip signature), Block*

- **No signature**: Pass, Instrument Applet*, Block
- **Invalid signature**: Pass, Instrument Applet (strip signature), Block*

3. For each of the four (destructive, non-destructive, write or read) operations that can be selectively enabled or disabled, click **Enable** or **Disable** to configure your security policy.
4. Click **Exceptions**, and then configure the files or folders that are exceptions to the security policy:

   a. Enter the **Directory/File Path** of the files that do not apply to the configured security policy.

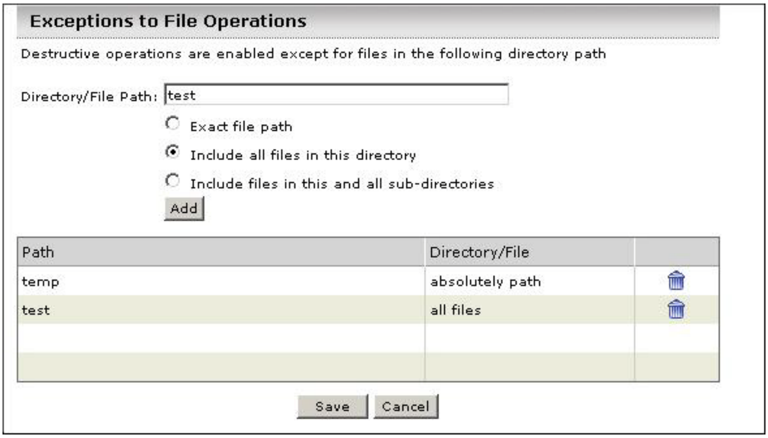
      - To configure a specific file path, select **Exact file path**.
      - To exclude the entire folder's contents from the security rule, select **Include all files in this directory**.
      - To exclude all of the folder's files, plus those in subdirectories, from the security rule, select **Include files in this and all subdirectories**.

      Note: All file paths are those on the client machine, where the applet runs. The file path format should be in the form required by the operating system running on the client.

   b. Click **Add** to add the exceptions to the given security policy.

   c. Configure other files or directories to exempt from the applet's security settings.

d. When you've completed configuring your file and folder exceptions, click **Save**.



Exceptions to File Operations

Destructive operations are enabled except for files in the following directory path

Directory/File Path: test

○ Exact file path

● Include all files in this directory

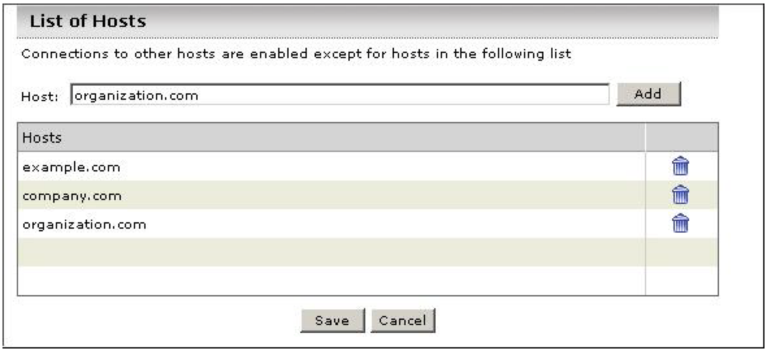
○ Include files in this and all sub-directories

Path	Directory/File	
temp	absolutely path	🗑
test	all files	🗑

FIGURE 9-19. Java applet instrumentation settings exception files and folders

5. On the **Java Applet Security Rules** tab, select **Bind local ports** to allow applets to bind to ports on the client workstation.
6. To allow applets to connect to their originating servers, select **Connect to their originating servers**.
7. To allow applets to connect to hosts other than the ones they originated from, select **Enable** or **Disable** next to **Host connections**, then configure exceptions to the security policy.
   a. Enter the **Host** that does not apply to the configured security policy.
   b. Click **Add** to add the exceptions to the given security policy.
   c. Add others host that do not apply to the security policy.

d. When you've completed configuring the hosts that are exceptions to the policy's security rules, click **Save**.



List of Hosts

Connections to other hosts are enabled except for hosts in the following list

Host: organization.com

Hosts	
example.com	🗑
company.com	🗑
organization.com	🗑

FIGURE 9-20. Exceptions to the Java applet host connection rules

8. Select **Create new thread groups** to allow applets to create new thread groups. To disallow this operation, clear it.
9. Select **Create unlimited active threads** to have IWSVA ignore thread activity from applets downloaded to clients on the LAN and specify a limit to restrict the number of threads applets can create at one time. To disallow this operation, clear it.
10. Select **Create unlimited active windows** to limit the number of active top-level windows applets can open. Enter the number of allowable windows in the provided text box. Clearing this option gives applets the freedom to open as many windows as they want—just like some malicious Java applets do to annoy users.
11. Enter any optional **Note** for future reference about this policy.
12. Click **Next** to continue with configure ActiveX security rules if you are configuring a new Applets and ActiveX policy. If you are modifying an existing policy, click **Save**.
13. Click **Deploy Policies** to immediately apply the policy; otherwise, the policy is applied after the database cache expires.
14. Enter any notes to save pertinent information about this policy, and then click **Save**.

Configuring ActiveX Security Rules

ActiveX security rules can be applied to the two different types of ActiveX controls:

- **Executable cabinet files** (*.cab): An ActiveX control distributed using the Windows native compressed archive format.
- **Portable executable (PE) files** (*.exe, *.ocx, and so on): An executable file format that has "portability" across all 32-bit and 64-bit versions of Windows.

For each of these two file types, you can configure security policies to:

- Block all ActiveX controls of that type
- Allow all ActiveX controls of that type
- Verify signatures, and alternatively block invalidly signed or unsigned files

Enter any notes about this policy and then click **Save**.

Applying Applet and ActiveX Policy Exceptions

There may be URLs or Web sites that you want exempt from an Applet and ActiveX policy (for example, the corporate intranet, business partner sites, and research tool sites).

In the **Exceptions** tab, select the name of the approved URL list to be exempted from the **Approved URL List** field.

You can create exception lists in the **HTTP > Configuration > Approved Lists** page (see *Specifying the Exceptions List* on page 9-70 for more information).

Applet and ActiveX Settings

Applet and ActiveX security policies determine certificate and signature status as configured on the **Applet and ActiveX Settings** page. For example, IWSVA can either attempt to validate signatures, strip the signatures and process all applets as being unsigned, or check the certificate's revocation status. In addition, IWSVA can re-sign applets after instrumentation.

To validate the signature of an ActiveX control, IWSVA can check the expiration of the signing certificate, check all certificates in the signing chain (exclusive of the signing certificate) and check the revocation status of the certificate (where a revocation information source is available for a certificate).

To configure how IWSVA validates Java applet and ActiveX signatures:

1. Click **HTTP > Applets and ActiveX > Settings** from the main menu.
2. Complete the settings on the **Java Applets** and **ActiveX Executable**s tabs.
3. Click **Save**.

Java Applet Signature Validation

When IWSVA processes signed applets, it can handle digital signatures in one of two ways:

- Strip signatures and treat all incoming applets as unsigned applets, a restrictive security setting that treats all applets, signed or unsigned, in the same manner. In a normal client browser environment, the unsigned applet does not have access to the client system's resources, but it can still produce annoying behavior such as opening many windows.
- Perform full signature validation on the applets.

Adding Certificates for Applet Signature Verification

Java applet signatures are verified using root certificates installed. To see the list of root certificates, select **HTTP > Configuration > Digital Certificates** from the main menu. ActiveX signatures are verified against the root certificates in the IWSVA device's Windows certificate store.

If your environment requires running applets signed with root certificates that are not installed along with IWSVA, then add them to the IWSVA digital certificate store.

To add a certificate to the IWSVA certificate store:

1. Click **HTTP > Configuration > Digital Certificates** from the main menu.
2. On the **Active Certificates** tab, click **Add**, select the certificate, and then click **Add**.
3. Return to the **Active Certificates** screen and verify that the added certificate appears on the list.

Certificate Expiration

IWSVA can be configured to:

- Check that the certificate used to sign the applet has not expired
- Check that the certificates in the certification path are all valid

Untrusted Signature Status

If IWSVA is unable to determine whether the certificate should be trusted because of its certification path, then the applet's signature status can be set to:

- Unsigned (which means the signature is stripped), or
- Invalid

Revocation Status

Digital certificates can be revoked by their issuer. IWSVA can check whether a certificate has been revoked when a status source is available.

If IWSVA cannot access the defined status source, you can configure IWSVA to set the status of the certificate to Valid, Unsigned (Strip signature), or Invalid.

Applet Re-signing

IWSVA can re-sign instrumented applets with your company's own "private key" before they are sent to client workstations. Because applets lose their original certificates during instrumentation, you might want to re-sign them to ensure that clients' Web browsers always accept the applets without any restrictions.

To use the re-signing feature, you need two keys: 1) a "private key" that must be imported into IWSVA, and 2) a certificate containing the "public key" equivalent to your "private key" that must be imported into your clients' Web browsers. The certificate enables the browsers to recognize the signature you affix to instrumented applets. Without this certificate, these applets are treated as another unsigned applet—either blocked by the browser or given limited access to system resources.

IWSVA supports the PKCS12 key format. If you do not have a key yet, you can purchase one from any of the well-known Certificate Authorities (CAs).

To re-sign applets after instrumentation:

1. On the **Java Applets** tab of the **Applet and ActiveX Settings** page (**HTTP > Applets and ActiveX Settings**), check **Re-sign the applets with the following certificate**.
2. Type the path or click **Browse** to navigate to the certificate to use for re-signing.
3. Enter the certificate's **Password**.
4. Click **Add**.
5. Click **Save**.

ActiveX Signature Validation

To verify whether an ActiveX control is validly signed, IWSVA can check the control's certificate in several ways—for both a Cab file and PE file. This validation includes checking the expiration of the signing certificate, the expiration of all certificates in the signing chain, or by checking the revocation status of the certificate (when a status source is defined).

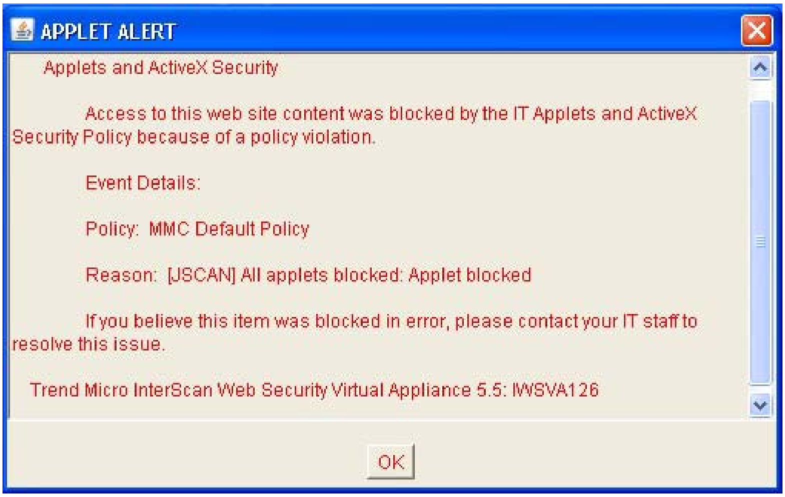
To configure how IWSVA checks the signature status of a signed ActiveX control:

1. Select **HTTP > Applets and ActiveX > Settings** from the main menu, and click the **ActiveX Executables** tab.
2. Enable the types of signature checking to use for ActiveX controls:
   - Check the expiration of signing certificate
   - Check the expiration of all certificates in the chain
     If the signature has a timestamp countersignature:
     - Use timestamp when a certificate is expired
     - Timestamp countersignatures do not expire
   - Check the revocation status of the certificate (where a status source is defined)
     If unable to access the defined status source, set status to:
     - Valid
     - Invalid
3. Click **Save**.

Client-side Applet Security Notifications

There are several alert messages that might be displayed in the client’s browser in response to IWSVA Java applet security policies.

If an applet is blocked due to its signature or certificate status, the requesting client is presented with a message showing the policy that blocked the applet, along with the reason:



APPLET ALERT

Applets and ActiveX Security

Access to this web site content was blocked by the IT Applets and ActiveX Security Policy because of a policy violation.

Event Details:

Policy: MMC Default Policy

Reason: [JSCAN] All applets blocked: Applet blocked

If you believe this item was blocked in error, please contact your IT staff to resolve this issue.

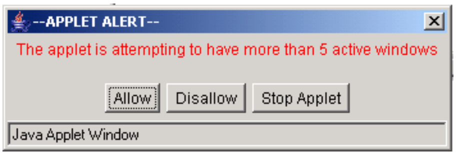
Trend Micro InterScan Web Security Virtual Appliance 5.5: IWSVA126

FIGURE 9-21. Blocked applet notification

If an instrumented applet attempts to perform an operation that is not allowed by a policy’s configuration, a notification displays the disallowed operation and the user is prompted on how to proceed. Available options are:

- **Allow**: The instrumented applet continues to run, including the operations not allowed by the policy.
- **Disallow**: The operation that triggered the Applet security policy is stopped, but the instrumented applet continues to run.

- **Stop Applet**: The instrumented applet is terminated.

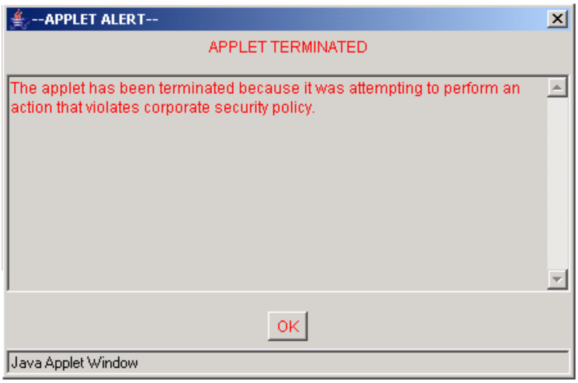


--APPLET ALERT--

The applet is attempting to have more than 5 active windows

FIGURE 9-22. Applet Security Violation Notification

If the client chooses **Stop Applet**, another notification is displayed to indicate that the applet has terminated.



--APPLET ALERT--

APPLET TERMINATED

The applet has been terminated because it was attempting to perform an action that violates corporate security policy.

FIGURE 9-23. Applet Execution Termination Notification

Managing Digital Certificates

For IWSVA to determine that a Web server's or an applet's signature is trusted, the root Certification Authority (CA) certificate on which the signature is based must be added to the IWSVA certificate store.

There are three types of digital certificates that are involved in producing a digital signature:

- The "end" or "signing" certificate, which contains the public key to be used to validate the actual applet signature

- One or more "intermediate" Certification Authority (CA) certificates, which contain the public keys to validate the signing certificate or another intermediate certificate in the chain
- The "root" CA certificate, which contains the public key used to validate the first intermediate CA certificate in the chain (or, rarely, the signing certificate directly). An otherwise valid signature is "trusted" by IWSVA if the CA certificate of the signature is known to IWSVA, is active, and is not flagged.

If IWSVA encounters an unknown certificate during SSL handshake or applet signature processing, it saves the certificate in the "inactive" list, along with the URL of the Web site or applet that contained the signature. Intermediate and root certificates are collected in this way. If required later, a CA certificate collected this way can be "activated" (made trusted by IWSVA) so that the signatures of applets that depend on it can be processed as valid. Intermediate CA and end certificates might be activated, but this only has an effect if the root certificate is also activated. In other words, activating an intermediate CA or signing certificate does not make them trusted (only Intermediate and root CA certificates can be made trusted), but any certificate might be flagged.

To manage the certificates in the IWSVA certificate store, you can perform the following operations:

- **Delete a certificate:** Removes the selected certificate(s) from the certificate store.
- **De-activate a certificate:** Keep the certificate in the IWSVA certificate store, but do not trust certificates that use it in their certification path.
- **Activate a certificate:** Make a CA certificate trusted.
- **Flag the certificate:** Flag all signatures that use the certificate in its certification path, marks the certificate as being specifically untrusted.
- **Clear flagged certificate:** Re-instate the trusted status of a certificate that was previously flagged, so that certificates that use the certificate in their certification path is trusted.

To view existing certificates:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Switch between the **Active Certificates** and **Inactive Certificates** tabs to see which certificates are already known to IWSVA.

To add a trusted certificate or a trusted certificates list:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Ensure the **Active Certificates** tab is active.
3. Click **Add**.

   The **Add Certificates** screen opens.
4. Do one of the following:
   - To upload a new trusted certificate: under **Upload a new certificate**, type the path or click **Browse** to select the certificate to add and click **Add**.
   - To upload a list of trusted certificates: under **Upload the CAs exported from IE in PKCS#7/P7B format**, type the path or click **Browse** to select the certificate list to add and click **Add**.

Note: Certificates are commonly contained in files with the extensions .cer, .der, .crt. The certificates list file format should be PKCS#7/P7B. Also, only active CA certificates are considered trusted, but any active certificate might be flagged.

The screen returns to the **Active Certificates** tab. The certificates that you added should be visible, along with the type of certificate and its expiration date.

To delete a certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Select the certificate(s) to delete.
3. Click **Delete**.

To de-activate a trusted certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Make sure the **Active Certificates** tab is active.
3. Check the certificate(s) to de-activate.
4. Click **De-activate**.
5. The certificate(s) that you selected moves to the **Inactive Certificates** tab.

To activate a certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Make sure the **Inactive Certificates** tab is active.

3. Select the certificate(s) to activate.
4. Click **Activate**.
5. The certificate(s) that you selected moves to the **Active Certificates** tab.

To flag a certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Make sure the **Active Certificates** tab is active.
3. Select the certificate(s) to flag.
4. Click **Flag Certificate**.
5. The flagged certificate(s) remains visible on the **Active Certificates** tab, with a red flag in the status column.

To remove a certificate from being flagged:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Make sure the **Active Certificates** tab is active.
3. Select the flagged certificate(s) to be cleared (certificates with flagged status have a red flag in the **Status** column).
4. Click **Clear Flagged Certificate**.
5. The flagged certificate(s) remains visible on the **Active Certificates** tab, without a red flag in the **Status** column.

Chapter 10

Access Quotas and URL Access Control

Access quotas limit a client's bandwidth consumption to a fixed amount per unit of time. URL trusting can improve browsing performance by exempting trusted URLs from scanning and other InterScan Web Security Virtual Appliance (IWSVA) operations. URL blocking refuses requests to URLs that you specify or whose patterns are contained in the Phish pattern file.

Topics in this chapter include:

Introduction to Access Quota Policies

The IWSVA includes a policy for other clients that can be defined (there is no access quota in Global Policy). If no policy matches the connection, then the client has unlimited access. After modifying access quota policies and saving the policies to the database, the IWSVA service in a multiple server configuration environment reloads the policies according to the time-to-live (TTL) value configured in the **Policy Deployment Settings** screen (**Administration > IWSVA Configuration > Policy Deployment**.)

If the quota is exceeded while making a download, the download is allowed to continue. However, succeeding downloads/browsing requests (before the access quota interval expires) are refused. Users are allowed access again after the access quota interval expires.

Note: For a group quota policy, the quota is for each client within the policy's scope, and all clients in the same policy have the same quota.

Managing Access Quota Policies

The clients within the scope of an access quota policy, the bandwidth quota and the time interval for the quota's duration are configurable. Access Quota Policies can also be applied to IPv6 clients as with the IPv4 clients. Account fields should support IPv6 addresses. You can define one rule for any IPv6 host, and this policy rule is triggered when the client accesses the Internet through IWSVA.

When selecting available policies, both IPv4 and IPv6 policies will appear. In the Account field, acceptable account entries include a single IPv6 address, an IPv6 range, or an IPv6 network mask similar to what has been supported with IPv4.

To add an access quota policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. Select **Enable access quota control**.
3. From the drop-down menu, select the access quota interval—either **day**, **week**, or **month**.

   The value for the access quota interval is globally applied to all access quota policies, including all existing policies.
4. Click **Save**.

5. Click **Add**.
6. Select **Enable policy** and enter the access quota.
7. Select the users to which the policy applies.

   The options on this page depend upon the user identification method that you are using—either *IP address*, *Host name (modified HTTP headers),* or *User/group name authentication*. These settings are configured in the **Administration > IWSVA Configuration > User Identification | User Identification** tab. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method starting on page 8-6.

   Regardless of the user identification method you have configured, you can always enter IP addresses of the clients to which the policy applies.
8. Type some optional notes to record any special information about the policy.
9. Click **Save**.
10. When returned to the **Access Quota Policies** page, click **Deploy Policies** to immediately apply the policy; otherwise, the policy is applied after the database cache expires.

There might be occasions when you want to temporarily deactivate a policy, without deleting the settings from the database.

To deactivate a policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. From the **Access Quota Policies** screen, click the linked item in either the **Account** or **Access quota** column to go to the Edit Policy screen.
3. Clear **Enable policy** at the top of the screen and then click **Save**.

   Disabling the policy does not take effect until the policy cache refreshes, or you click **Deploy Policies**.

If you no longer have any need for a policy (for example, if the employee using the client leaves your organization), you can either delete the whole policy or users within the policy's scope from the IWSVA database.

To delete a policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. From the **Access Quota Policies** screen, select the policy and then click **Delete**.

Deleting the policy does not take effect until the policy cache refreshes, or you click **Deploy Policies**.

Overview of URL Access Control

IWSVA can control a URL's access based on Web Reputation feedback, the URL Filtering module, or a combination of both. The combination of Web Reputation and the URL Filtering module is a multi-layered, multi-threat protection solution provided by IWSVA.

The URL Filtering module grants or denies Web access based on the category to which a URL belongs. Web Reputation grants or denies Web access based on whether the requested URL is a phishing or pharming threat that has hacking potential, or has a reputation score that deems it untrustworthy. Both the URL Filtering module and Web Reputation are controlled by the specifications you make in policies. See **HTTP > URL Access Control**

When a user attempts to access a Web site, the following events occur:

- IWSVA checks the requested URL against the URL blocking list and trusted URL list (see Overview of URL Access Control on page 10-4).

  If the URL is found on the URL blocking list, the request is denied. If the URL is found on the URL trusted list, access is granted and no form of access control is done.
- If the URL is not on the blocked or trusted list, IWSVA sends the requested URL to Web Reputation for processing.
- From a remote database, Web Reputation retrieves the appropriate URL rating for the URL.

  The rating can either be "high," "medium," or "low." The sensitivity level you specify determines whether or not IWSVA blocks the URL (see Specifying Web Reputation Rules on page 9-44).

  If the URL is found on an approved list, IWSVA skips the anti-phishing and anti-pharming detection for this URL (see Specifying the Exceptions List on page 9-70).
- Web Reputation then determines if the requested URL is a phishing or pharming threat and if so, flags the URL accordingly (see Anti-phishing, Anti-pharming, and C&C Callback Attempt Detection on page 9-45).

- The final process of Web Reputation is to determine the category of the URL (see URL Filtering Category Mapping on page G-1).

  The category information is used later by the URL Filtering module.
- Web Reputation returns the URL rating to IWSVA, any phishing or pharming flags, and the URL category.
- If a URL is flagged for phishing or pharming, IWSVA blocks access to the Web site.
- Next, if you are using the URL Filtering module, this module uses the Web category information for the requested URL to determine if access is permissible.

  If the URL is found on the approved URL list, the URL bypasses the category filtering and proceeds to the final step in URL access control.

  If the category of the requested URL is permitted in the URL Filtering policy, then the URL is passed on to the final step; otherwise, the URL is blocked.
- Finally, based on the Web Reputation URL rating, IWSVA determines whether the requested URL is below or above the sensitivity level specified in the scan policy.

  If the URL is found on an approved list, IWSVA skips the sensitivity level checking for this URL (see Specifying the Exceptions List on page 9-70).

  If the rating falls below the sensitivity level, the requested URL is blocked. However, if the rating is above the sensitivity level, IWSVA grants access.

Specifying URL Access Control

IWSVA can optionally trust some URLs and exempt them from scanning and filtering to improve browsing performance to low risk sites. It can also block access to sites using a user-configured list, or by checking requested sites against the Phish pattern file, a compilation of sites associated with "phishing" schemes or other malicious acts.

Configuring Trusted URLs

IWSVA can be configured to trust some URLs and exempt them from scanning and filtering. Because this opens a security risk by allowing unchecked content into your network, configuring a URL as "trusted" must be considered carefully. Because trusted URLs are not scanned, browsing performance is improved. Good candidates for trusting are Web sites that are frequently accessed and contain content you can control (for example, your company's intranet sites).

Trusted URL information is kept in the `/etc/iscan/TrustedURLs.ini` file. The path for the `TrustedURL.ini` file is set using the `normalLists` parameter under the `[URL-trusting]` section in the `/etc/iscan/intscan.ini` configuration file.

When configuring trusted URLs, you can specify the sites using the following:

- The Web site, which includes any sub-sites
- Exact-match strings within a requested URL

You can apply exceptions to sites that would otherwise match the criteria for the trusted URL list, so IWSVA scans or filters them as usual.

A list of trusted URLs and their exceptions can also be imported from a file, in addition to configuring them through the user interface. Write a comment or title (which IWSVA ignores) at the top of a file that contains a list of Web sites or strings, and then write one rule per line. Group sites to be trusted under [allow] as shown in the following example, and group exceptions to the Trusted URL List under [block]:

```
Trusted URLs Import File {this title is ignored}


[allow]

unwanted.com*

www.blockedsite.com*

urlkeyword

banned.com/file

banned.com/downloads/


[block]

www.blockedsite.com/file

www.unwanted.com/subsite/
```

Note: For HTTPS decryption policies, the strings to match vary depending on whether you set IWSVA in proxy or transparency mode.
- In proxy mode, IWSVA matches the domain names, not the full URL. Thus, you only need to specify the domain names.
- In transparency mode (WCCP or bridge mode), IWSVA matches the CommonNames in the server certificates received.

Managing your trusted URLs and exceptions:

1. Click **HTTP > URL Access Control > Global Trusted URLs** from the main menu.
2. In the **Trusted URLs** configuration page, select **Enable Trusted URLs** to enable URL trusting.

   WARNING! When you select the "Enable Trusted URLs" option, the content of trusted URLs will not be filtered and scanned for viruses.

3. Select how you want to specify the URL to trust:
   - **Web site** match (including all sub-sites)
   - **String** match (URL must contain the string)
4. Type the URL string to **Match** and click **Trust** to add it to the Trusted URLs list (shown below the "**Do Not Scan these URLs**" section). To configure exceptions to the trusted URLs list, click **Do Not Trust** and your entry is entered under **Exceptions to the Trusted URL List**.
5. To remove a trusted URL or exception from your trusted URLs list, highlight the item and click **Remove**. **Remove All** clears all the items.
6. Click **Save**.

To import a list of trusted URLs and their exceptions:

1. Click **HTTP > URL Access Control > Global Trusted URLs**.
2. Browse or type the name of the file that contains the list of trusted URLs and their exceptions into the "**Import Trusted list and exceptions**" field.
3. Click **Import**. The trusted URLs and their exceptions from the file appear in the appropriate fields on the interface.
4. Click **Save**.

Blocking URLs

IWSVA can block Web sites and URL strings in the global blocked URL list.

Note: If you have installed the ICAP proxy handler, configure the ICAP client to scan files in pre-cache request mode to make this feature work.

You can block an HTTPS Web site by entering the FQDN.

When configuring URLs to block, you can specify the sites using the following:

- The Web site, which includes any sub-sites
- Keyword matching within a URL
- Exact-match strings within a requested URL

You can apply exceptions to the blocked URL list so IWSVA allows requests as usual. Using this feature, you can block a given site to allow access to some of its sub-sites or files. The URL Blocking list (including exceptions) is maintained in the `/etc/iscan/URLB.ini` file. The path for the `URLB.ini` file is set using the "normalLists" parameter under the [URL-blocking] section in the `/etc/iscan/intscan.ini` file.

In addition to adding the URLs through the Web console, URL block lists can be imported from a text file.

Using a Local List

You can configure IWSVA to block access to URLs based on a list of blocked sites and exceptions that you maintain for your environment.

When adding URLs to the **Block List** and "**Exceptions to the Block List**," it is best that you first make all additions to one list and then save this configuration before you make additions to the other list. This method helps ensure that the same URL exists in both lists. If you attempt to add a URL to the **Block List** or **Exceptions to the Block List** and it already exists in the other list, IWSVA prevents the addition and displays a warning message stating that the entry already exists in the other list.

To configure URLs to block:

1. Click **HTTP > URL Access Control > Global URL Blocking**.
2. Select "**Enable URL blocking**."
3. On the **URL Blocking** page, type the full Web address or URL keyword, or exact-match string in the **Match** field.

   To identify a folder or directory in a given Web site, use a forward slash (/) after the last character. For example, if you want to block `www.blockedsite.com` but allow access to its `charity` directory:

   a. Type `www.blockedsite.com` in the **Match** field, then click **Block**.

   b. Type `www.blockedsite.com/charity/` in the **Match** field, and click **Do Not Block**. (If you write `charity` without the forward slash, IWSVA considers `www.blockedsite.com/charity` as a file.)

   Note: For HTTPS decryption policies, the strings to match vary depending on whether you set IWSVA in proxy or transparency mode.
   - In proxy mode, IWSVA matches the domain names, not the full URL. Thus, you only need to specify the domain names.
   - In transparency mode (WCCP or bridge mode), IWSVA matches both the CommonNames and URLs. You must include these in the blocking list if you want to block an HTTPS site.

4. Click **Remove** to remove the highlighted entries from the list (or **Remove All** to remove all entries).
5. Click **Save**.

Importing a List of Blocked URLs from a File

IWSVA can import a list of URLs to block from a file. Type a descriptive title or comment on the first line of a file that contains a list of Web sites, URL keywords, or strings, and then write one rule per line. Group sites to be blocked under `[block]` as shown in the example, and group exceptions under `[allow]`. For example:

```
URL Blocking Import File {this title will be ignored}

[block]
www.blockedsite.com*
unwanted.com*
```

```
urlkeyword
banned.com/file
banned.com/downloads/

[allow]
www.blockedsite.com/file
www.unwanted.com/subsite/
www.trendmicro.com*
```

To include the "*" and "?" characters in a URL blocking string rather than having IWSVA consider them as wildcards, use variable %2a or %2A to represent ***** and variable %3f or %3F to represent **?**. For example, to block `www.example.com/*wildcard` literally, specify the blocking rule as `www.example.com/%2awildcard` instead of `www.example.com/*wildcard`.

If importing the list is not successful, verify that you have followed the specified format for the URL Blocking import file before contacting customer support. Be sure you have:

- Listed blocked entries under `[block]` and exceptions under `[allow]`
- Formatted entries containing wildcards described in this document or Online Help

To import a list of URLs to block:

1. Format a text file as described with the URLs to block, along with any exceptions.
2. Click **HTTP > URL Access Control > Global URL Blocking** on the main menu.
3. Specify the location of the file to import in the "**Import block list and exceptions"** field by clicking **Browse**, and clicking **Import**.
4. Click **Save**.

Chapter 11

URL Filtering

This chapter presents an overview and workflow of the InterScan Web Security Virtual Appliance (IWSVA) URL filtering module with procedures for creating and configuring URL filtering policies.

URL filtering, along with Web Reputation, is part of the multi-layered, multi-threat protection solution provided by IWSVA (see Overview of URL Access Control on page 10-4).

Topics in this chapter include the following:

Introducing URL Filtering

The default settings for the IWSVA URL filtering module assume that your organization's primary interest is to avoid legal liabilities associated with viewing of offensive material and/or prevent employee abuse of non-business websites. However, because there are instances that require exceptions, additional policies can be created to allow access to restricted category groups for employees whose job functions require broader access. For example, members of the Human Resources or IT departments might need unrestricted Internet access to conduct investigations into violations of your organization's acceptable Internet use policies.

IWSVA supports the Safe Search feature provided by search engine filtering providers (such as Google and Yahoo). Safe Search is used to filter adult sites and content from the search results and helps protect children from exposure to adult material.

In addition, IWSVA provides enhanced filtering by combining dynamic filtering with the advanced Web Reputation databases. Browsing Web sites related to online trading, shopping, auction bidding, dating, gambling, and other non-work related activities during work time reduces employee productivity and decreases bandwidth available for legitimate browsing. IWSVA allows Internet access to be customized according to user and workgroup-specific needs, thus optimizing the use of the Internet.

See **HTTP > URL Filtering > Policies | policy | Rule** tab.

IWSVA's URL filtering policies provide a granular and flexible mechanism to manage Internet access. Each policy has three basic elements that include the following:

- IWSVA access to the Web Reputation database that contains URLs in over 82 categories, such as "gambling," "games," and "personals/dating." Categories are contained in the following logical groups:
  - Custom Categories
  - Network Bandwidth
  - Internet Security
  - Communications and Search
  - Adult
  - Business
  - Lifestyle
  - General

- Access to Web sites in each category can be allowed, blocked, or monitored during time periods designated as scheduled time object.
- Different policies can be configured for different users in your environment.

Access to all identified URLs within a targeted category might be managed according to policy. The database associates each URL with one or more categories. To accurately define a Web site, the URL may belong to multiple URL categories. For example, a shopping site that contains malware may belong to the Shopping category as well as the Malware Accomplice category. Depending on how many URL categories the URL falls into, the URL filtering policy may manage the access differently. If a URL that your organization needs to access is associated with a prohibited category, you can create exceptions to URL filtering rules to override the database's classification. The patterns specified in the Approved URL List are matched against the URL, not to the content of the document to which the URL refers. IWSVA gives you the option of configuring a URL filtering approved-list by matching Web site, URL keyword, and exact-string categories.

Another way to bypass IWSVA's default URL categorization is to create Custom Categories and assign the necessary access privileges to allow user access.

URL Filtering Actions

The following are the filtering actions that you can apply for a given policy with a scheduled time object:

- **Allow**—Connection to the target server is allowed and users can access the Web site.
- **Block**—Connection to the target server is not established and users are not allowed to access the Web site. A log entry is also created for this event.
- **Match Next Policy**—Connection to the target server depends on the policy configured at the next level.
- **Block with Override**—Connection to target service is not established unless the user can type a specific password to override the category blocking.

Note: When you apply the "block with override" action to categories, administrators need to configure the password used for overriding when creating the policy.

- **Monitor**—Connection to the target server is allowed and users can access the Web site. A log entry is also created for this event.
- **Time Limit**—Connection to the target server which accesses selected categories of URLs is allowed for the period of time configured by the administrator.

Note: 1. Selecting the “Time Limit” action for categories requires administrators to enter a value in “Time quota” text box in the Time Limit Settings section under the list of categories.

2. The default quota unit is five minutes. Trend Micro recommends that administrators set the “Time quota” value to a multiple of five. Otherwise, IWSVA ignores the remainder less than five. For example, if the value is set to 4 minutes, IWSVA interprets that as 0 minutes. If the value is set to 9 minutes, system interprets that as 5 minutes.

- **Warn**—Connection to the target server is allowed but a notification displays, warning users that the URL about to be accessed belongs to a category that violates company policy. Users have the option of continuing to the page or going back to the previous page.

URL Filtering Workflow

The input for URL filtering consists of the URL and the user’s ID (IP address, IP address range, user name, group name, or host name). A user is identified according to the user identification method that IWSVA is configured to use (see Configuring the User Identification Method starting on page 8-6).

A URL requested by a user can be classified into one or more of 82-plus categories, which are organized into 7 pre-defined groups. IWSVA passes the requested URL through IWSVA's URL filtering engine to be filtered according to their policies for the user making the request. Based on the category to which the requested URL belongs and the policy's action, the URL can be allowed, blocked, monitored or issued a warning.

Note: Manual updates to the URL filtering engine can be done from the **Manual Update** screen.

Managing URL Filtering Policies

IWSVA is pre-configured with two default URL filtering policies—the Global Policy that applies to all clients on the network, and the Guest Policy that applies to clients that access IWSVA with a guest account.

Note: The Guest Policy is only supported if you have configured IWSVA as follows:
- Allow guest access using Captive Portal as Authentication Method
- Enable the guest user login port after selecting the forward proxy mode in the Deployment Wizard

Enabling URL Filtering

Make sure that the URL filtering module is enabled before you start. The Account fields support IPv6 addresses. You can define one rule for any IPv6 host, and this policy rule is triggered when the client accesses Web sites through IWSVA.

When selecting policies, both IPv4 and IPv6 policies will appear. In the Account field, acceptable account entries include a single IPv6 address, an IPv6 range, or an IPv6 mask similar to what has been supported with IPv4.

IWSVA supports the “URL Warn mode” feature with IPv6, and can automatically redirect the warning message to IWSVA’s IPv6 or IPv4 addresses to the client based on the version of the client’s IP address.

- When a client uses an IPv4 address, IWSVA sends a redirect request with IWSVA’s IPv4 address.
- When a client uses an IPv6 address, IWSVA sends a redirect request with IWSVA’s IPv6 address.

To enable URL filtering:

1. Click **HTTP > URL Filtering > Policies** from the main menu.
2. Select **Enable URL filtering**.
3. Click **Save**.

Enabling Dynamic URL Categorization

Interscan Web Security Virtual Appliance (IWSVA) uses Trend Micro URL Filtering Engine (TMUFE) to filter URLs. If an accessed URL is not present in the TMUFE database, IWSVA uses Dynamic URL Categorization technology to perform real time categorization of the Web site based on the Web site content and HTTP URL.

Dynamic URL Categorization uses a pattern file that contains key words, rules and other information to filter out Web sites.

To enable dynamic URL categorization:

1. Click **HTTP > URL Filtering > Policies** from the main menu.
2. Select **Enable Dynamic URL Categorization**.
3. Click **Save**.

Creating a New Policy

Creating a new URL filtering policy is a four-step process:

- Select the accounts to which the policy applies.
- Specify the Web site categories to be allowed, blocked, monitored or warned during the time defined in scheduled time object.
- Select a Safe Search setting
- Select an exception list

To create a new policy:

1. Open the IWSVA Web console and click **HTTP > URL Filtering > Policies** from the main menu.
2. Click **Add**.

   The **URL Filtering Policy: Add Policy** screen appears.
3. Type a descriptive **Policy name**.

   Policy names that include references to the users or groups to which they apply, for example, "URL Filtering Policy for Researchers," are easy to remember.
4. Select the users to which the policy applies.

   The options on this page depend upon the user identification method that you are using—either *IP address*, *Host name (modified HTTP headers),* or *User/group name authentication*. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method starting on page 8-6.

5. Click **Next**.
6. On the **Specify Rules** screen, ensure that **Enable policy** is selected.
7. Select one of the following filtering actions for each URL category or sub category:
    - **Allow**—Connection to the target server is allowed and users can access the Web site.
    - **Block**—Connection to the target server is not established and users are not allowed to access the Web site. A log entry is also created for this event.
    - **Match Next Policy**—Connection to the target server depends on the policy configured at the next level.
    - **Block with Override**—Connection to target service is not established unless the user can type a specific password to override the category blocking.
    - **Monitor**—Connection to the target server is allowed and users can access the Web site.
    - **Time Limit**—Connection to the target server which accesses selected categories of URLs is allowed for the period of time configured by the administrator.
    - **Warn**—Connection to the target server is allowed but a notification displays, warning users that the URL about to be accessed belongs to a category that violates company policy. Users have the option of continuing to the page or going back to the previous page.
8. Select to apply the filtering action during the time defined in scheduled time object.
    - **Action During/Scheduled Times**—Select the filtering action to apply and then set the schedule. To select all the categories of a group, click the check box for the group. The group does not need to be expanded for you to select all categories in a group. Restricted days and hours are defined in the URL Filtering Settings (Schedule tab) page. For more information, see Scheduled Time Settings on page 11-12.
9. Click **Apply** to apply the filtering action to the selected categories.

Note: Repeat steps 8 and 9 if you want to apply a different filtering action to sub-categories in the same group.

10. (Optional) In the **Password Override Settings** section, you must enter the password used for the overriding the blocking action. This is only necessary if you configure a policy to use the "Block with Override" action setting for a URL Filtering category.

    Note: Passwords are policy-specific.

11. Type an optional **Note** to include useful information about this policy for future reference.
12. Click **Next**.
13. Select a Safe Search setting for each search engine and click **Next**.
    - **Strict**—Filters out adult contents from all search results (including image, video, and Web search).
    - **Moderate**—Filters out adult contents from Web search results only (excluding image search).
    - **Off**—Does not filter search results. This is the default setting.
14. In the **Specify Exception Lists** screen, select an approved URL list name from the drop-down list box if you want to apply an exception list. URLs in the exception list will bypass URL filtering.
15. Click **Save**.
16. In the **URL Filtering Policies** screen, set the priority of the new policy (under the **Priority** column) by clicking on the up or down arrows.

    The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies. For accounts that belong to more than one policy, IWSVA will execute the policy on a first match bases. Policies that contain the account after the first match policy is executed are skipped.
17. Click **Save**.
18. To immediately apply the policy, click **Deploy Policies Now**; otherwise, the policy is applied after the database cache expires.

Modifying and Deleting Policies

IWSVA gives you the option of editing any existing policy to better suit your current environment. You can also delete unnecessary account(s) from a policy.

To modify an existing policy:

1. Click **HTTP > URL Filtering > Policies** from the main menu.
2. Click the **Account Name** or **Policy Name** links of the policy to be modified.
3. The **URL Filtering Policy: Edit Policy** screen opens.
    - Change the scope of your policy by adding or deleting clients on the **Account** tab.
    - From the **Rule** tab, modify filtering action for the URL categories.
    - From the **Safe Search Engine** tab, change the Safe Search mode for each search engine.
    - From the **Exception** tab, select an exception list that you want to apply to this policy.
4. Click **Save**.
5. Go to **HTTP** > **URL Filtering > Policies** and set the priority of your policies using the arrows. The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies.
6. Click **Save**.
7. Click **Deploy Policies** to immediately apply the policy; otherwise, the policy is applied after the database cache expires.

URL Filtering Settings

There are several settings related to URL filtering that you can modify to reflect the realities of your work environment:

- Over 82 predefined Web site categories, organized in seven (7) logical groups
- Configuring your own custom categories
- Select the time object defined in “Scheduled Times.”

Additionally, if you believe a URL is classified in the wrong category, you can send a request to Trend Micro to consider re-classifying the URL. You can also look up the category of a URL that you are not sure of.

Creating Custom Categories

You can define new URL categories in addition to the categories already provided by Trend Micro. For example, you can create a category called "Competitor's Web site" that contains the URLs of your company's competitors.

The **HTTP > Configuration > Custom Categories** screen displays a list of user-defined categories. Click **Add** to create a new one or click a category name to edit an existing one.

- **Category Name**—Type a brief but descriptive name for the custom category. Names must be unique.
- **Match**—Enter a Web site, a keyword or phrase, or a string of characters in the field, and then tell IWSVA how to apply the match. This field supports both the ? and * wildcards. Entries in this field are added one-by-one to the custom category.

Note: For HTTPS decryption policies, the strings to match vary depending on whether you set IWSVA in proxy or transparency mode.
- In proxy mode, IWSVA matches the domain names, not the full URL. Thus, you only need to specify the domain names.
- In transparency mode (WCCP and Bridge mode), IWSVA matches the CommonNames in the server certificates received.

  - **Web site**—Limits the search to the string as a whole; used with one or more wildcards, this type of setting can be especially useful for applying the configured URL filtering action to an entire Web site. There is no need to include http:// or https:// in the URL (it is automatically stripped).
  - **URL keyword**—Looks for any occurrence of the letters and/or numbers within a URL, and will match regardless of where the string is found (the string "sex" would be considered a match for "http://www.encyclopedia/content/sexton.htm" and the page blocked). Using wildcards in this field greatly increases the chance of false positives and unexpected results.
  - **String**—Limits the search to the string as a whole, for example to target a specific site, page, file, or other particular item.

- **Import Custom Category List**—You can import an existing list of URLs that you want to add to a category. For example if you have a list of your competitors' URLs you have compiled using a text editor, you can import the list rather than enter them one-by-one. Imported lists must conform to a defined standard (refer to the Online Help for more information).

Requesting URL Reclassification and URL Lookup

Organized in seven logical groups, IWSVA includes default categories that provide a baseline level of URL filtering. For example, Web sites related to humor and jokes would be found in the "Joke Programs" category, which is located in the *Internet Security* group.

If you do not agree with the default classification of a URL, Trend Micro enables you submit a request for a reclassification. You can also use the Exception List or Custom Categories to bypass domain and Web site ratings categorized by Trend Micro's URL filtering database.

Before rolling out URL filtering policies, Trend Micro recommends verifying that the default categorizations are appropriate for your organization. For example, a clothing retailer might need to remove a swimsuit Web site from the "Intimate Apparel/Swimsuit" category located in the *Adult* group in order to allow legitimate market and competitor research.

If you want to know a category of a URL, you can look it up when specifying URL filtering settings in the **HTTP > URL Filtering > Settings | URL Reclassification & Lookup** tab.

Unrated and Unknown URLs

An *unrated* URL is a Web site that Trend Micro knows about but has not yet put into a filtering category.

An *unknown* URL is a Web site that is one of the following:

- Unknown to Trend Micro
- A Web site that is not in the Web Reputation database
- The daemon might be down or the remote rating server is inaccessible to give the URL a rating

An unknown URL has a rating of zero (0) and cannot be blocked.

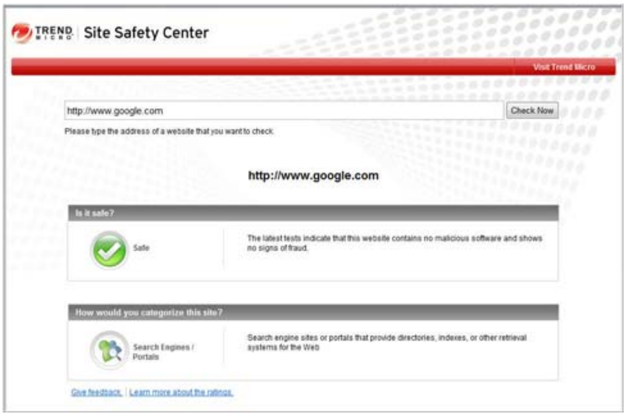
Requesting a Reclassification

To request a URL reclassification:

1. Click **HTTP > URL Filtering > Settings** from the main menu.
2. Click the **URL Reclassification & Lookup** tab.
3. Click on the link to the Trend Micro Site Safety Center.

   The Trend Micro Online URL Query - Feedback System screen appears.
4. Enter the suspect URL in the field and click **Check Now.**

   Figure 11-1 shows the results from an approved URL.



http://www.google.com

Please type the address of a website that you want to check

http://www.google.com

The latest tests indicate that this website contains no malicious software and shows no signs of fraud.

Search engine sites or portals that provide directories, indexes, or other retrieval systems for the Web

FIGURE 11-1. Trend Micro Online URL Query - Site Safety Center screen

5. To suggest a change, click **Give Feedback** and type the necessary information.

Scheduled Time Settings

IWSVA enables you to specify the settings of the days and hours you want to set for different actions.

When creating URL filtering policies, set a policy to take effect for specific time range.

Note: It is assumed that all IWSVA devices in a cluster are within the same time zone.

Before implementing URL filtering policies in your organization, Trend Micro recommends creating a new time object for your time schedule.

To configure the URL filtering policy schedule:

1. Open the IWSVA Web console and click **Administration > IWSVA Configuration > Scheduled Times**.
2. Specify the time object name and description. Select the time period in which you would like to apply the action.
3. Click **Save**.

URL Access Warning TTL

The URL Access Warning Time-to-Live (TTL) setting allows the administrator to configure the amount of time between displayed warning messages, if the user chooses to be reminded after the initial warning messages displays.

Note: The repeated warning message only occurs if the user opts to continue to a Web page after the initial warning message.

To configure URL access warning TTL, navigate to **HTTP** > **URL Filtering** > **Settings** > **URL Warning TTL** tab, and change the URL Access Warning Time-to-Live (TTL) setting here.

The default value is 5 minutes. This setting is configured per user/per category.

The warning message displays if the value for the policy rule's selected action is set to Warn. See Creating a New Policy on page 11-6 for more information.

See Configuring URL Access Warning Notifications on page 14-35 for more about the notifications.

URL Filtering Exceptions

IWSVA provides the option to configure exceptions to URL filtering by approved lists (see Specifying the Exceptions List on page 9-70). URLs in the exception list will not be blocked or monitored. If your clients have a legitimate need to view Web sites that are being blocked or monitored by URL filtering, include the URL to an approved URL list and apply the list to the policy.

Note: IWSVA still applies Safe Search filtering to Web sites in the approved URL list.

To apply an approved URL list to a URL filtering policy:

1. Open the IWSVA Web console and click **HTTP > URL Filtering > Policies** and click a policy name to edit it.
2. In the **Exceptions** tab, select the approved URL list name.

   Note: URLs in the exception list will not be warned. For more information, see Configuring URL Access Warning Notifications on page 14-35.

3. Click **Save**.

URL Filtering Time Quota Extension

The Time Quota extension is for the URL Filtering policies with a "Time Limit" action. If an IWSVA system admin would like to allow Internet browsing to continue for an individual after the time limit has been exhausted, the time period can be extended here. Users will receive a notification if the time quota has been reach. A log is recorded for users who exhaust their quotas.

This page shows the following information:

- **User**—Identifies user by name or IP address. Admins can also search for a user or sort by the users name.
- **Daily Time Quota Allotment**—Displays time allotted in a policies for the amount of time that can be used for browsing.
- **Extend Time Given**—Displays extended time given already, if any.
- **Daily Time Quota Used**—Displays the total of time used browsing, which may include the original time allotted plus any time extensions, or portions of time extensions that have been used.
- **Extend Quota**—Provides a place to configure the extension with:
  - **Check box**—Check to extend time
  - **Amount**—Numeric value of extension
  - **Units of measure**—Time in minutes or hours for the extension

Note: Time can only be extended for URL Filtering policies that have the "Time Limit" action as part of the policy rule.

To extend the allotted time for Internet browsing:

1. Go to **HTTP > Access Quota Policies > Time Quota URL Filtering Extension**.
2. Find the appropriate user by sorting the User column or using the search field.
3. Go to the Extend Quota column in the row of the appropriate user.
4. Check the check box to allow time to be extended.
5. Type the number of minutes or hours the extension will encompass and select the appropriate unit of time (hours or minutes).
6. Click **Save** for the extension to take effect.

Chapter 12

FTP Scanning

This chapter describes FTP virus scanning and the different ways FTP scanning can be deployed and configured for your environment.

Topics in this chapter include:

Introduction

InterScan Web Security Virtual Appliance (IWSVA) can scan FTP uploads and downloads for viruses and other malicious code in a manner similar to how it processes HTTP traffic. Unlike HTTP scanning, however, a single configuration is applied to all clients on your network—user or group-based policies are not supported for FTP scanning.

IWSVA FTP scanning uses either a stand-alone proxy or works in conjunction with another FTP proxy on the network. To deploy FTP scanning into your environment, first configure the FTP settings that control the type of proxy and the type of data connection (either passive or active FTP; see Passive and Active FTP starting on page 12-3). The next step is to configure the scanning rules that control the traffic direction that is scanned, the type of files to block or scan, how compressed and large files are handled, and the actions taken when malicious code is detected.

After setting the FTP scanning settings, there are optional security and performance settings to consider modifying. Access control lists can be configured to selectively allow client FTP access based on the client's IP address. To improve performance when frequently accessing FTP sites over which you have direct control of the content, specific FTP servers can be added to an approved list so that downloads from them are not scanned. Moreover, to further lock down the IWSVA device, FTP access to specific ports can either be allowed or denied.

Note: IWSVA does not support active FTP scanning in WCCP mode.

FTP Settings

IWSVA FTP scanning settings include options for using either the IWSVA native (stand-alone) proxy or a separate FTP proxy, two options for how data connections are made (active FTP vs. passive FTP).

Proxy Settings

IWSVA FTP scanning provides two proxy setting options—a "stand-alone" mode whereby clients connect to the native IWSVA proxy that later connects with the FTP server, and an "FTP proxy" mode whereby IWSVA passes requests through a separate FTP proxy that in turn connects to the FTP server.

- In stand-alone mode, the client needs to use `<username>@<FTP server name>` as the FTP username to indicate which FTP server IWSVA should connect to.
- In FTP proxy mode, no username is required because IWSVA always connects to the FTP proxy and server designated in the configuration settings.

FTP proxy mode can also be used to protect a single FTP server by specifying the FTP server's hostname/IP address and port number in the FTP proxy configuration. In this case, the IWSVA FTP scanning module is dedicated to the specified FTP server, in a manner similar to a reverse proxy for HTTP scanning.

Passive and Active FTP

IWSVA uses either active or passive FTP for data connections, depending on your firewall setting. FTP uses two ports, a data port and a command port. In *active* FTP, the server connects to the client to establish the data connection. In *passive* FTP, the client connects to the server.

When passive FTP is selected in the IWSVA configuration, IWSVA converts the "active" mode on the client side into the "passive" mode on the server side. Mode conversion is performed only when the IWSVA configuration is passive and the client uses the active mode. If the IWSVA configuration is active, no conversion is performed, so passive requests from the client are still passive requests on the server side.

Client Requests

To configure the FTP settings, you need to specify the proxy settings and the data connection.

The FTP Proxy supports IPv6 FTP Proxies similar to the support of the IPv4 FTP Proxy, and the Web UI accepts both IPv4 and IPv6 addresses.

You can have IWSVA act as an FTP proxy server. If you need to protect FTP uploads on multiple servers, install one instance of the IWSVA FTP module for each server.

To configure the FTP settings:

1. Click **FTP > Configuration > General** from the main menu.
2. Under the **Proxy Settings** section, select the appropriate FTP setting based on your topology—either **Use stand-alone mode** if you want the native IWSVA proxy to connect to FTP sites, or **Use FTP proxy** for the FTP service to work with an existing FTP proxy (specify the host name of the **Proxy server** and the **Port**).
3. Choose the type of data connection to use—either **Passive FTP** or **Active FTP**.
4. Click **Save**.

FTP Scanning Options

IWSVA can scan FTP traffic for both IPv4 and IPv6 servers based on predefined policies.

For the Proxy Deployment mode, IWSVA supports the deployment scenarios that follow and can auto-transition for FTP, HTTP, and HTTPS traffic between the IPv4 and IPv6 networks when deploying IWSVA as a dual stack network environment. This means the IPv4 client can also access an IPv6 server or an IPv6 client can access an IPv4 host with an IWSVA proxy along with an IPv4 client accessing an IPv4 client and an IPv6 client access IPv4 server.

TABLE 12-1. Proxy Deployment Mode Scanning Scenarios Supported

NO.	CLIENT	SERVER	SUPPORTED (Y/N)
1	IPv4	IPv4	Y
2	IPv6	IPv6	Y
3	IPv4	IPv6	Y
4	IPv6	IPv4	Y

For other supported deployment modes, IWSVA cannot transition between IPv4 and IPv6 networks as the following table shows.

TABLE 12-2. Other Deployment Mode Scanning Scenarios Supported

NO.	CLIENT	SERVER	SUPPORTED (Y/N)
1	IPv4	IPv4	Y
2	IPv6	IPv6	Y
3	IPv4	IPv6	N
4	IPv6	IPv4	N

The FTP virus scanning settings are similar to the HTTP scanning settings, with two differences:

- FTP scanning does not support user or group-based policies; therefore, one configuration is applied to all clients that access the FTP sites through IWSVA.
- The traffic direction to scan can be configured—either to uploads, downloads, or both.

Enabling FTP Traffic and FTP Scanning

Before your clients can access the FTP sites through IWSVA, the FTP traffic must be enabled.

To enable or disable FTP scanning:

1. Open the IWSVA Web console and click **FTP > Scan Rules**.
2. Select **Enable FTP scanning**.
3. Click **Save**.

Scan Direction

Depending on how you want to use IWSVA FTP scanning, you can selectively configure the FTP scanning module to scan uploads, downloads or both. For example, if you have deployed antivirus software to all of the workstations in your organization, disabling uploads might be justified to achieve a performance benefit, because the files should already be scanned on the client.

File Blocking

You can specify the types of files to block for security, monitoring or performance purposes. You can block file types such as Java applets, Microsoft Office documents, audio/video files, executables, images, or other types that you can manually configure. If your organization has policies that prohibit certain types of files in your network, IWSVA FTP file blocking can stop them at the FTP gateway.

File Scanning

When configuring the types of files to be scanned, there are three options:

- **All scannable files:** All files are scanned (the safest option).
- **IntelliScan:** Only file types known to harbor viruses are scanned (file type is determined by checking the file header). See About IntelliScan starting on page 9-54 for more information.
- **Specified file extensions:** Only files with specified file extensions are scanned.

Trend Micro recommends scanning all files, unless performance considerations require choosing one of the other options. See *Configuring FTP Scanning Settings* on page 12-8 for more information.

Priority for FTP Scan Configuration

If the configurations on the **FTP Virus Scan** screen conflict with each other, the program scans according to the following priority:

1. Block these file types
2. Scan these file types (if not blocked)

Intellitrap

Detects potentially malicious code in real-time, compressed executable files that arrive with HTTP data. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of compressed files that help reduce the risk that a virus compressed using these methods will enter a network through the Web. Malicious, compressed executable files receive the actions specified in the Action tab. IntelliTrap is enabled by default.

Compressed File Handling

Compressed files can pose special challenges to antivirus software performance, because they must be decompressed before the individual files within the archive can be scanned. IWSVA provides the option to block, quarantine, or pass all compressed files at the gateway.

Alternatively, you can also configure IWSVA to apply the selected action on compressed files that meet one of the following conditions:

- Decompressed file count exceeds a given threshold
- Cumulative decompressed file size exceeds a configured maximum
- Recursively compressed file exceeds a certain number of compressed layers

Note: IWSVA can also block specified file types within a compressed file during FTP scanning.

Large File Handling

If the delay when downloading large files is unacceptable, IWSVA can be configured to skip scanning of files larger than a configured threshold. Additionally, the FTP scanning module can use the “deferred scanning” method for large files to prevent the client connection from timing out. See Deferred Scanning starting on page 9-62 for more information.

Note: The FTP scanning module does not support the “scan before delivering” large file handling methods used by the HTTP scanning module.

Encrypting Quarantined Files

If IWSVA is configured to quarantine files as a scan action, it can optionally encrypt the files to prevent them from accidentally being executed by someone browsing the quarantine folder. Note that after encrypted, the files can only be decrypted by a representative from Trend Micro's Support department.

Scanning for Spyware/Grayware

IWSVA can scan for many additional non-virus risks for which patterns are contained in the spyware/grayware pattern file. For a summary of these risks, see Spyware and Grayware Scanning Rules starting on page 9-66.

Data Loss Prevention

IWSVA can scan for data loss using the policies you create in **HTTP > Data Loss Prevention > Policies**. In **FTP > Scan Rules | Data Loss Prevention** tab, select the name of the DLP template and then modify scan criteria based on whether you would like allow, block or monitor using specific filtering you apply.

FTP Scanning Exception List

You can apply an approved list that contains the names of files that you want to exempt from file type blocking. In addition, you can configure IWSVA to bypass virus/spyware scanning and compressed file handling action on files in an approved list.

For more information, see Specifying the Exceptions List on page 9-70.

Configuring FTP Scanning Settings

To configure FTP scanning:

1. Click **FTP > Scan Rules** from the main menu.
2. Select **Enable FTP scanning**.
3. Select the types of FTP transfers to scan—either **Upload**, **Download**, or both.
4. Under the **Block these file types** section, select the file types to be blocked.
5. Select the files to scan:

- To scan all file types regardless of extension, select **All scannable files**. IWSVA opens compressed files and scans all files within. Scanning all files is the most secure configuration.
- To use true-file type identification, select **IntelliScan**. IntelliScan uses a combination of true attachment type scanning and exact extension name scanning. True attachment type scanning recognizes the file type even when the file extension has been changed. IntelliScan automatically determines which scanning method to use.
- To scan file types based on their extensions, select **Specified file extensions**. This contains the list of file types known to harbor viruses. IWSVA scans only those file types that are explicitly specified in the **Default Extensions** list and in the **Additional Extensions** text box. The default list of extensions is periodically updated from the virus pattern file.

  Use this option, for example, to decrease the aggregate number of files IWSVA checks, therefore, decreasing the overall scan times.

Note: There is no limit to the number or types of files you can specify. Do not precede an extension with the (*) character. Delimit multiple entries with a semicolon.

6. Under **Compressed file handling**, select an action (Block, Quarantine, or Pass) and select to apply the action to one of the following:
   - All compressed files
   - Compressed files if

   If you enable the second option, type a value for the following parameters:
   - Decompressed file count exceeds (default is 50000)
   - Size of a decompressed file exceeds (default is 200MB)
   - Number of layers of compression exceeds (0-20, default is 10)
   - Compression ratio of any file in the archive exceeds 99 percent
7. Under **Large File Handling**, select **Do not scan files larger than** and enter the file size.
8. To avoid browser time-out issues when downloading large files, select **Enable Deferred Scan** and type the file size above which deferred scanning occurs. Also, select from the drop-down list the percentage of data to be sent to the client unscanned.

WARNING! The partial delivery of a file might result in a virus leak; therefore, this would be a performance versus an absolute security choice for you. Use this option only when you are currently experiencing an issue with time-outs.

9. To encrypt files sent to the quarantine directory to prevent them from being inadvertently opened or executed, select **Encrypt quarantined files**.
10. Click **Save** and switch to the **Spyware/Grayware Scan Rule** tab.
11. Select the types of additional risks to scan for, and click **Save**.
12. In the **Data Loss Prevention** tab, select a DLP Template you have previously created at **HTTP > Data Loss Prevention > Policies** from the DLP Template list.
13. Modify filtering rules and determine whether to Scan, Block, or Monitor with the filter. Click **Save**.
14. In the **Exceptions** tab, select an approved file name list from the drop-down list.

    Select **Do not scan the contents of selected approved lists** if you do not want to scan the contents of the files in the approved lists for viruses. In addition, compressed file handling action will not be applied.
15. Switch to the **Action** tab, and select the actions for IWSVA to take in response to scanning.
16. Click **Save**.

Setting Scan Actions on Viruses

FTP > Scan Rules > Action tab **Infected files** -You can specify the action for FTP scanning to take upon finding an infected file (the recommended action setting is **Clean**):

- Choose **Quarantine** to move an infected file to the quarantine directory without cleaning. The requesting client does not receive the file.
- Choose **Delete** to delete an infected file. The requesting client does not receive the file.
- Choose **Clean** to automatically clean and process an infected file. The requesting client receives the cleaned file if it is cleanable.

Uncleanable Files - You can specify the action for FTP scanning to take upon finding an uncleanable file, which includes worms and Trojans (the recommended action setting is **Delete**):

- Choose **Pass** to send an uncleanable file to the client without cleaning (Trend Micro does not recommend this choice, because it might allow infected files into your network).
- Choose **Quarantine** to move, without cleaning, an uncleanable file to the quarantine directory. The requesting client does not receive the file.
- Choose **Delete** to delete an uncleanable file. The requesting client does not receive the file.

Password-protected File - You can specify the action for FTP scanning to take in handling a password-protected compressed file (the recommended action setting is **Pass**):

- Choose **Pass** to send a password-protected file to the client without cleaning.
- Choose **Quarantine** to move, without cleaning, a password-protected file to the quarantine directory. The requesting client does not receive the file.
- Choose **Delete** to delete a password-protected file. The requesting client does not receive the file.

Macro - In the event a file containing macros (not necessarily macro viruses) is detected during FTP transfers, the following actions are available (the recommended action setting is **Pass**).

- Choose **Quarantine** to move the files containing macro(s) to the quarantine directory.
- Choose **Clean** to remove macros before delivering the file.
- Choose **Pass** to disable special handling of files containing macro(s).

FTP General Configuration Settings

To configure the FTP settings, you need to specify the proxy settings and the data connection.

The FTP Proxy supports IPv6 FTP Proxies similar to the support of the IPv4 FTP Proxy, and the Web UI accepts both IPv4 and IPv6 addresses.

You can have IWSVA act as an FTP proxy server. If you need to protect FTP uploads on multiple servers, install one instance of the IWSVA FTP module for each server.

Proxy Settings

- **Use stand-alone mode**—Choose this option when IWSVA is installed as the only FTP proxy on the network.
- **Use FTP Proxy**—Choose this option if IWSVA is installed on a network with an existing FTP proxy; IWSVA may be on the same machine as the FTP proxy or a different one, which will affect the values you enter for the following fields:
    - **Proxy server**—Specify the host name or IP address of the FTP proxy that IWSVA receives FTP traffic from; If IWSVA FTP scanning is installed on the same machine as the FTP server, use "localhost"
    - **Port**—Indicates the port number that the FTP proxy uses to deliver FTP traffic to IWSVA, typically, port 21

Data Connection

Because most firewalls are configured to reject unsolicited port requests from outside the LAN, IWSVA supports both Active and Passive file transfers. Passive transfers are usually necessary if there is a firewall on the LAN, or if you have experienced failed data channels when trying to setup Active FTP.

Click **FTP > Configuration > General** from the main menu.

- **Passive FTP**—Choose this option if IWSVA is running inside a firewall that allows only Passive FTP.

  In Passive FTP (or PASV mode), the FTP client initiates contact with the FTP server. The FTP server tells the client to which port to connect for data transfer and the client opens another connection to the server on this port.
- **Active FTP**—Choose this option if IWSVA was installed as a Stand-alone, is running inside a firewall that allows Active FTP, or if it was installed to be running outside the firewall (not recommended).

  In Active FTP, the FTP client initiates contact with the FTP server and then negotiates a mutual data transfer port. (Port 22020 is usually used in IWSVA.) The server connects back to the client using the negotiated port.

Note: Your firewall must be able to open this port dynamically and let the FTP server communicate with the client, or you must manually open the port.

Note: The maximum number of client requests and number of worker threads to create can be manually configured by editing the `/etc/iscan/intscan.ini` file.

FTP Access Control Settings

IWSVA includes several access control settings for additional security and performance tuning:

- FTP access can be enabled based on the client's IP address.
- Trusted servers over which you have close control of their content and are frequently accessed can be added to an approved list and transfers are not scanned for a performance benefit.
- The IWSVA FTP server can be locked down by denying access to ports that you configure.

By Client IP

By default, all clients on the network are allowed to access FTP sites through the IWSVA device (provided FTP traffic is enabled, see Enabling FTP Traffic and FTP Scanning starting on page 12-5).

When selecting policies, both IPv4 and IPv6 policies will appear. Client Access Control accepts a single IPv6 address, an IPv6 range, or an IPv6 mask similar to what has been supported with IPv4.

To limit FTP access based on client IP address:

1. Click **FTP > Configuration > Access Control Settings** from the main menu.
2. Switch to the **Client IP** tab.
3. Select **Enable FTP Access Based on Client IP**.
4. Enter the IP addresses of clients allowed FTP access through IWSVA. The following are acceptable entries:

- **IP**: a single IP address, for example, 123.123.123.12.
- **IP range**: clients that fall within a contiguous range of IP addresses, for example, from 123.123.123.12 to 123.123.123.15.
- **IP mask**: a single client within a specified subnet, for example, entering IP = 192.168.0.1 and Mask = 255.255.255.0 identifies all machines in the 192.168.0.x subnet. Alternatively, the Mask can be specified as a number of bits (0 to 32).

5. Type a descriptive name in the **Description** field. (40 characters maximum)
6. Click **Add** and continue entering other clients that are allowed to access FTP sites.
7. Click **Save**.

Via Approved Server IP List

To reduce possible performance issues when accessing trusted FTP sites over which you directly control the content, you can exempt some FTP sites from scanning by adding their IP addresses to an approved list.

Note: Skipping scanning through the IP approved list only applies to file downloads. Uploaded files are still scanned.

When selecting policies, both IPv4 and IPv6 policies will appear. Server Access Control accepts a single IPv6 address, an IPv6 range, or an IPv6 mask similar to what has been supported with IPv4.

To add trusted servers to the approved list:

1. Click **FTP > Configuration > Access Control Settings** from the main menu.
2. Switch to the **Approved Server IP List** tab.
3. Enter the IP addresses of FTP sites to exempt from IWSVA FTP virus scanning. See Identifying Clients and Servers starting on page 7-13 for information and examples about how to identify the servers.
4. Type a descriptive name in the **Description** field. (40 characters maximum)
5. Click **Add** and continue entering other FTP sites to exempt.
6. Click **Save**.

Via Destination Ports

By default, clients can access any port on the IWSVA FTP server. To increase security, you can selectively allow or deny access to the ports.

To configure IWSVA FTP ports to which clients can connect:

1. Click **FTP > Configuration > Access Control Settings** from the main menu.
2. Switch to the **Destination Ports** tab.
3. Choose the action to apply to a port, either **Deny** or **Allow**.
4. Enter the **Port** or **Port Range** to which the action applies.
5. Type a descriptive name in the **Description** field. (40 characters maximum.)
6. Click **Add**.
7. Continue to add other ports to allow or deny.
8. Click **Save**.

Note: The destination port list at the bottom of the **Destination Port** tab reflects the processing order (or reverse priority order). Destination port access control is only applied during an FTP command connection, and FTP data connections are not affected. A typical configuration is 1. “Deny ALL” and 2. “Allow 21” which results in only allowing access to port 21.

Chapter 13

Command Line Interface Commands

This chapter describes the Command Line Interface (CLI) commands that you can use in the InterScan Web Security Virtual Appliance (IWSVA) product to perform monitoring, debugging, troubleshooting, and configuration tasks.

CLI commands allow administrators to perform additional configuration tasks, such as enabling and disabling Squid caching, and to perform debug and troubleshooting functions. The CLI interface also provides additional commands to monitor critical resources and functions, such as monitoring the traffic that flows in or out of a network interface.

Topics included in this chapter are:

SSH Access

Access to the IWSVA CLI interface can be obtained through the IWSVA terminal (keyboard and monitor connected directly to the IWSVA server) or remotely using a SSH v2 connection to the management IP address. Before you access the CLI using SSH, you must first enable SSH access control in the Web console (**Administration > Network Configuration > Remote CLI**).

Preventing Password Brute Force Attacks through SSH

IWSVA can protect against password brute force attacks. If a remote terminal attempts to log on to IWSVA with the wrong password using SSH, IWSVA will reject subsequent log on attempts. This feature is enabled and disabled through the CLI.

To enable the anti-password brute force attack function:

1. Log on to IWSVA using the root, enable, or admin account. "root" and "admin" account users can log on using SSH, but the "enable" account users can only log on to the IWSVA local machine.
    - If logging on with the root account, type **`clish`** and **`enable`** to access the clish privileged mode.
    - If logging on with the admin account, type **`enable`** to access the clish privileged mode.
    - If logging on with the enable account, you are already in the clish privileged mode.
2. To enable the function, type the following command: **`configure service pswd_protection enable`**

To disable the anti-password brute force attack function:

1. Follow Step 1 in the previous procedure.
2. To disable the function, type the following command: **`configure service pswd_protection disable`**.

Command Modes

To access the command line interface, you will need to have the administrator account and password. IWSVA's CLI commands are separated into two categories—non-privileged and privileged commands.

Non-privileged commands are basic commands that allow the administrator to obtain specific low security risk information and to perform simple tasks. The non-privileged command prompt ends with an angle bracket (>).

Login to CLI from remote SSH - Login IWSVA CLI by admin account and password from remote SSH (only supports non-privileged commands).

Login to CLI at local SSH - Login local SSH as `root` account, run command `clish` to login CLI (only supports non-privileged commands).

Privileged commands provide full configuration control and advanced monitoring and debugging features. To use privileged commands, type `enable` and the password for the Enable account. The screen displays `enable#` as the privileged command prompt. To return to non-privileged commands, type `exit`.

Note: Some CLI commands are not available to child members of an HA cluster. because these parameters need to be configured through the parent member of the cluster. Some of the commands unavailable through the child server are: `configure system date`, `configure module ntp`, `configure system password`, `configure service ssh`, and `configure system timezone`

Command List

The following table lists the available commands:

TABLE 13-1. Command Line Interface Commands

COMMAND	SYNTAX	DESCRIPTION
configure module database password	configure module database password	Configure the database password

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module http bypass_non_http disable	configure module http bypass_non_http disable	Disable non-HTTP traffic bypass
configure module http bypass_non_http enable	configure module http bypass_non_http enable	Enable non-HTTP traffic bypass
configure module http scan_before_deliver_port	configure module http scan_before_deliver_port <port> [mgmt_interface]	Configure both IPv4 and IPv6 addresses for the redirecting port to scan before delivery. IPv4 and IPv6 redirect requests will be sent directly to the client.
configure module http x-forwarded-for action add	configure module http x-forwarded-for action add	Add the IP address of the last hop to the XFF HTTP header
configure module http x-forwarded-for action keep	configure module http x-forwarded-for action keep	Make no changes in the XFF HTTP header
configure module http x-forwarded-for action remove	configure module http x-forwarded-for action remove	Remove the XFF HTTP header from the HTTP request for upstream security
configure module http x-forwarded-for parse disable	configure module http x-forwarded-for parse disable	Disable parsing of the XFF HTTP header
configure module http x-forwarded-for parse enable	configure module http x-forwarded-for parse enable	Enable parsing of the XFF HTTP header to obtain the original IP address for policy matching

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module https hardware_engine cavium	configure module https hardware_engine cavium	Use "cavium" hardware accelerate card; this operation requires that the hardware card be inserted into the machine
configure module https hardware_engine none	configure module https hardware_engine none	Do not use SSL hardware accelerate card
configure module https logacccfullurl	configure module https logaccfullurl <enable/disable>	Configure logaccfullurl
configure module identification mac_address <enable/disable>	configure module identification mac_address <enable/disable>	Include/exclude MAC address for hostname identification method
configure module ldap groupcache interval	configure module ldap groupcache interval <interval>	Configure IWSVA LDAP user group membership cache interval *interval* UINT interval (in hours)
configure module ldap ipuser_cache disable	configure module ldap ipuser_cache disable	Disable IWSVA LDAP IP user cache
configure module ldap ipuser_cache enable	configure module ldap ipuser_cache enable	Enable IWSVA LDAP IP user cache
configure module ldap ipuser_cache interval	configure module ldap ipuser_cache interval <interval>	Configure IWSVA LDAP IP user cache interval *interval* FLOAT interval (in hours)

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module ldap www-auth port	configure module ldap www-auth port <port>	Configure the user/group authentication port in transparent mode (WCCP or bridge mode)
configure module log transaction disable	configure module log transaction disable	Disable the Transaction Log
configure module log transaction enable	configure module log transaction enable	Enable the Transaction Log
configure module log transaction filter disable	configure module log transaction filter disable	Disable the Transaction Log filter.
configure module log transaction filter enable	configure module log transaction filter enable <fromip> <toip>	Enable the Transaction Log filter. PARAM name: "fromip" IP address AAA.BBB.CCC.DDD where each part is in the range 0-255 PARAM name: "toip" IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
configure module log verbose filter disable	configure module log verbose filter disable	Disable verbose log filter
configure module log verbose filter enable	configure module log verbose filter enable <fromip> < toip>	Enable verbose log filter
configure module log verbose ftp disable	configure module log verbose ftp disable	Disable verbose FTP logs

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module log verbose ftp enable	configure module log verbose ftp enable	Enable verbose FTP logs
configure module log verbose http disable	configure module log verbose http disable	Disable verbose HTTP logs
configure module log verbose http enable	configure module log verbose http enable	Enable verbose HTTP logs
configure module log verbose wccp disable	configure module log verbose wccp disable	Disable verbose WCCP logs
configure module log verbose wccp enable	configure module log verbose wccp enable	Enable verbose WCCP logs
configure module ntp schedule <enable/disable>	configure module ntp schedule <enable/disable>	Enable or disable scheduled NTP time synchronization
configure module ntp schedule	configure module ntp schedule <interval> <primary_server> [secondary_server]	Configure scheduled NTP time synchronization *interval* (30m, 1h, 2h, 4h, 6h, 12h, 1d, 2d, 3d, 1w, 1M) *primary_server* ADDRESS Primary NTP server *secondary_server* ADDRESS Secondary NTP server

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module ntp sync	configure module ntp sync <server>	Configure IPv4 and IPv6 NTP server synchronization *server* ADDRESS NTP server
configure network bonding add	configure network bonding add <bondingname> [interface1] [interface2] [interface3] [interface4]	Add a link aggregation bonding interface <bondingname> is the name of the bonding interface
configure network bonding options miimon	configure network bonding options miimon <interval>	Configure miimon options of specified bonding device <interval> is the specific miimon interval to be set. Default is 100. **Note:** Miimon is a value setup in milli-seconds.
configure network bonding options xmit_hash_policy	configure network bonding options xmit_hash_policy <policy>	Configure xmit_hash_policy options of specified bonding device <policy> is the specific xmit_hash_policy to be set Default is 1 (3layer). 0 (2layer) is also available.

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network bonding remove	configure network bonding remove <bondingname>	Remove a link aggregation bonding interface <bondingname> is the name of the bonding interface
configure network bridge interface	configure network bridge interface [interface1] [interface2] [interface3] [interface4] [interface5] [interface6] [interface7] [interface8]	Configure the default bridge interface *internal* IFNAME Interface name or link aggregation bonding name *external* IFNAME Interface name or link aggregation bonding name
configure network bridge redirect ftpports	configure network bridge redirect ftpports <ports>	Configure the redirection ftp ports *ports* MULTIPORTS Redirect ports <port1;port2;...>
configure network bridge redirect httpports	configure network bridge redirect httpports <ports>	Configure the redirection HTTP ports *ports* MULTIPORTS Redirect ports <port1;port2;...>
configure network bridge redirect httpsports	configure network bridge redirect httpsports <ports>	Configure the redirection HTTPS ports *ports* MULTIPORTS Redirect ports <port1;port2;...>

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network bridge stp	configure network bridge stp	Configure the default bridge STP settings
configure network bridge stp disable	configure network bridge stp disable	Disable STP on IWSVA
configure network bridge stp enable	configure network bridge stp enable	Enable STP on IWSVA
configure network bridge stp priority	configure network bridge stp priority	Set the STP priority of IWSVA
configure network dns ipv4	configure network IPv4 dns <dns1> [dns2]	Configure DNS settings *dns1* IP_ADDR Primary IPv4 DNS server *dns2* IP_ADDR Secondary IPv4 DNS server
configure network dns ipv6	configure network IPv6 dns <dns1> [dns2]	Configure DNS settings *dns1* IP_ADDR Primary IPv6 DNS server *dns2* IP_ADDR Secondary IPv6 DNS server
configure network hostname	configure network hostname <hostname>	Configure the hostname hostname HOSTNAME Hostname or FQDN

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network interface ipv4 dhcp <network_interface_name> [vlan]	configure network interface ipv4 dhcp <network_interface_name> [vlan]	Configure the default Ethernet interface to use DHCP to obtain the IPv4 address. vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure network interface ipv6 dhcp <network_interface_name> [vlan]	configure network interface ipv6 dhcp <network_interface_name> [vlan]	Configure the default Ethernet interface to use DHCP to obtain the IPv6 address. vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure network interface duplex	configure network interface duplex <ethname> <duplex>	Configure the duplex of the Ethernet interface
configure network interface ping <interface_name> <action>	configure network interface ping <interface_name> <enable/disable>	Accept/disallow ICMP-request on the separated management interface
configure network interface ipv4 static	Configure the network interface to use ipv4 static. <interface_name> <IPv4 address> <network mask> [vlan]	Configure the default Ethernet interface to use the static IPv4 configuration.

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network interface ipv6 static	Configure the network interface to use ipv6 static. <interface_name> <IPv6 address> <network mask> [vlan]	Configure the default Ethernet interface to use the static IPv6 configuration.
configure network lanbypass auto	configure network lanbypass auto	The system auto-adjusts the LAN bypass status.
configure network lanbypass off	configure network lanbypass off	Never bypass traffic
configure network lanbypass on	configure network lanbypass on	Always bypasses traffic
configure network mgmt disable	configure network mgmt disable	Disable the separate IWSVA management interface
configure network mgmt interface	configure network mgmt interface <interface_name>	Configure IWSVA management interface name
configure network portgroup add	configure network portgroup add <pgname> [interface1] [interface2] [interface3] [interface4] [interface5] [interface6] [interface7] [interface8]	Add a port group
configure network portgroup linkloss <pgname>	configure network portgroup linkloss <pgname>	Configure the port group link loss forward settings

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network portgroup remove <pgname>	configure network portgroup remove <pgname>	Remove a port group
configure network portgroup vlan <pgname>	configure network portgroup vlan <pgname>	Configure the port group VLAN ID
configure network proxy interface	configure network proxy interface <proxy>	Configure the default proxy interface *proxy* IFNAME Interface name
configure network route ipv4/ipv6 add <ip_prefixlen> <via> <dev>	configure network route ipv4/ipv6 add <xxx.xxx.xxx.xxx/LL> <via> <device>	Add a route for a specified NIC device in VA
configure network route ipv4/ipv6 default <gateway>	configure network route ipv4/ipv6 default <gateway>	Reset the default gateway by executing configure network route default <*.*.*.*>
configure network route ipv4/ipv6 del <ip_prefixlen> <via> <dev>	configure network route ipv4/ipv6 del <xxx.xxx.xxx.xxx/LL> <via> <device>	Delete a route for a specified NIC device in VA
configure service pswd_protection disable	configure service pswd_protection disable	Disable SSH password protection service
configure service pswd_protection enable	configure service pswd_protection enable	Enable SSH password protection service

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure service recycle time	configure service recycle time <hh:mm>	Enable recycling by time PARAM name "time" Use hh:mm time format between 00:00 and 23:59
configure service recycle disable time	configure service recycle disable time	Disable recycling by time
configure service recycle transaction	configure service recycle transaction <TRANSACTION_NUMBER>	Enable recycling by transaction PARAM name "transaction" Daemon will recycle after 100000-99999999 transaction(s)
configure service recycle disable transaction	configure service recycle disable transaction	Disable the transaction recycling
configure service ssh disable	configure service ssh disable	Disable the SSH daemon
configure service ssh enable	configure service ssh enable	Enable the SSH daemon
configure service ssh port	configure service ssh port <port>	Configure SSH port number *port* PORT SSH port number [1 ~ 65535]

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module socks_sftp_proxy enable	configure module socks_sftp_proxy enable	Enable SFTP with socks
configure module socks_sftp_proxy disable	configure module socks_sftp_proxy disable	Disable SFTP with socks
configure module socks_sftp_proxy port	configure module socks_sftp_proxy port <port>	Change the default port number Range: 1-65535
configure system date	configure system date <date> <time>	Configure date and save to CMOS *date* DATE_FIELD [DATE_FIELD] *time* TIME_FIELD [TIME_FIELD]
configure system ha	configure system ha	Configure high availability
configure system ha remove	configure system ha remove	Remove HA configuration and reboot IWSVA

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system ha synchronization interval	configure system ha synchronization interval	Configure the HA synchronization interval PARAM name: "Interval" Interval (in minutes) at which HA will synchronize settings to child server. Range in minutes: 5-60
configure system harddisk	configure system harddisk	Add new hard disk and extend IWSVA data partition space **Note:** IWSVA only supports adding one new hard disk and extends the IWSVA data partition space each time.
configure system hwmonitor	configure system hwmonitor	Configure system hardware monitoring information.
configure system hwmonitor interval	configure system hwmonitor interval [1-60]	Configure hardware status polling in minutes. Range is 1-60 minutes. Default duration determined by the IPMI polling cycle.
configure system keyboard	configure system keyboard	Configure system keyboard layout type

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system keyboard us	configure system keyboard us	Configure system keyboard layout type to U.S. English
configure system password	configure system password <user>	Configure account password *user* USER The user name for which you want to change the password. The user could be 'enable', 'root' or any user in the IWSVA's Administrator group
configure system timezone Africa Cairo	configure system timezone Africa Cairo	Configure timezone to Africa/Cairo location
configure system timezone Africa Harare	configure system timezone Africa Harare	Configure timezone to Africa/Harare location
configure system timezone Africa Nairobi	configure system timezone Africa Nairobi	Configure timezone to Africa/Nairobi location
configure system timezone America Anchorage	configure system timezone America Anchorage	Configure timezone to America/Anchorage location
configure system timezone America Bogota	configure system timezone America Bogota	Configure timezone to America/Bogota location
configure system timezone America Buenos_Aires	configure system timezone America Buenos_Aires	Configure timezone to America/Buenos_Aires location

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone America Chicago	configure system timezone America Chicago	Configure timezone to America/Chicago location
configure system timezone America Chihuahua	configure system timezone America Chihuahua	Configure timezone to America/Chihuahua location
configure system timezone America Denver	configure system timezone America Denver	Configure timezone to America/Denver location
configure system timezone America Godthab	configure system timezone America Godthab	Configure timezone to America/Godthab location
configure system timezone America Lima	configure system timezone America Lima	Configure timezone to America/Lima location
configure system timezone America Los_Angeles	configure system timezone America Los_Angeles	Configure timezone to America/Los_Angeles location
configure system timezone America Mexico_City	configure system timezone America Mexico_City	Configure timezone to America/Mexico_City location
configure system timezone America New_York	configure system timezone America New_York	Configure timezone to America/New_York location
configure system timezone America Noronha	configure system timezone America Noronha	Configure timezone to America/Noronha
configure system timezone America Phoenix	configure system timezone America Phoenix	Configure timezone to America/Phoenix

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone America Santiago	configure system timezone America Santiago	Configure timezone to America/Santiago
configure system timezone America St_Johns	configure system timezone America St_Johns	Configure timezone to America/St_Johns
configure system timezone America Tegucigalpa	configure system timezone America Tegucigalpa	Configure timezone to America/Tegucigalpa
configure system timezone Asia Almaty	configure system system timezone Asia Almaty	Configure timezone to Asia/Almaty location
configure system timezone Asia Baghdad	configure system timezone Asia Baghdad	Configure timezone to Asia/Baghdad location
configure system timezone Asia Baku	configure system timezone Asia Baku	Configure timezone to Asia/Baku location
configure system timezone Asia Bangkok	configure system timezone Asia Bangkok	Configure timezone to Asia/Bangkok location
configure system timezone Asia Calcutta	configure system timezone Asia Calcutta	Configure timezone to Asia/Calcutta location
configure system timezone Asia Colombo	configure system timezone Asia Colombo	Configure timezone to Asia/Colombo location
configure system timezone Asia Dhaka	configure system timezone Asia Dhaka	Configure timezone to Asia/Dhaka location
configure system timezone Asia Hong_Kong	configure system timezone Asia Hong_Kong	Configure timezone to Asia/Hong_Kong location

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Asia Irkutsk	configure system timezone Asia Irkutsk	Configure timezone to Asia/Irkutsk location
configure system timezone Asia Jerusalem	configure system timezone Asia Jerusalem	Configure timezone to Asia/Jerusalem location
configure system timezone Asia Kabul	configure system timezone Asia Kabul	Configure timezone to Asia/Kabul location
configure system timezone Asia Karachi	configure system timezone Asia Karachi	Configure timezone to Asia/Karachi location
configure system timezone Asia Katmandu	configure system timezone Asia Katmandu	Configure timezone to Asia/Katmandu location
configure system timezone Asia Krasnoyarsk	configure system timezone Asia Krasnoyarsk	Configure timezone to Asia/Krasnoyarsk location
configure system timezone Asia Kuala_Lumpur	configure system timezone Asia Kuala_Lumpur	Configure timezone to Asia/Kuala_Lumpur location
configure system timezone Asia Kuwait	configure system timezone Asia Kuwait	Configure timezone to Asia/Kuwait location
configure system timezone Asia Magadan	configure system timezone Asia Magadan	Configure timezone to Asia/Magadan location
configure system timezone Asia Manila	configure system timezone Asia Manila	Configure timezone to Asia/Manila location
configure system timezone Asia Muscat	configure system timezone Asia Muscat	Configure timezone to Asia/Muscat location

TABLE 13-1. **Command Line Interface Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Asia Rangoon	configure system timezone Asia Rangoon	Configure timezone to Asia/Rangoon location
configure system timezone Asia Seoul	configure system timezone Asia Seoul	Configure timezone to Asia/Seoul location
configure system timezone Asia Shanghai	configure system timezone Asia Shanghai	Configure timezone to Asia/Shanghai location
configure system timezone Asia Singapore	configure system timezone Asia Singapore	Configure timezone to Asia/Singapore location
configure system timezone Asia Taipei	configure system timezone Asia Taipei	Configure timezone to Asia/Taipei location
configure system timezone Asia Tehran	configure system timezone Asia Tehran	Configure timezone to Asia/Tehran location
configure system timezone Asia Tokyo	configure system timezone Asia Tokyo	Configure timezone to Asia/Tokyo location
configure system timezone Asia Yakutsk	configure system timezone Asia Yakutsk	Configure timezone to Asia/Yakutsk location
configure system timezone Atlantic Azores	configure system timezone Atlantic Azores	Configure timezone to Atlantic/Azores location
configure system timezone Australia Adelaide	configure system timezone Australia Adelaide	Configure timezone to Australia/Adelaide location
configure system timezone Australia Brisbane	configure system timezone Australia Brisbane	Configure timezone to Australia/Brisbane location

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Australia Darwin	configure system timezone Australia Darwin	Configure timezone to Australia/Darwin location
configure system timezone Australia Hobart	configure system timezone Australia Hobart	Configure timezone to Australia/Hobart location
configure system timezone Australia Melbourne	configure system timezone Australia Melbourne	Configure timezone to Australia/Melbourne location
configure system timezone Australia Perth	configure system timezone Australia Perth	Configure timezone to Australia/Perth location
configure system timezone Europe Amsterdam	configure system timezone Europe Amsterdam	Configure timezone to Europe/Amsterdam location
configure system timezone Europe Athens	configure system timezone Europe Athens	Configure timezone to Europe/Athens location
configure system timezone Europe Belgrade	configure system timezone Europe Belgrade	Configure timezone to Europe/Belgrade location
configure system timezone Europe Berlin	configure system timezone Europe Berlin	Configure timezone to Europe/Berlin location
configure system timezone Europe Brussels	configure system timezone Europe Brussels	Configure timezone to Europe/Brussels location
configure system timezone Europe Bucharest	configure system timezone Europe Bucharest	Configure timezone to Europe/Bucharest location

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Europe Dublin	configure system timezone Europe Dublin	Configure timezone to Europe/Dublin location
configure system timezone Europe Moscow	configure system timezone Europe Moscow	Configure timezone to Europe/Moscow location
configure system timezone Europe Paris	configure system timezone Europe Paris	Configure timezone to Europe/Paris location
configure system timezone Pacific Auckland	configure system timezone Pacific Auckland	Configure timezone to Pacific/Auckland location
configure system timezone Pacific Fiji	configure system timezone Pacific Fiji	Configure timezone to Pacific/Fiji location
configure system timezone Pacific Guam	configure system timezone Pacific Guam	Configure timezone to Pacific/Guam location
configure system timezone Pacific Honolulu	configure system timezone Pacific Honolulu	Configure timezone to Pacific/Honolulu location
configure system timezone Pacific Kwajalein	configure system timezone Pacific Kwajalein	Configure timezone to Pacific/Kwajalein location
configure system timezone Pacific Midway	configure system timezone Pacific Midway	Configure timezone to Pacific/Midway location
configure system timezone US Alaska	configure system timezone US Alaska	Configure timezone to US/Alaska location
configure system timezone US Arizona	configure system timezone US Arizona	Configure timezone to US/Arizona location

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone US Central	configure system timezone US Central	Configure timezone to US/Central location
configure system timezone US East-Indiana	configure system timezone US East-Indiana	Configure timezone to US/East-Indiana location
configure system timezone US Eastern	configure system timezone US Eastern	Configure timezone to US/Eastern location
configure system timezone US Hawaii	configure system timezone US Hawaii	Configure timezone to US/Hawaii location
configure system timezone US Mountain	configure system timezone US Mountain	Configure timezone to US/Mountain location
configure system timezone US Pacific	configure system timezone US Pacific	Configure timezone to US/Pacific location
enable	enable	Enable administrative commands
exit	exit	Exit the session
ftpput	ftpput <url> <filename> [--active]	Upload file through FTP protocol *url* STRING [ftp://username:password@hostname/path] *filename* FILENAME The file name and path to upload *active* ACTIVETYPE FTP active mode
help	help	Display an overview of the CLI syntax

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
history	history [limit]	Display the current session's command line history
ping	ping [-c num_echos] [-i interval] <dest>	*-c num_echos* UINT Specify the number of echo requests to be sent [5] *-i interval* UINT Wait interval seconds between sending each packet *dest* ADDRESS Host name or IP address
ping6	ping6 <IPv6 address>	Use this command to ping IPv6 hosts.
reboot	reboot [time]	Reboot this machine after a specified delay or immediately *time* UINT Time in minutes to reboot this machine [0]
resolve	resolve <dest>	Resolve an IP address on the network *dest* ADDRESS Remote ip address to resolve
resolve6	resolve6 <IPv6 dest>	Resolve an IPv6 IP address on the network *dest* ADDRESS Remote ipv6 address to resolve

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
restart service database	restart service database	Restart the database daemon
restart service ftpd	restart service ftpd	Restart the FTP traffic scanning daemon
restart service httpd	restart service httpd	Restart the HTTP traffic scanning daemon
restart service iwss_daemons	restart service iwss_daemons	Restart all IWSVA services
restart service logtodb	restart service logtodb	Restart the daemon that saves logs to database
restart service maild	restart service maild	Restart the email notification daemon
restart service metric_mgmt	restart service metric_mgmt	Restart the metric management daemon
restart service ssh	restart service ssh	Restart the SSH daemon
restart service svcmonitor	restart service svcmonitor	Restart the monitor daemon
restart service tmcmagent	restart service tmcmagent	Restart the TMCM agent
restart service tmsyslog	restart service tmsyslog	Restart the syslog daemon
restart service wccpd	restart service wccpd	Restart the WCCP daemon
restart service webui	restart service webui	Restart the tomcat daemon

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show kernel iostat	show kernel iostat	Display Central Processing Unit (CPU) statistics and input/output statistics for devices, partitions and network file systems (NFS)
show kernel messages	show kernel messages	Display kernel messages
show kernel modules	show kernel modules	Display modules loaded in the kernel
show kernel parameters	show kernel parameters	Display running kernel parameters
show memory statistics	show memory statistics	Display memory statistics
show module config all	show module config all	View the all the config files
show module config database	show module config database	View the database config files
show module config file intscan	show module config file intscan	View the intscan config file
show module config file IWSSPIJavascan	show module config file IWSSPIJavascan	View the IWSSPIJavascan config file
show module config file IWSSPIProtocolFtp	show module config file IWSSPIProtocolFtp	View the IWSSPIProtocolFtp config file.

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module config file IWSSPIProtocolHttpProxy	show module config file IWSSPIProtocolHttpProxy	View the IWSSPIProtocolHttpProxy config file
show module config file IWSSPIProtocolIcap	show module config file IWSSPIProtocolIcap	View the IWSSPIProtocolIcap config file
show module config file IWSSPIScanVsapi	show module config file IWSSPIScanVsapi	View the IWSSPIScanVsapi config file
show module config file IWSSPISigScan	show module config file IWSSPISigScan	View the IWSSPISigScan config file
show module config file IWSSPIUrlFilter	show module config file IWSSPIUrlFilter	View the IWSSPIUrlFilter config file
show module database backup	show module database backup	Display database backups
show module database password	show module database password	Display the database password
show module database settings	show module database settings	Display the configuration of the database
show module database size	show module database size	Display the size of IWSVA database
show module http x-forwarded-for	show module http x-forwarded-for	Display the configuration of the XFF HTTP header module

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module ldap groupcache interval	show module ldap groupcache interval	Display IWSVA LDAP user group membership cache interval
show module ldap ipuser_cache	show module ldap ipuser_cache	Display the configuration of IWSVA LDAP IP user cache. Client IP cache associates a client IP address with a user who recently authenticated from that same IP address. Any request originating from the same IP address as a previously authenticated request will be attributed to that user, provided the new request is issued within a configurable window of time from that authentication. The caveat is that client IP addresses seen by IWSVA must be unique to a user within that time period; thus this cache is not useful in environments where there is a proxy server or source NAT between the clients and IWSVA, or where DHCP frequently reassigns client IPs.

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module ldap ipuser_cache interval	show module ldap ipuser_cache interval	Display IWSVA LDAP IP user cache interval
show module ldap www-auth port	show module ldap www-auth port	Display the authentication port
show module log admin	show module log admin [log_suffix]	View the admin log file The log_suffix format is date.revision. Example: 20120518.0001 To view the admin log, use: show module log admin 20120518.0001
show module log ftp	show module log ftp [log_suffix]	View the ftp log file The log_suffix format is date.revision Example:20120518.0001 To view the ftp log, use: show module log ftp 20120518.0001

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module log http	show module log http [log_suffix]	View the http log file The log_suffix format is date.revision Example:20120518.0001 To view the ftp log, use: show module log ftp 20120518.0001
show module log mail	show module log mail [log_suffix]	View the mail log file The log_suffix format is data.revision Example:20120518.0001 To view the mail log, use: show module log mail 20120518.0001
show module log postgres	show module log postgres	View the postgres log
show module log tmudump	show module log tmudump	View the tmudump log file
show module log update	show module log update [log_suffix]	View the update log file *log_suffix* LOGSUFFIX [log_suffix] []
show module metrics ftp	show module metrics ftp	Display IWSVA ftp performance metrics
show module metrics http	show module metrics http	Display IWSVA http performance metrics

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module ntp schedule	show module ntp schedule	Display the scheduled NTP server configuration
show module webui port	show module webui port	Display Web server port settings
show network neighbour	show network neighbour [dest]	Display system arp tables *dest* ADDRESS Remote IP address to arp
show network bonding <bonding name>	show network bonding <bonding name>	Display bonding settings If <bonding name> is missing, all bonding settings display. If <bonding name> is specified, specified bonding settings display.
show network bridge redirect ftpports	show network bridge redirect ftpports	Display the FTP redirection port numbers
show network bridge redirect httpports	show network bridge redirect httpports	Display the HTTP redirection port numbers
show network bridge redirect httpsports	show network bridge redirect httpsports	Display the HTTPS redirection port numbers
show network bridge stp	show network bridge stp	Display the bridge STP settings
show network capture	show network capture [filename]	Display packets captures *filename* STRING [filename] []

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show network connections <all/listening> <all/tcp/udp>	show network connections <all/listening> <all/tcp/udp>	Display system connections or daemons. For example, execute “show network connections listing” to display which daemons are running.
show network conntrack	show network conntrack	Display state tracked connections
show network conntrack expect	show network conntrack expect	Display state expected connections
show network data interface	show network data interface Interface: eth0 IPv4 address/mask: 10.168.10.78/255.255.255.0 IPv6 address/prefix: 2001:20::1/64 Type: static	Display network address
show network dns	show network dns	Display network dns servers
show network ethernet	show network ethernet <ethname>	Display Ethernet card settings *ethname* IFNAME Interface name

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show network firewall filter	show firewall filter The IPv6 firewall rules are appended to the IPv4 firewall rules.	Display firewall filter
show network firewall nat	show firewall nat	Display firewall NAT
show network gateway ipv4/ipv6	show network gateway IPv4 gateway: 10.168.10.254 IPv6 gateway: 2001:10::1	Display ipv4/ipv6 network gateways
show network hostname	show network hostname	Display network hostname
show network interfaces	show network interfaces	Display network interface information
show network interfaces status	show network interfaces status	Display the link status of the network card
show network interfaces status once	show network interfaces status once	Display the link status of the network card once
show network interfaces statistic	show network interfaces statistic	Display the link status of the network card
show network lanbypass	show network lanbypass	Displays the current configuration status of LAN-bypass function If LAN-bypass used, it would show one of the following states: on / off / auto.

TABLE 13-1. Command Line Interface Commands (Continued)

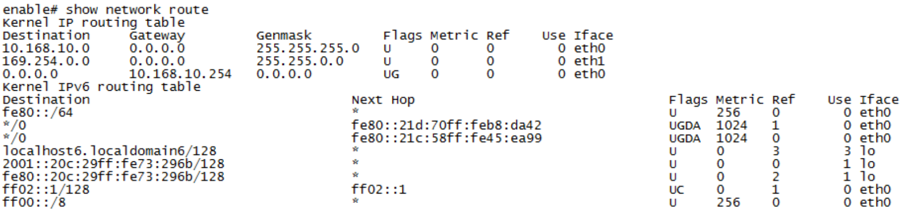
<table>
<tr><th>COMMAND</th><th>SYNTAX</th><th>DESCRIPTION</th></tr>
<tr><td>show network mgmt interface</td><td>show network mgmt interface
Management interface: enable
Interface: eth1
IPv4 address/mask: 10.168.20.78/255.255.255.0
IPv6 address/prefix: 2001:10::1/64
Type: static</td><td>Display the status and address information</td></tr>
<tr><td>show network ping</td><td>show network ping</td><td>Display data and management status</td></tr>
<tr><td>show network portgroup</td><td>show network portgroup</td><td>Display current port group settings</td></tr>
<tr><td>show network route ipv4/ipv6</td><td>show network route ipv4/ipv6
(routes displayed as follows):</td><td>Display an IPv4/IPv6 network routing table</td></tr>
<tr><td colspan="3"><pre>
enable# show network route
Kernel IP routing table
Destination   Gateway   Genmask   Flags Metric Ref   Use Iface
10.168.10.0   0.0.0.0   255.255.255.0   U   0   0   0 eth0
169.254.0.0   0.0.0.0   255.255.0.0   U   0   0   0 eth1
0.0.0.0   10.168.10.254   0.0.0.0   UG   0   0   0 eth0
Kernel IPv6 routing table
Destination   Next Hop   Flags Metric Ref   Use Iface
fe80::/64   *   U   256   0   0 eth0
*/0   fe80::21d:70ff:feb8:da42   UGDA 1024   1   0 eth0
*/0   fe80::21c:58ff:fe45:ea99   UGDA 1024   0   0 eth0
localhost6.localdomain6/128   *   U   0   3   3 lo
2001::20c:29ff:fe73:296b/128   *   U   0   0   1 lo
fe80::20c:29ff:fe73:296b/128   *   U   0   2   1 lo
ff02::1/128   ff02::1   UC   0   1   0 eth0
ff00::/8   *   U   256   0   0 eth0
</pre></td></tr>
<tr><td>show network sockets</td><td>show network sockets</td><td>Display open network socket statistics</td></tr>
</table>

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show process library	show process library <pid>	A library call tracer *pid* UINT <pid>
show process stack	show process stack <pid>	Print a stack trace of a running process *pid* UINT <pid>
show process [target]	show process [target]	Display process information *target* STRING [optional name/ID with wildcard support] []
show process top	show process top	Display information about running processes
show process trace	show process trace <pid>	Trace system calls and signals *pid* UINT <pid>
show service ssh	show service ssh	Show status of SSH service
show storage partition	show storage partition [partition]	Report file system usage in readable format only *partition* STRING [optional partition] []
show storage space	show disk space [target]	Report file space usage in readable format only *target* STRING [optional directory or filename] [/]
show storage statistic	show storage statistic	Display disk statistics

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show system configuration	show system configuration	Display IPv4 and IPv6 summary information for the running configuration
show system configuration [-verbose]	show system configuration [-verbose]	Display detailed information of running configuration
show system date Replaces: show date	show system date	Display current date/time
show system ha	show system ha	Display HA information, such as: Cluster name, Description, HA mode, Deployment mode, Cluster IP address(es) (IPv4 and/or IPv6) - should be configured as 172.16.2.200/2001:10::1 for example, Preemption, Member list, Role, Localhost, Hostname, IP address, Weight
show system hwmonitor	show system hwmonitor	Display hardware monitoring information.
show system hwmonitor interval	show system hwmonitor interval	Show current polling interval value.
show system hwmonitor sel	show system hwmonitor sel	Shows the hardware event log information as a base for sending SNMP traps.

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show system hwmonitor sensor	show system hwmonitor sensor	Shows all the information gathered from sensors.
show system keyboard	show system keyboard	Display default keyboard table
show system openfiles	show system openfiles [target]	Display open files *target* STRING [optional directory or filename] []
show system timezone	show timezone	Display the timezone on IWSVA
show system uptime	show system uptime	Show how long the system has been running
show system version	show system version	Display IWSVA version
shutdown	shutdown [time]	Shutdown this machine after a specified delay or immediately *time* UINT Time in minutes to shutdown this machine [0]
start service database	start service database	Start the database daemon
start service ftpd	start service ftpd	Start the FTP traffic scanning daemon
start service httpd	start service httpd	Start the HTTP traffic scanning daemon
start service logtodb	start service logtodb	Start the daemon that saves logs to database

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
start service maild	start service maild start	Start the email notification daemon
start service metric_mgmt	start service metric_mgmt	Start the metric management daemon
start service ssh	start service ssh	Enable the sshd daemon
start service svcmonitor	start service svcmonitor	Start the monitor daemon
start service tmcmagent	start service tmcmagent	Start the TMCM agent
start service tmsyslog	start service tmsyslog	Start the syglog daemon
start service wccpd	start service wccpd	Start the WCCP daemon
start service webui	start service webui	Start the tomcat daemon
start shell	start shell	Administrative shell access
start task database backup	start task database backup	Back up your database
start task database reindex	start task database reindex	Reindex the IWSVA database
start task database restore	start task database restore [filename]	Restore your database from a backup
start task database truncate	start task database truncate <DATE_FIELD>	Truncate the IWSVA database
start task database vacuum	start task database vacuum	Vacuum the IWSVA database

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
Note: If the administrator finds that database may not be fully vaccuumed, tune the "max_fsm_pages" parameter in the `postgresql.conf` configuration file found at `/var/iwss/postgres/pgdata/`.		
start task capture interface	start task capture interface <interface> [-h host] [-p port]	Capture network interface traffic *interface* IFNAME interface to capture packets *-h* host IP_ADDR filter by IP address *-p* port UINT filter by port number
start task monitor ftp	start task monitor ftp	Monitor the FTP log
start task monitor http	start task monitor http	Monitor the HTTP log
stop process	stop process <pid>	Stop a running process *pid* UINT <pid>
stop process core	stop process core <pid>	Stop a running process and generate a core file *pid* UINT <pid>
stop service database	stop service database	Stop the database daemon
stop service ftpd	stop service ftpd	Stop the FTP traffic daemon
stop service httpd	stop service httpd	Stop the HTTP traffic daemon

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
stop service logtodb	stop service logtodb	Stop the daemon that saves logs to database
stop service maild	stop service maild	Stop the email notification daemon
stop service metric_mgmt	stop service metric_mgmt	Stop the metric management daemon
stop service ssh	stop service ssh	Disable the sshd daemon
stop service svcmonitor	stop service svcmonitor	Stop the monitor daemon
stop service tmcmagent	service stop tmcmagent	Stop the TMCM agent
stop service tmsyslog	stop service tmsyslog	Stop the syslog daemon
stop service wccpd	stop service wccpd	Stop the WCCP daemon
stop service webui	stop service webui	Stop the tomcat daemon
traceroute	traceroute [-h hops] <dest> [-n]	TraceRoute *-h hops* UINT Specify maximum number of hops *dest* ADDRESS Remote system to trace *-n* DASHN Do not resolve hostname []

TABLE 13-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
traceroute6	traceroute6 <IPv6 address>	TraceRoute6 *-h hops* UINT Specify maximum number of hops *dest* ADDRESS Remote IPv6 host to trace *-n* DASHN Do not resolve hostname []
wget	wget <url> <path>	Download file through HTTP/FTP protocols *url* STRING [http://username:password@hostname/path] *path* FILENAME The local path to download file

Chapter 14

Reports, Logs, and Notifications

This chapter describes how administrators can get timely information about their gateway security through InterScan Web Security Virtual Appliance (IWSVA) reports, logs, and notifications.

Topics in this chapter include the following:

Introduction to Reports

IWSVA and malicious code detections, files blocked, and URLs accessed. You can use this information about IWSVA program events to help optimize program settings and fine tune your organization's security policies.

You can configure and customize reports. For example, IWSVA allows you to generate reports for all or specific user(s), user group(s), or device group(s), either on demand (in real time) or on a scheduled basis.

To allow you to share the selected report information with those who need it, IWSVA can send the generated report through email as file attachments.

IWSVA user accounts can generate reports based on the role associated with their accounts. That is, if a role allows access to the data related to an IP address range, the user account can generate reports related to those IPs addresses only.

Report Information

Enter the desired report name and a short description of the report. Enable the report by selecting either Yes or No.

Report Settings

When generating a report template you need to specify the following information:

- Generate the report based on a specific schedule.
- Generate the report based on a specific time period.
- Indicate the time for which to generating report (working time, leisure time, or any customized time filter).
- Indicate the device group for which to generate report.
- Indicate the type of output (PDF, HTML, or CSV file).
- Indicate the number of reports to save and keep.

Note: For Report Settings, time is measured as follows:
Last 1 Day: From the start of the day 00:00 to day -1

Email This Report

For all reports,

Select Email This Report and complete the settings:

- Enter the "From" email address.
- Enter the "Recipients" email address to send a copy of the report to a specific person or to an email distribution list after the report has been generated.
- Enter the intended message.
- "Enable" the report to be sent as an attachment.
- Indicate your selection of notification in the event of a message delivery failure.

Report By (Users and Groups)

Select the user(s) and or group(s) for which you want to generate a report. Options include:

- **All users**: All clients accessing the Internet through IWSVA
- **Specific user(s)**: Clients with specific IP addresses, host names, or LDAP directory entries
- **All groups**: All groups in the LDAP directory; if using the IP address or host name identification method, then "All groups" is equivalent to "All users"
- **Specific group(s)**: Either specified LDAP groups or a range of IP addresses

When generating reports for specific users or groups, the user selection method is determined by the method configured under **Administration > IWSVA Configuration > User Identification | User Identification** tab. For more information about user identification, see Configuring the User Identification Method starting on page 8-6.

Types of Reports

IWSVA can generate bar or table chart graphs that represent the following categories of reports:

- Internet Security — See reports that itemize the following top n Internet security detections:
  - malware/spyware detection

  - botnet detection
  - document exploit APT detection
  - custom defense APT blocking
  - C&C contact alert count by date
  - C&C address
  - user/hosts detected by C&C contact alert
  - group detected by C&C contact alert
  - malicious sites blocked
  - users blocked by malware/spyware
  - users blocked by malicious sites
  - groups blocked by malware/spyware
  - groups blocked by malicious sites
  - users by botnet detection
  - most violation for HTTP malware scan policy
  - malicious sites blocked by date
  - malware/spyware detection by date
  - malware/spyware detection trend
- Internet Access — See reports itemizing the following top n Internet Access detections:
  - applications visited
  - URL categories visited
  - sites visited
  - users by requests
  - groups by requests
  - URL categories sorted by browse times
  - sites visited by browse times
  - users by browse time
  - activity level by hours
- Bandwidth — See reports itemizing the following top n bandwidth detections:
  - URL categories by bandwidth

- applications by bandwidth
- users by bandwidth
- groups by bandwidth
- sites by bandwidth
- total traffic by days

- Policy Enforcement — See reports itemizing the following top n policy enforcement detections:
  - URL categories blocked
  - applications blocked
  - users enforced
  - groups enforced
  - sites blocked
  - users by HTTP inspection
  - most violation for URL filtering policy
  - most violation for application control policy
  - most violation for access quota control policy
  - most violation for applets and ActiveX policy
  - most violation for HTTP inspection policy
- Data Security — See reports itemizing the following top n data security detections:
  - DLP templates blocked by requests
  - blocked users
  - blocked groups
  - most violation for data loss prevention policy
- Custom Report — Include defined Log Favorites to be reported. See *Report Types* on page 14-8 for more information.

Generating Reports

As with the behavior of IPv4, reports can be generated by a specific IPv6 user or an IPv6 group of users. The selected user or group of users page also supports IPv6 addresses or ranges.

Reports can be generated in CSV, PDF, or HTML formats for both IPv4 and IPv6 users without encountering layout issues. As with the behavior of IPv4, when generating user-related reports, all IPv6 users can be accounted for in the report without encountering layout issues.

Configuring Reports

IWSVA enables you to generate reports for either all or a subset of the clients accessing the Internet. You can save the generated report in PDF, HTML, or CVS format.

To configure reports:

1. Click **Reports** in the main menu.
2. Click **Add** to add a new report template.
3. Enter a name and description for the report template. When you are ready for the template to take effect, click **Yes** to enable it.
4. Under **Report Settings**, select a schedule for the report (either **Once Now**, **Once in Future**, **Every Day**, **Every Week,** or **Every Month**), and then select the **Report Period**. Click **Custom Time Range** to generate a report in a given time range, and then select the **From** and **To** dates.
5. Select a schedule time filter (**Always**, **working time**, **leisure time** or a time filter customized in **Administration > IWSVA Configuration > Scheduled Times**).
6. Select the device group.

   Note: To add a device group, choose **Administration > IWSVA Configuration > Central Log/Reporting** and click **Add** under **Device Group Management**. By default, all devices are added to the same group.

7. Select the report output.
8. Configure the email recipients, subject, and message along with the optional settings.
9. Under **Report By**, select the users for which the report is generated—either **All Users**, **Specific Users/Groups** - IPv6 addresses can also be defined when choosing Specific user(s), **All groups**, or **Specific group(s)**. For more information about running reports for specific users or groups, see *To select specific users or group(s):*.

10. Under **Report Types**, select the report type(s) and enter the desired report record number(s).

> **Note:** IWSVA groups multiple report parameters into a single report, with each report parameter having its own section.

11. Select the chart type (Bar. Table or both) from the menu.
12. Click **Save Report**.

The following table provides information about the parameters that can comprise a report:

TABLE 14-1. Report Parameter Availability Depends on the Report Type

REPORT BY	REPORT PARAMETERS INCLUDED
All users	Includes all listed report parameters except for "Individual user reports"
Specific Users/Groups	Includes only the "Individual user reports" parameters
* For Web Reputation (including anti-pharming and anti-phishing), blocked sites appear in these reports. But to find a blocked site, the information is only in "Top N Malicious Sites Blocked."	

To select specific users or group(s):

1. Click **Reports** in the main menu.
2. Under **Report by**, select **Specific Users / Groups**, and then click **Select**.

   The **Select Users / Groups** pop-up screen opens according to the configured user identification method (**Administration > IWSVA Configuration > User Identification | User Identification**).
3. Type the IP host name or address range (or search for a group name in your LDAP directory if using the "User/group name authentication" identification method).
4. Type specific users or groups and click **Search**.
5. Click **Add**.

6. After adding all the groups, click **Save**.

Report Types

For each report parameter, you can specify how many records you want to include in reports. For each report type, the default includes records like: the top number of users, URLs, categories, and so on, for each report type. Specifying a very large number, such as 99, will affect report size and generation time.

The Top Categories (weighted) reporting parameter provides information about URL categories, even ones that are blocked or monitored. Also, this parameter provides the number of requests of every URL category and URL visited. This information can help you determine which URL category needs to be blocked or monitored for different Internet groups.

For the reporting parameters, the following conditions apply:

- The user can be an address, username, or a host name.
- For HTTP, URL addresses include the whole address, not just the top-level domain. For HTTPS, URL addresses include only the top-level domain.
- Content is listed by most frequently visited URLs specified by the user, and sorted by number of visits.

Management can review this activity and then determine if requests are permissible.

For custom reports, you can include saved or "favorited" logs to a customized report. Custom report uses the time range and users specified in the report template. Other settings are the same as those configured in the favorited logs.

Scheduling Reports

You can configure IWSVA to generate scheduled reports on a once now, once in the future, daily, weekly, or monthly basis.

To configure scheduled reports:

1. Create a new report in **Reports** from the main menu.
2. Click **Add** or a report name to edit it.
3. Enter a report name for the new report. Under **Report Settings** set the time and/or date to generate the scheduled report.

4. Select **Email** and the attachment format, and type the email address(es) to which IWSVA should send the generated report as a file attachment. You must also enter the **From** and **Subject** fields. Separate multiple email addresses with commas.

Note: The SMTP server related settings are in **Notifications > Send notifications to....**

5. Click **Save**.

To delete a scheduled report:

1. Click **Reports** on the main menu.
2. Select the report template to remove and then click **Delete**.

Saved Scheduled Reports

When a scheduled report is generated, IWSVA sends the report to specified recipients and saves a copy to the database. You can view or download the saved report under **Reports** and click the **Saved Reports** tab. You can configure the number of saved reports IWSVA is to store in the database.

Introduction to Logs

The IWSVA database stores all log data, but log data can also be stored in text log files for backward compatibility with previous IWSVA versions or used with an external reporting tool. Storing the log data in text log files provides redundancy to verify that the database is properly updated. Trend Micro recommends using the database as the only storage location for log data.

Note: For Log Analysis, time is measured as follows:
Last 1 Hour: From current time to start of this hour.
Last 1 Day: From current time to start of this hour - 23 hours

Log are categorized by log type, and are mapped or grouped as follows:

- *Bandwidth*
- *Policy Enforcement*
- *Internet Access*
- *Internet Security*

- *Data Security*
- *Access Control*

Bandwidth

Each log display can utilize any one of the following filters:

- Incoming traffic
- Outgoing traffic
- All traffic
- User Name
- Device Group
- Client IP
- App ID
- Policy Name

Continue sorting with time range filters: Today, last 1 hour, last 12 hours, last 1 day. last seven days, or a customized time range. Set the top number of instances you would like to show from Top 5 to Top 20. Choose the output in which you would like to display your results; bar, line, pie chart and so on.

Policy Enforcement

Each log display can utilize any one of the following filters:

- Action
- Message Type
- Device Group
- Client IP
- Channel
- App ID
- Policy Name
- User Name
- Rule Name
- URL Category

Continue sorting with time range filters: Today, last 1 hour, last 12 hours, last 1 day. last seven days, or a customized time range. Set the top number of instances you would like to show from Top 5 to Top 20. Choose the output in which you would like to display your results; bar, line, pie chart and so on.

Internet Access

Each log display can utilize any one of the following filters:

- Domain
- Device Group
- Client IP
- User Name
- URL Category

Continue sorting with time range filters: Today, last 1 hour, last 12 hours, last 1 day. last seven days, or a customized time range. Set the top number of instances you would like to show from Top 5 to Top 20. Choose the output in which you would like to display your results; bar, line, pie chart and so on.

Internet Security

Each log display can utilize any one of the following filters:

- Action
- Message Type
- Malware Name
- Device Group
- Client IP
- Channel
- Policy Name
- User Name

Continue sorting with time range filters: Today, last 1 hour, last 12 hours, last 1 day. last seven days, or a customized time range. Set the top number of instances you would like to show from Top 5 to Top 20. Choose the output in which you would like to display your results; bar, line, pie chart and so on.

Data Security

Each log display can utilize any one of the following filters:

- Action
- Device Group
- Client IP
- Channel
- Policy Name
- User Name
- Rule Name

Continue sorting with time range filters: Today, last 1 hour, last 12 hours, last 1 day. last seven days, or a customized time range. Set the top number of instances you would like to show from Top 5 to Top 20. Choose the output in which you would like to display your results; bar, line, pie chart and so on.

Access Control

Each log display can utilize any one of the following filters:

- Action
- Message Type
- Device Group
- Client IP
- Channel
- Policy Name
- User Name

Continue sorting with time range filters: Today, last 1 hour, last 12 hours, last 1 day. last seven days, or a customized time range. Set the top number of instances you would like to show from Top 5 to Top 20. Choose the output in which you would like to display your results; bar, line, pie chart and so on.

Options for Recording Data

Detail Log Settings in the IWSVA Web console are under **Logs > Log Settings** (see Log Settings starting on page 14-13 for more information).

Querying and Viewing Logs

The IWSVA Web console provides tools to query log files.

- **Log Search** - A search box for each individual facet is provided in IWSVA. It includes an "autocomplete" function that reveals possible results with the search term highlighted.
- **Time Zone** - All logs are displayed within the same time zone that was originally configured in your client.
- **Pie Charts** - Pie charts now include an "other" category. For example, if the user chooses to view the top five malware instances, each malware will have a wedge of the chart and an "other" wedge will appear that includes all malware outside the top five. (If here are only five instances malware, then the "other" wedge does not appear.
- **Add to Favorites** - Add to Favorites enable you to store the frequently-used log settings to the Log Analysis Favorites location. "Favorited" logs can be found at **Logs > Favorites**.

Note: Line and Pie charts both include "drill down" capabilities where you can click the section of the chart you are interested in learning more about and then view detailed information about that section.

Log Settings

From the **Log Settings** screen, you can configure:

- Global Log Settings such as the length of time to store logs and the maximum log size to store.
- Global Log Filter by user names using the bandwidth filter and by both user names and domains using policy enforcement, Internet access, Internet security, data security, and access control filters.

- Anonymous Logging can be enabled or disabled.
- Syslog Servers to use for additional log storage based on type and priority.
- Mounting a local or external location, off loading previous logs (at least the last 45th day logs) to the mounted location, and importing the logs from that location.

To configure Global Log Settings:

1. Go to **Logs** > **Log Settings**.

   The **Log Settings** screen appears.

2. Under **Global Log Settings** section, configure the following:

   a. **Store logs for**: Enter the number of days to retain logs before purging.

   Note: Setting the value to more than 62 days could cause the accumulated data to become large enough to affect performance.

   b. **Maximum logs disk size**: Set the maximum file size of log data to be stored. If log data exceeds the size specified, IWSVA deletes the oldest logs first.

   c. **Mound device**: Enter the path of the local or external location where you want to save logs, and then click **mount**.

   d. **Log Offload**: Select this option if you want to save the logs to the mounted location.

   e. **Log Import**: Select this option if you wan to import and use historical logs saved at the mounted location for log analysis.

   f. Click **Save**.

3. Under **Global Log Filter** section, do the following:

   a. Select a policy and a user from the drop down lists, and type a filter name in the text field provided.

   b. Click + icon.

   c. Click **Save**.

4. If you would like all logs forwarded to a syslog server, then under **Syslog Server** section, do the following:

   a. Click **Add**.

   The **Syslog Configuration: Add Server** screen appears.

  b. Select **Enable Syslog**

  c. Enter the IP address and port number of the server where the syslogs can be forwarded.

  d. Select the log type(s) or syslog priority level(s) you want to save.

  e. Click **Save** to save configuration and return to the **Log Settings** screen.

  f. Select the Syslog Server.

5. Click **Save**.

Global Log Filtering

Use global log filtering when you want specific data omitted from your logs. For example, use this filter in a case where you do not need to log Internet Access logs for user John Smith or Bandwidth usage for users who visit www.google.com.

Anonymous Logging

Some European countries have laws stating that user names cannot be recorded in logs. After enabling this feature, user names within the log will be recorded as MD5 values instead of the actual user names.

Log Offload and Retrieval

IWSVA has a log storage limit. If users do not want to purge old logs, they can offload the logs to their own devices for permanent storage. If they want to analyze the logs in future, they can retrieve these logs from their devices and restore them in IWSVA.

Exporting Log and Report Data as CSV Files

When viewing your log query or a real-time report, IWSVA supports exporting log data to a CSV file in order to view and analyze the data in other applications. Click the table icon and then **Export CSV file** and then download the file from the IWSVA server.

Exporting Report Data as PDF Files

In addition to the CSV export feature, IWSVA also allows you to export report data (up to 1000 raw logs) as PDF files that can be viewed using a PDF-reader application in any platform. Click **PDF** and follow the on-screen prompt to download the file from the IWSVA server.

Syslog Configuration

With syslog server support, IWSVA can send logs to external syslog servers. You can configure up to a maximum of four syslog servers and specify the type or priority level of the logs to send to each syslog server.

To configure a syslog server:

1. Click **Logs >Log Settings > Syslog Server** in the main menu.
2. Click **Add**.
3. For **Syslog Server Settings**:
   a. Select **Enable Syslog** to allow IWSVA to send logs to this syslog server

   b. Specify the **Server name/IP address.** IWSVA supports the sending of syslog messages to both IPv4 and IPv6 hosts. The Web UI can accept both IPv6 host names and addresses similarly to the behavior of IPv4.

   c. Specify the **UDP Port #** (the default is 514)
4. Under **Save the Following Logs**, specify the logs to send. You can select to send events to the syslog server by either the log type or the syslog priority level.
   - Click **By log type** and select the type(s) of logs. Or,
   - Click **By syslog priority level** and select the level(s)
5. Click **Save**.

Introduction to Notifications

Notifications can be issued in response to scanning, blocking, alerting, and program update events. There are two types of notifications—administrator notifications and user notifications. Notifications can be configured in **Notifications** on the main menu, described as follows:

- **Administrator notifications** provide information about HTTP/HTTPS scanning, HTTP/HTTPS file blocking, FTP blocked file types, FTP scanning, threshold alerts, restricted tunnel traffic, High Availability events, and Applets/ActiveX security events, as well as pattern file and scan engine updates. IWSVA sends administrator notifications through email to addresses that you configure in the "**Send notifications to...**" screen.
- **User notifications** provide information about HTTPS access errors, HTTPS certificate warnings, HTTP/HTTPS scans, HTTP/HTTPS file blockages, FTP scans, URL blockages, FTP blocked file types, High Availability events, and Applets/ActiveX scanning events. IWSVA presents user notifications in the client's browser or FTP client in lieu of the prohibited Web page or file that the client is trying to view or download.

The messages presented in both the administrator and user notifications are configurable and can include "tokens" or variables to customize notification messages with information about the event. In addition, user notification messages support HTML tags to customize the appearance of the message and provide links to other resources, such as security policy documents hosted on your intranet.

Note: As with IPv4, all tokens can be applied to IPv6 access, including:
%N - user name
%c: IP address:port after **Error! Hyperlink reference not valid** (for HTTPS decryption). For IPv6, it should be https://[IPv6 address]:port. IPv4 still retains https://IPv4 address:port.

Notification Email Settings

IWSVA sends administrator notifications to email addresses that you specify. The administrator enters email settings when installing IWSVA and when running the setup program, but email settings can also be modified post-installation on the **Notifications > Send notifications to...** screen on the Web console.

To configure email settings for administrator notifications:

1. Click **Notifications** in the main menu.
2. In the **Notifications** screen, click **Send notification to**.

3. Type the email address to send notifications, the sender's email address, the address to send the DLP notifications, the SMTP server, the SMTP server port, and the time interval between checking the mail queue. IWSVA supports sending notifications to IPv4 and IPv6 hosts. The Web UI can accept both hostname and IPv6 address as with IPv4.
4. If your mail server requires ESMTP, enable **Use Extended Hello (EHLO)** for IWSVA to initialize SMTP sessions using the EHLO command.
5. Click **Save**.

Notification Tokens/Parameters

To make notifications more meaningful, IWSVA can use tokens (or variables) as information placeholders in a notification. When an event occurs, IWSVA dynamically substitutes the specific information in place of the variable, providing detailed information about that specific event.

For example, you could create a generic notification as follows:

```
A virus was detected in HTTP traffic.
```

This notification lets you know there is a problem, but does not provide any details. Instead, you could configure the notification using variables as follows:

```
On %Y, IWSVA detected a security risk %v in the file %F. %N
attempted to download the file from %U.
```

The notification might read as follows:

```
On 5/28/08 6:31:56 PM, IWSVA detected a security risk
JS_TEST_VIRUS in the file EXT_JS.JS. 10.2.203.130 attempted
to download the file from
http://10.2.203.130/TESTDATA/virus/NonCleanable/EXT_JS.JS
```

With this information, administrators can contact the client and provide more security information. The notification in this example uses five variables: %Y, %v, %F, %N and %U.

The following table contains a list of variables that can be used in notification messages and pages.

TABLE 14-2. Description of Variables

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
HTTPS Access Denied and HTTPS Certificate Failure		
%o	IWSVA hostname	The IWSVA host name where the event was triggered
%u	URL/URI	
%c	IP address:port after “https://”	Refer to the default message for %c usage example
$$DETAILS	Details of certificate failure reason / access denied reason	
FTP Scanning and HTTP/HTTPS Scanning		
%A	Action taken	The action taken by IWSVA
%F	File name	The name of the file in which a risk is detected, for example, anti_virus_test_file.htm
%H	IWSVA host name	The IWSVA host name where the event was triggered
%L	Detailed file name and reason	
%M	Moved to location	The quarantine folder location where a file was moved
%N	User name	
%R	Transfer direction	
%U	URL/URI	
%V	Malware name (virus, Trojan, or Bot name)	The name of the risk detected
%X	Reasons/block type	
%Y	Date and time	The date and time of the triggering event

TABLE 14-2. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
HTTP/HTTPS Access Denied by Application Control		
%N	User name	
%A	Action	
%P	Path and file name	
%C	Category	
%Z	Policy name	
%Y	Date and time	
%H	IWSVA host name	
Data Loss Protection		
%T	Template name	
%U	URL/URI	
%Y	Date and time	The date and time of the triggering event
%A	Action taken	
%N	User name	
%Z	Policy name	
%H	IWSVA host name	
C&C Callback Attempt Detection		
%Z	Policy name	
%N	User name	
%U	URL/URI	
%A	Action	
%K	Risk level	
FTP Blocked File Type and HTTP/HTTPS Blocked File Type		
%U	URL/URI	

TABLE 14-2. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
The following tokens are only used in messages for administrators or in user notification messages:		
%F	File name	
%A	Action taken	
%H	IWSVA host name	
%R	Transfer direction	
%X	Reasons/block type	
%Y	Date and time	
%N	User name	
%V	Virus, Trojan or Bot name	
Applets and ActiveX Instrumentation		
%D	Protocol being scanned	
%H	IWSVA host name	
%N	User name	
%U	URL/URI	
%W	New certificate information	
%X	[reasons/block type]	
%Y	Date and time	
%Z	Policy name	
HA events		
%H	Host name	
%P	Peer name	
%R	Reason	
URL Filtering by Time Quota		
%U	URL/URI	

TABLE 14-2. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
%C	Category	
%H	IWSVA host name	
%N	User name	
%Q	Quantity of time	
%Y	Date and time	
URL Blocking by Access Control		
%H	IWSVA host name (only works in header field)	
%N	User name	
%U	URL/URI (only works in body)	
%Y	Date and time	
%X	Reason (only works in body)	
URL Blocking by HTTP Inspection		
%H	IWSVA host name	
%I	Filter name	
%N	User name	
%U	URL/URI	
%Y	Date and time	
URL Blocked by URL Filtering		
%C	Category	
%H	IWSVA host name (only works in header field)	
%N	User name	
%U	URL/URI	
%Y	Date and time	

TABLE 14-2. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
URL Access Warning		
%A	Action	
%B	Warn and continue	
%C	Category	
%H	IWSVA host name (only works in header field)	
%N	User name	
%U	URL/URI (only works in body)	
%Y	Date and time	

To customize URL Access Warning notifications, the message template must contain following form to display the “Continue” option:
`<form id="warncontinue" method="post" action="%B$$$IWSX_URL_ACTION$$$">`
`<INPUT type=hidden value="%A" name=data>`
`</form>`
A button or hyperlink must be defined to submit the form about the customized notification that allows users to continue. Example:
`  <input name="button2" type="button" value="Continue at your own risk"`
`style="width:195px"`
`onclick="document.getElementById('warncontinue').submit(); return`
`false;"></input>`		

URL Access Override		
%A	Action	
%B	Continue to URL/URI	
%C	Category	
%E	Policy default Time Limit	
%H	IWSVA host name	
%J	Policy maximum Time Limit	

TABLE 14-2. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
%N	User name	
%U	URL/URI (only works in body)	
%Y	Date and time	
%Z	Policy name	

If you customize URL Access Override notifications, the message template must contain some Java Script code to encrypt the password with base64 code. It should contain some elements: password, time limit and ttl_type. Otherwise, the customized notification page cannot work.
`<form id="overridecontinue" method="post" action="%B[Warn and Continue URL/URI]/$$$IWSX_URL_ACTION$$$">`
`<INPUT type=hidden value="%A[Action]" name=data>`
A button or hyperlink must be defined to submit the form about the customized notification that allows users to continue. Example:
`<input type="button" name="Button22" value="Submit" class="style3" onclick="doSubmit();" />`		

Threshold Alerts		
%m	Metric	
%t	Threshold value	

Configuring Notifications

To configure a notification, select the types of events that issue the notification and then edit the email and browser notification messages.

Using HTML Tags in User Notifications

You can use HTML to format user notification messages. While the HTML files can include reference links to external images or styles, IWSVA only supports uploading HTML files. Any additional files have to be uploaded separately to a Web server, and Trend Micro recommends using absolute links to help avoid broken links.

Configuring Applets and ActiveX Security Notification Settings

When IWSVA detects an attempt to download a Java Applet or ActiveX object that violates a security policy, the application sends an administrator a notification through email and a user notification message in the requesting client's browser.

To configure the Applets and ActiveX security notification settings:

1. Click **Notifications** in the main menu, then click **Applets and ActiveX Instrumentation**.
2. Under **Administrator Notification**, select **Send a message when a malicious Applet or ActiveX attempt is detected**.
3. If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 14-18.
4. For the **User Notification Messages**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and either type or import the customized message's content.
      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

5. Click **Save**.

Configuring C&C Contact Callback Notifications

When IWSVA detects an attempt to download C&C contact objects that violate a security policy, the application sends an administrator a notification through email and a user notification message in the requesting client's browser.

To configure the C&C Contact Callback notification settings:

1. Click **Notifications** in the main menu, then click **C&C Callback Notification**.
2. Under **Administrator Notification**, select **Send a message when C&C callback event is detected**.
3. Choose to send the message to the root recipient after either every incident, or after a specific risk level has been surpassed (low, medium, or high).
4. If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 14-18.
5. For the **User Notification Messages**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and either type or import the customized message's content.
      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
6. Click **Save**.

Configuring Data Loss Prevention Notifications

When IWSVA detects data leakage that violates a security policy, the application sends an administrator a notification through email and a user notification message in the requesting client's browser.

To configure the Data Loss Prevention notification settings:

1. Click **Notifications** in the main menu, then click **Data Loss Prevention**.
2. Under **Administrator Notification**, select **Send a message when data leakage is detected**.
3. If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 14-18.
4. For the **User Notification Messages**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and either type or import the customized message's content.
      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
5. Click **Save**.

Configuring FTP Data Loss Prevention Notifications

When IWSVA detects FTP data leakage that violates a security policy, the application sends an administrator a notification through email and a user notification message in the requesting client's browser.

To configure the FTP Data Loss Prevention notification settings:

1. Click **Notifications** in the main menu, then click **FTP Data Loss Prevention**.
2. Under **Administrator Notification**, select **Send a message when data leakage is detected**.
3. If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 14-18.
4. For the **User Notification Messages**:
   a. Select **Default** to display the default warning message.

b. Select **Customized** to display a custom message and either type or import the customized message's content.

- You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

5. Click **Save**.

Configuring FTP Blocked File Type Notifications

In addition to scanning FTP uploads and downloads, InterScan Web Security Virtual Appliance can block file types at the FTP gateway. To prevent performance issues, the FTP scanning module supports special configurations for compressed files and large files. Spyware and grayware scanning is also supported.

InterScan Web Security Virtual Appliance FTP scanning can be deployed into your environment in conjunction with another FTP proxy server or InterScan Web Security Virtual Appliance can act as its own FTP proxy. And to help ensure the security of the InterScan Web Security Virtual Appliance server, several security-related configurations are available to control access to the InterScan Web Security Virtual Appliance server and its ports.

To configure the FTP blocked file type notification settings:

1. Click **Notifications** on the main menu, then click **FTP Blocked File Type.**
2. Under **Administrator Notification**, check **Send a message when the FTP blocked file type is accessed.**

   Depending on what IWSVA is configured to block, this option can result in a large number of notification messages sent to the default recipient. As an alternative to item-by-item notifications, bear in mind that blocked files are written to a log, and can be included in one of the IWSVA generated reports.
3. If you do not want to use the default notification messages, highlight the default text and type your own. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 14-18.
4. For the **User Notification Message**:

   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and type the customized content.

      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

5. Click **Save**.

Configuring FTP Scanning Notification Settings

When IWSVA detects malicious code in a user's FTP transfer, it can automatically send a customized administrator notification to the designated email addresses and/or display a notification in the requesting FTP client program.

To configure the FTP scanning notification settings:

1. Click **Notifications** on the main menu, then click **FTP Scanning**.
2. Under **Administrator Notification**, select the trigger detection events for sending a notification (**Virus** and/or **Trojan** and/or **Other malicious code**).
3. If you do not want to use the default notification messages, highlight the default text and type your own. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 14-18.
4. For the **User Notification Message**:
   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and type the customized content.

      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
5. Click **Save**.

Configuring HTTP/HTTPS File Blocking Notifications

When IWSVA blocks a file, it sends an administrator notification through email, and a user notification message is displayed in the requesting client's browser.

To configure HTTP/HTTPS file blocking notifications:

1. Click **Notifications** and then click **HTTP/HTTPS Blocked File Type**.
2. Under **Administrator Notification**, select **Send a message when the blocked file type is accessed**.
3. If you do not want to use the default notification message, highlight the default text and type your own version. If applicable, insert tokens in the text as described in Notification Tokens/Parameters starting on page 14-18.
4. Type the **Headline** to appear in the browser.

   The default headline is *Trend Micro InterScan Web Security Event*. The headline is common for virus infection messages, file-type blocking, and URL blocking messages.
5. For the **User Notification Message**:

   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and either type or import content from an HTML file.

      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
6. Verify the notifications by clicking **Preview**.
7. Click **Save**.

Configure HTTP/HTTPS Scanning Notifications

When IWSVA detects malicious code in a file requested by a client, it issues an administrator notification through email and a user notification in the requesting client's browser.

Because IntelliTrap is considered a type of security threat, it uses the same notifications as HTTP/HTTPS Scanning.

To configure HTTP/HTTPS scanning notifications:

1. Click **Notifications** and then click **HTTP/HTTPS Scanning**.
2. Under **Administrator Notification**, select the trigger detection events for sending a notification (**Virus** and/or **Trojan** and/or **Other Internet Threats** and/or **Bots**)

   Note: IntelliTrap notification is associated with **Other Internet Threats**. Therefore, IntelliTrap notification is enabled when you select **Other Internet Threats**.

3. If you do not want to use the default notification message, highlight the default text and type your own version. If applicable, insert tokens in the message as described in Notification Tokens/Parameters starting on page 14-18.
4. Type the **Headline** to appear in the browser.

   The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.

5. For the **User Notification Message** for **Message for downloaded file** and **Message for uploaded file**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and either type or import the customized message's content from an HTML file.
      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
   c. Verify that the notifications appear correctly by clicking **Preview**.
6. Click **Save**.

Configuring HTTPS Access Denied Notifications

Whenever users are denied to access a Web site through HTTPS connections, they will see an HTML page explaining that their request has been rejected.

To configure HTTPS access denied notifications:

1. Click **Notifications** and then click **HTTPS Access Denied**.
2. Type the **Headline** to appear in the browser.

   The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
3. For the **User Notification Message**:
   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and either type or import content from an HTML file.

   - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
   - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
4. Verify the notifications by clicking **Preview**.
5. Click **Save**.

Configuring HTTPS Certificate Failure Notifications

Whenever users are denied to access a Web site whose certificate does not pass the verification tests, they will see an HTML screen with the warning message. Users have the option to continue accessing the Web site without decrypting and checking HTTPS traffic.

To configure HTTPS certificate failure notifications:

1. Click **Notifications** and then click **HTTPS Certificate Failure**.
2. Type the **Headline** to appear in the browser.

   The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
3. For the **User Notification Message**:
   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and either type or import content from an HTML file.

- You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

4. Verify the notifications by clicking **Preview**.
5. Click **Save**.

Configuring HTTP/HTTPS Access Denied by Application Control Notifications

Whenever users are denied to access an HTTP/HTTPS Web site whose certificate does not pass the verification tests, they will see an HTML screen with the warning message. Users have the option to continue accessing the HTTP/HTTPS Web site without decrypting and checking HTTP/HTTPS traffic.

To configure HTTPS certificate failure notifications:

1. Click **Notifications** and then click **HTTP/HTTPS Access Denied by Application Control**.
2. Type the **Headline** to appear in the browser.

   The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
3. For the **User Notification Message**:
   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and either type or import content from an HTML file.

      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
4. Verify the notifications by clicking **Preview**.
5. Click **Save**.

Enabling Pattern File Updates Notifications

IWSVA can send notifications when the product attempts to update engines or pattern files based on scheduled pattern updates.

Note: IWSVA will not send notifications for manual pattern updates.

To enable pattern file update notifications:

1. Click **Notifications** from the main menu, then click **Pattern File Updates**.
2. For the pattern update attempts:
   a. Select the update events that trigger a notification. You can configure notifications for **Successful**, **Unsuccessful** or **Not needed** update attempts.

   b. Type a **Subject** for the notification message. Default is *IWSVA pattern update result*.
3. Click **Save**.

Configuring Threshold Alert Settings

IWSVA can send notifications when the product has exceeded the threshold values you have set.

To enable threshold alert notifications:

1. Click **Notifications** from the main menu, then click **Threshold Alerts**.
2. For the thresholds alerts:
   a. Enable the threshold alert type, value, and the frequency limitations of your notification messages.

   b. To change the recipient, click **Notifications** in the main menu, and then "**Send notifications to...**" in the upper right corner.

   c. Use the default message or create one of your own under **Notification Message**.
3. Click **Save**.

Configuring URL Access Warning Notifications

The URL Access Warning Mode sends notifications if the URL Filtering rules action is set to "Warn" and the user attempts to access a URL that belongs to a category prohibited by company policy. (See Creating a New Policy on page 11-6 for details.) The user receives the warning before seeing the Web page.

The user has an option to click one of the following links in the warning message:

- Go back to previous webpage safely OR
- Continue at your own risk (not recommended)

To configure the URL Access Warning notifications:

1. Click **Notifications** on the main menu and then click **URL Access Warning**.
2. Type the **Headline** to appear in the browser.

   The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
3. For the **User Notification Message**:

   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and either type or import content from an HTML file.

   - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
   - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
   - The notification must contain a form to submit necessary information to IWSVA if end users choose to continue. The format is:

```
<form id="warncontinue" method="post" action="%B$$$IWSX_URL_ACTION$$$">

<INPUT type=hidden value="%A" name=data>

</form>
```

- A button or hyperlink must be defined to submit the form about the customized notification for users to continue. Example:

```
<a href="javascript:void(0)"
onclick="document.getElementById('warncontinue').submit();

return false;">Continue to this website (not recommended)</a>
```

4. Verify the notifications by clicking **Preview**.
5. Click **Save**.

Configuring URL Access Override Notifications

A user receives the URL Access Override Mode notification if a user tries to access a URL in a category that has a "block with override" action set by company policy. The user receives the override warning and needs to enter a password to continue. In the notification, the user sees the amount of additional time allowed for browsing. After entering the correct password, the user continues to the requested Web page.

The user has an option to click one of the following links in the warning message:

- Discontinue browsing that page if password is not known
- Enter the password and continue browsing for the specified period of time

The administrator must first set the category action in the policy to the "Block with Override" action setting. See Creating a New Policy on page 11-6 for details.

To configure a user notification message for URL Access Overrides:

1. Click **Notifications** in the main menu, then click **URL Access Override**.
2. Under **User Notification Message for URL Access Override**:
   - **a.** Type the **Headline** to appear in the browser.

     The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
   - **b.** Click **Default** to display the default warning message.
   - **c.** Click **Customized** to display your own warning message. Type the message in the text box, or **Import** it from a HTML file on your local machine.
     - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).

- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

d. If you customize URL Access Override notifications, the message template must contain some Java Script code to encrypt the password with base64 code. It should contain some elements: password, time limit and ttl_type. Otherwise, the customized notification page cannot work.

Example:

```
<form id="overridecontinue" method="post" action="%B[Warn and Continue
URL/URI]$$$IWSX_URL_ACTION$$$">

<INPUT type=hidden value="%A[Action]" name=data>

..

</form>
```

e. A button or hyper link must be defined to submit the form about the customized notification for users to continue.

Example:

```
<input type="button" name="Button22"

value="Submit" class="style3"

onclick="doSubmit();" />
```

3. Verify the notifications by clicking **Preview**.
4. Click **Save**.

Configuring a URL Blocking by Access Control Notification

When IWSVA detects an attempt to access a URL in the Phish pattern file or a prohibited URL from the local IWSVA list, IWSVA displays a warning screen in the browser of the requesting client to indicate the URL was blocked.

To configure a user notification message for URL Blocking by Access Control:

1. Click **Notifications** in the main menu, then click **URL Blocking by Access Control**.
2. Under **User Notification Message for Restricted or Blocked URLs**:

   a. Type the **Headline** to appear in the browser.

The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.

b. Click **Default** to display the default warning message.

c. Click **Customized** to display your own warning message. Type the message in the text box, or **Import** it from a HTML file on your local machine.

- You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

3. Verify the notifications by clicking **Preview**.
4. Click **Save**.

Configuring a URL Blocking by HTTP Inspection Notification

When IWSVA detects an attempt to access a URL in violation of an HTTP Inspection policy with a blocking action, IWSVA displays a warning screen in the browser of the requesting client to indicate the URL was blocked.

To configure a user notification message for HTTP Inspection:

1. Click **Notifications** in the main menu, then click **URL Blocking by HTTP Inspection**.
2. Under **User Notification Message for Restricted or Blocked URLs**:

a. Type the **Headline** to appear in the browser.

The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.

b. Click **Default** to display the default warning message.

c. Click **Customized** to display your own warning message. Type the message in the text box, or **Import** it from a HTML file on your local machine.

- You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).

- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

3. Verify the notifications by clicking **Preview**.

Configuring a URL Blocking by URL Filtering Notification

When IWSVA detects an attempt to access a URL in the Phish pattern file or a prohibited URL from the local IWSVA list, IWSVA displays a warning screen in the browser of the requesting client to indicate the URL was blocked.

To configure a user notification message for URL Blocking by URL Filtering:

1. Click **Notifications** in the main menu, then click **URL Blocking by URL Filtering**.
2. Under **User Notification Message for Restricted or Blocked URLs**:
   a. Type the **Headline** to appear in the browser.

      The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection, file-type blocking, and URL blocking messages.

   b. Click **Default** to display the default warning message.

   c. Click **Customized** to display your own warning message. Type the message in the text box, or **Import** it from a HTML file on your local machine.

      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
3. Verify the notifications by clicking **Preview**.
4. Click **Save**.

Enabling Notifications for URL Filtering Engine and Scan Engine Updates

Though less frequent than pattern file updates, Trend Micro periodically releases new versions of the scan engine to reflect advances in virus and malicious code detection methods. IWSVA can issue administrator notifications in response to scheduled scan engine updates.

Note: IWSVA will not send notifications for manual engine updates.

To enable URL Filtering and Scan Engines Update Notifications:

1. Click **Notifications** from the main menu, then click **URL Filtering and Scan Engines Update**.
2. For the scan engine and/or the URL filtering engine, select the update events to trigger a notification.

   You can configure notifications for **Successful**, **Unsuccessful,** or **Not needed** update attempts.
3. For the scan engine and/or the URL filtering engine, type the **Subject** of the notification email message.
4. Click **Save**.

Configuring URL Filtering by Time Quota Notification Settings

If a rule in a URL Filtering policy has a time limit action, the URL Filtering by Time Quota notification can be received by a user. End-users will see it appear in their Web browser whenever a policy is configures with the "Time Limit" action in **URL Filtering > Policies | Rule** tab. See Creating a New Policy on page 11-6 for details.

Whenever users try to download a page that has been configured in IWSVA with a time limit action, and if the time limit has been exhausted, they will see an HTML page explaining that their request has been rejected (if the option is enabled). See URL Filtering Time Quota Extension on page 11-14 for details.

To configure the URL Filtering by Time Quota notification settings:

1. Click **Notifications** in the main menu, then click **URL Filtering by Time Quota**.
2. If you do not want to use the default notification message, check the Customized check box and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 14-18.
3. Click **Save**.

Configuring Smart Scan Event Notifications

IWSVA can send a notification email when global Smart Protection Server is unavailable, and IWSVA switches to conventional scan.

To enable 'Smart Protection Server Unavailable' notifications:

1. Click **Notifications** on the main menu and then click **Smart Scan Events**.
2. Select the **Send a message when Smart Protection Server is unavailable** check box.
3. Click **Save**.

Note: IWSVA sends out email notifications only when the Smart Protection Server is not reachable and IWSVA switches to conventional scan. IWSVA will not send notifications if you manually switch from Smart Scan to Conventional Scan.

Note: The Smart Scan Even Notification does not use any token variable.

Enabling SNMP Trap Notifications

IWSVA supports sending SNMP traps in response to security, update, or program events.

Note: SNMP Settings will not be shown on the **Notifications** page as long as SNMP is not enabled. To send SNMP traps, you need to configure the SNMP settings and then enable this feature. Choose **Administration > Network Configuration > SNMP Settings**.

To enable sending SNMP traps:

1. Click **Notifications** on the main menu and then click **SNMP Notification Settings. . .** at the bottom of the screen.
2. Select the types of events that triggers an SNMP trap. The different classes are:
   - **Virus or Internet threats**—Events related to virus or malicious code detections

- **Security violations**—Activities that are prohibited by IWSVA policies, not related to viruses or malicious code
- **Pattern, database or scan engine updates**—Events related to IWSVA updates
- **IWSVA service interruptions**—Issues with any of the essential IWSVA services
- **System performance metric**—IWSVA periodically sends an SNMP trap with the following performance data:
    - CPU load percentage
    - Memory load percentage
    - Disk load percentage
    - Concurrent connection (ICAP request and response mode and proxy mode)
    - Incoming and outgoing throughput (bytes per second)
- **High Availability events**—Issues with any of the essential HA functions, if HA is used.
- **Hardware monitoring events**—Events related to monitored hardware components:
    - Voltage
    - Fan
    - CPU
    - Storage
    - Temperature

3. Click **Save**.

Chapter 15

Administration

This chapter describes the administrative functions available in IWSVA.

Topics in this chapter include the following:

Overview

The Administration menu includes the following options:

- Audit Log on page 15-3
- IWSVA Configuration on page 15-3
    - User Identification on page 15-4
    - Policy Deployment on page 15-13
    - Database Connection on page 15-13
    - Quarantine Management on page 15-14
    - System Time on page 15-15
    - Scheduled Times on page 15-16
    - Register to Control Manager on page 15-16
    - Configuration Replication on page 15-17
    - Central Log/Reporting on page 15-17
    - Scan Method on page 15-18
    - PAC File Management on page 15-19
    - Network Configuration on page 15-19
    - Network Interface on page 15-20
    - Web Console on page 15-20
    - Remote CLI on page 15-21
    - SNMP Settings on page 15-21
    - Static Routes on page 15-22
- Management Console on page 15-23
    - Role-based Administration on page 15-24
    - Role Management on page 15-24
    - Account Administration on page 15-29
    - Access Control Settings on page 15-31
- Syslog Server on page 15-32
- Config Backup/Restore on page 15-33
- System Updates on page 15-33
- System Maintenance on page 15-34

- System Event Log on page 15-35
- Product License on page 15-35
- Support on page 15-39

Audit Log

The audit log contains information that describes any configuration changes that users make to the application. For instance, after a migration or rollback procedure is activated by a user, an entry recording the migration activity is created in the audit log.

Note: All IPv6 related configuration changes will be logged the same as the IPv4 audit logs.

To view the audit log:

1. Click **Administration > Audit Log** in the main menu.
2. Under **Time period**, select the time for which you want a report generated.

   Click **Range** to view the virus log in a given time range, then select the start and end dates.
3. Under **User(s)**, select the user(s) for which you want to view log entries. Click **Add** (or **Add All** for all users listed). To remove user(s) from the right list box, click **Remove** (or **Remove All** for all users listed).
4. Under the **Sort by** section, select an option by which to sort the display log. The options are "User" and "Date."
5. Click **Show Log**. The **Audit Log** screen opens.
6. Click **Refresh** to update the screen.

IWSVA Configuration

IWSVA Configuration contains the following items:

- User Identification on page 15-4
- Policy Acknowledgement Screen on page 15-11
- Approved Authentication List on page 15-13
- Policy Deployment on page 15-13

- Database Connection on page 15-13
- Quarantine Management on page 15-14
- System Time on page 15-15
- Scheduled Times on page 15-16
- Register to Control Manager on page 15-16
- Configuration Replication on page 15-17
- Central Log/Reporting on page 15-17
- Scan Method on page 15-18
- PAC File Management on page 15-19

User Identification

IWSVA supports multiple user identification methods:

- IP address
- Host name
- User/group name

Note: Changing the user identification method can affect any existing policies you might have created, as well as logs and reports.

With IWSVA, when you want to use a user/group-based policy and you have an LDAP server on the network, choose the **User/group Authentication Setting** and contact your LDAP administrator for information about the various attribute settings.

Select your preferred method of user identification for reports, logs, notification messages, and for creating scan policies.

User/Group Authentication Settings

Basic (single Active Directory server)

With IWSVA's enhanced LDAP functionality, several settings for Microsoft's Active Directory can automatically be detected that will simplify your configuration. Many use Microsoft Active Directory; this might be the best option for those with less-complex configurations.

To use Basic (single Active Directory server), click **Administration > IWSVA Configuration > User Identification** and check **Basic** (single Active Directory server) on the **User Identification** screen.

Under the Basic (single Active Directory server) view, only the following settings are necessary:

- Domain name
- Service account
- Password

Your LDAP vendor must use Microsoft Active Directory for the auto-detect function to work correctly. IWSVA automatically detects all the available servers for any given domain and then chooses the most appropriate one for your configuration, as well as other important settings.

IWSVA does auto-detection as follows:

- Acquires the LDAP server list through a DNS query
- Filters out unconnected servers
- The fastest GC or DC will be selected as the primary LDAP server when more than one GC or DC is located among LDAP servers.
- Domain names will be translated into BDN.
- Kerberos information is generated and authenticated.

Advanced (other or multiple LDAP servers)

Use this option to do fine-grained or complex LDAP configurations. Besides Active Directory, other LDAP servers as well as multi-domain forests and redundant LDAP servers are supported in the **Advanced (other or multiple LDAP servers)** view. You can add multiple domains for User/Group Authentication. IWSVA sequentially queries these domains for user identification and policy enforcement.

To use Advanced (other or multiple LDAP servers) from the web console, click **Administration > IWSVA Configuration > User Identification** and check **Advanced (other or multiple LDAP servers)** in **User Identification**.

You can add, remove, or edit domain configurations from the **Advanced (other or multiple LDAP servers)** view, and create a list that shows all the configured domains. View the details of any one domain by clicking the domain name or the down-array button.

Note: IWSVA cannot check whether a domain is a sub-domain. If you specify two domains, one is going to be the other's sub-domain, but IWSVA treats them as independent domains.

To configure the New LDAP Configuration page:

1. Enable **Advanced (other or multiple LDAP servers)** and click **Add New Domain** or any existing LDAP domain name to view the details.
2. Enter or edit the following:
   - **Domain name**
   - **Server type**
   - **Service account**
   - **Password**
   - **LDAP server hostname**
   - **Listening port number**
   - **LDAP port number**
   - **LDAP encryption**
   - **Base distinguished name (BDN)**

   Note: The default encryption method is None. If LDAP server supports LDAPv3 StartTLS extension or LDAP over SSL, select the appropriate encryption method.

3. For the Authentication Method, select one that meets your expectations, then enter your Kerberos domain or realm, the Kerberos server, and the Kerberos port.
4. For Authentication High Availability, you can enable additional server relationships for the same domain by selecting **Enable additional LDAP servers for the same domain**. Set the server relationship (Round Robin or Fail-over) and enter the names of any additional backup LDAP servers.

Configuring one domain is a considerable undertaking. To complete a simple configuration, use the auto-detect button provided in the Basic view. It automatically fills the form. You can modify the domain configuration base on the output of an auto-detected configuration. This button is only available for Microsoft Active Directory users in the Basic view.

To some extent, the authentication method settings depend on the LDAP vendor. Some authentication methods are only valid for certain vendors. The following table shows their relationship.

TABLE 15-1. LDAP Vender Authentication Method Relationships

	ACTIVE DIRECTORY	OPENLDAP	SUN IPLANET DIRECTORY SERVER	NOVELL EDIRECTORY
Simple	**No**	Yes	Yes	Yes
Kerberos	Yes	Yes	**No**	Yes
Digest - MD5	**No**	Yes	Yes	Yes

IWSVA supports high availability for LDAP authentication. You can specify one backup LDAP server that shares the same configuration with the primary one. However, two high availability modes are supported:

- Round Robin: By default, IWSVA alternately authenticates users with all LDAP servers.
- Fail-over: When the primary server is down, IWSVA refers to other servers to authenticate users.

Note: Each domain can configure only one BDN and LDAP server type, and the BDN should be unique from other domains.

When multiple domains are supported, you can use any account that belongs to any domain to log in. At first, IWSVA checks the domain names, then authenticates users for the matched domain name server. If no domain name has been input, it will use the first one as the default login domain name.

5. After your configuration is ready, click **Save**. Click **Cancel** to start over. After successfully saving your configuration, return to the LDAP server list.

   The following conditions cannot be saved; you will be prompted with a corresponding error message:

   - No LDAP servers present
   - No BDN listed
   - Missing administrator account or password
   - Missing authentication information when choosing Advanced Authentication Mode
   - Failing to pass the LDAP connection test

Global Authentication Cache Settings

Fixed TTL - The expiration time for each record in the Client IP to User ID cache is different. When a record's life reaches its expiration time, this record is purged. The expiration time for a record is calculated as follows:

Expiration time = Record generation time + Fixed TTL

Last active TTL - When adding a record into the Client IP to User ID cache, this record has a pre-configured expiration interval, for example, 360 seconds. Before reaching the expiration time, if this record is hit, the expiration interval for this record is refreshed and becomes 360 seconds again. If a record is not hit during the expiration interval, this record is purged.

By default, Last Active TTL is enabled.

Standard Authentication Method

Standard Authentication can be configured by selecting Standard Authentication (provided by the operating system or browser) option on the **Administration > IWSVA Configuration > User Identification** screen from the Web console.

In Standard Authentication, authentication is implemented through the authentication features provided by OS or browser.

When the client participates in the domain accesses to Web through the browser supporting NTLM authentication, no pop-up window appears to request authentication since the authentication information is automatically sent from the browser.

If the client does not participate the domain, the browser does not support NTLM authentication, or automatic authentication is disabled by the browser, pop-up will appear to request authentication since automatic authentication is not implemented.

Captive Portal

To configure Captive Portal, select the Captive Portal (Custom Authentication Page delivered by IWSVA to browser) option on the **Administration > IWSVA Configuration > User Identification** screen from the Web console.

If the Captive Portal is configured, custom authentication page appears, and authentication will be requested when the client participates in the domain accesses to Web for the first time (automatic authentication will not be implemented transparently).

The login interface screen can be customized. The screen appears when users access the restricted network for the first time or users are not recognized by IWSVA.

IWSVA also provides an Advanced mode to create a customized Captive Portal. In the Advanced mode, you can write you own HTLM. However, at least the following Java Script must first be inserted into a customized Captive Portal:

```
<SCRIPT LANGUAGE="JavaScript">function
accesspolicy(){var str1 =
window.location.href;//alert(str1);var
s=str1.indexOf("?forward=");//alert(s);var
d=str1.indexOf("&IP");//alert(d);var
uri=str1.substring(s+9,d)+"/$$$GUEST_POLICY$$$";//alert(
uri);return uri;}</SCRIPT><form name="loginForm"
method="POST"
```

```
action="com.trend.iwss.gui.servlet.captiveportal"><tr><t
d>User name: </td><td><input name="username" type="text"
class="button" size="24"
/></td><td>&nbsp;</td></tr><tr><td>Password:</td><td><in
put name="password" type="password" class="button"
size="24" /></td><td><input name="Submit"
type="submit"></td></tr></form><div class="accessmsg"
[Display GuestPolicy Message...] >If you are a guest,
please select the Guest Access option to access the
Internet</div><input name="Access" type="button"
onclick="window.location.href=accesspolicy();" [Display
GuestPolicy...]/>
```

This Java Script is required for the Authentication Form, the Guest Access button, and the Event Handler to appear. Without this script, users will be unable to pass the authentication.

Note: Captive Portal is not supported in ICAP mode.

Allow Guest Login

You can enable guest access when the **Allow Guest Login** box is checked. When enabled, an additional button labeled **Guest** appears. Guests can access the Internet by selecting this button, however, their behavior is under the control of the guest policy. The guest policy automatically appears when guest access is enabled in the policy list. Otherwise, it is invisible.

To allow guest access:

1. In the **Authentication Method** section, select the **Captive Portal (Custom Authentication Page delivered by IWSVA to browser)** option.
2. Click the **Allow Guest Login** checkbox.
3. You can predesign a "look" for the Captive Portal page and save it as HTML. Match the look and feel of your own corporate branding through the use of colors, logos, and text. Copy and paste your customized HTML code into the empty box. Use the <%T%> tag to display the login credentials and guest access buttons.
4. Click **Preview Login Screen** to view your results.
5. Click **Save** to preserve your settings.

Cookie Mode

Cookie mode is used for user identification in NAT and terminal server environments. To use Cookie Mode, ensure that Adobe Flash Player has been installed on the client machine and that browser cookies are enabled.

Cookie Mode is only available when user/group authentication is enabled and Captive Portal is selected.

Use the “Stay signed in” option on the Captive Portal login page to enable cookie “lifetime” for up to one year. If the “Stay signed in” option is not selected, cookie “lifetime” is one day.

None

(Not recommended) Logged events and reports will be anonymous; URL Filtering and other policies are created based on IP addresses.

Note: 1. Host name identification is only supported for end-users browsing with Internet Explorer on Microsoft Windows platforms.
2. Because IWSVA is unable to obtain host name information before decrypting HTTPS contents, IWSVA does not support host name identification for HTTPS decryption policies in the bridge or WCCP modes.
3. You can use the `configure module identification mac_address enable` command in the CLI to include the machine address (MAC) of the client computers in event logs, reports, and notifications. You must run the `register_user_agent_header.exe` file on each client.

WARNING! **Before choosing the Host name, you need to prepare all clients on the LAN by running the `register_user_agent_header.exe` file on each client. This file can be found as part of the installation package. You can conveniently run this file by adding it to your Windows domain login script (or by creating one for just this purpose).**

Policy Acknowledgement Screen

The Policy Acknowledgement Screen tab informs corporate network users of the company Internet usage policy.

Basic Mode

When the Policy Acknowledgement Screen (PAS) is enabled, user are shown a copy of your corporate internet access policy. However, before the **Policy Acknowledgement Screen** can be used, LDAP authentication must first be enabled.

The PAS can be customized through the **Policy Acknowledgement Screen** tab in the **Administration > IWSVA Configuration > User Identification** tab on the Web console. You can also enable or disable the **Policy Acknowledgement Screen** in this location.

Customize a Policy Acknowledgement Screen:

1. **Display Policy Acknowledgement Screen** - When this box is checked, whether or not IWSVA can authenticate users transparently, all users will be directed to the PAS. If IWSVA fails to authenticate the user transparently, Captive Portal will request users to provide a username and password to continue. If IWSVA has already authenticated the user transparently, users can click the button labeled "Go" to continue. In both cases, PAS will appear and reveal your company's usage policy for those accessing the Internet. The PAS only appears when the user accesses the Internet for the first time. After that, it does not appear until the cache expires.

Customize a Policy Acknowledgement Screen with Basic Settings:

1. Enter a Welcome message.
2. Enter your company name: such as Trend Micro, Google, and so on.
3. Upload a company logo. Image size should be less than 1MB.
4. Enter an external HTTP link.
5. Enter a policy message.
6. Click **Save**.

Display a Policy Acknowledgement Screen:

1. Access the screen options at **Administration > IWSVA Configuration > User Identification | Policy Acknowledgement Screen**.
2. Click the check box for Display Policy Acknowledgement Screen. A separate screen will appear displaying an appropriate use policy message to users each time they access the Internet after a 24-hour cycle.
3. Configure this screen in one of two ways. The Basic mode or the Advanced mode - as described in the sections that follow.

Approved Authentication List

After enabling LDAP authentication, all users must provide a username and a password except that whose IP addresses fall within your company's Approved Authentication List. You can define this list with a particular IP address, IP Range, or an IP Mask. Select **Administration > IWSVA Configuration > User Identification > Approved Authentication List** to create or edit your company's approved list.

Policy Deployment

After creating or modifying a policy, you can immediately deploy it to the IWSVA policy database by clicking **Deploy**. Alternatively, you can do nothing and the policies will be automatically deployed according to the Time-to-Live (TTL) interval set in the Administration > Policy Deployment page.

By default, IWSVA will automatically deploy new policies after 30 minutes for the following types of Application Control, Bandwidth Control, and HTTP policies:

- Virus scan policy
- HTTPS policy
- Applet and ActiveX policy
- HTTP Inspection policy
- URL filtering policy
- Access quota policy
- Application Control policy
- Bandwidth Control policy
- DLP policy

Database Connection

IWSVA uses either an existing PostgreSQL database, or installs its own PostgreSQL database. The database holds policy settings and log data. Database connection can be checked on the **Administration > IWSVA Configuration > Database Connection** tab on the Web console. Database settings are stored in the `/etc/iscan/intscan.ini` file. These fields show the choices made during Setup, and should not be changed independent of the Linux ODBC Data Source.

Database Connection Settings:

- **ODBC data source name**—Shows the ODBC name chosen during Setup.
- **User name**—Shows the user name for the ODBC data source; determined during Setup. Default is "sa"
- **Password**—Displays the encrypted ODBC password chosen during Setup.
- **Test Database Connection**—Click to check that the Policy Database and Log Database connections are correct and that the connection is working. Response messages are generated from the native ODBC data source.

Quarantine Management

Most Internet threats, including spyware, Trojans, and worms cannot be "cleaned" because they do not actually "infect" the file. Trend Micro recommends you delete worms (because of the huge numbers possible) and quarantine or delete spyware, Trojans, and other unwanted programs that IWSVA has been configured to detect.

Quarantine Directory

Specify quarantine directory—When the Scan Policy Action for HTTP and/or FTP scanning is Quarantine, IWSVA moves those files to the directory specified here. The default location is:

```
/var/iwss/quarantine
```

Note: Trend Micro recommends that you encrypt all quarantined files as described in Encrypting Quarantined Files on page 15-14.

Encrypting Quarantined Files

Quarantined files are likely to be dangerous. Encrypting files for quarantine can help protect against accidental reinfection or the effects of some other type of malicious code.

Trend Micro recommends that if you choose to quarantine rather than delete suspect files, that you encrypt them before saving to the quarantine directory.

Note: See the "How to" section of the IWSVA Online Help for instructions on decrypting quarantined files.

To encrypt HTTP quarantines:

1. Click **HTTP > Advanced Threat Protection > Policies**, and then either choose an existing policy from the list, or click **Add** to create a new one.
2. Open the Virus/Malware Scan Rule tab. At the bottom of the page, click the **Encrypt quarantined files** check box.

To encrypt FTP quarantines:

1. Click **FTP > Scan Rules**.
2. Open the **Virus Scan Rule** tab. At the bottom of the page, click **Encrypt quarantined files**.

System Time

In the System Time page of the IWSVA Web console, you can manually configure the date and time. IWSVA also supports NTP servers and synchronizes the date and time information based on the specified schedule.

System Time Settings

Synchronize date and time with an NTP server—Select this option to obtain date and time information from the specified NTP server. IWSVA supports both IPv4 and IPv6 NTP servers. You can enable automatic time synchronization based on the schedule you select from the list. Click **Synchronize Now** to connect to the NTP server and update the system date and time. This also allows you to test whether the NTP server is available.

Set the system time manually—Select this option and enter the system date and time in the fields.

Time Zone

Select your continent and nearest city from the lists provided.

Scheduled Times

When configuring URL Filtering, Application Control, or Bandwidth Control policies, you can have IWSVA differentiate between multiple scheduled times. For example, you can allow recreational Web surfing or use of IM applications before and after scheduled work hours. Filtering schedules can be policy based—different schedules can be given to different individuals or groups.

Register to Control Manager

Note: Control Manager does not support IPv6, so you will not be able to connect TMCM with an IPv6 connection. IWSVA can connect to TMCM with IPv4 addresses and retain all other legacy functionality.

Use the **Administration > IWSVA Configuration > Register to Control Manager** screen to configure the communication between the Communication Protocol (MCP) agent and the Trend Micro Control Manager server.

- **Connection Settings**—Specify the entity name (instance of IWSVA on the particular machine). The entity name appears in the Control Manager product tree, helping you to identify the product.
- **Control Manager Server Settings**—Specify the FQDN (Fully Qualified Domain Name) or IP address of the Control Manager server. The Web server authentication user name is used by the Internet Information Services (IIS) server for authentication. This information is not used by Control Manager.
- **MCP Proxy Settings**—In this section, specify the proxy server for communication with the Control Manager server.
- **Two Way Communication Port Forwarding**—Two-way communication allows the TMCM server to send commands in real-time to IWSVA. If the user does not specify this information, the agent defaults to one-way communication, which means IWSVA polls the TMCM server at set intervals to retrieve the commands.

Configuration Replication

Provides IWSVA device registration and configuration replication from an IWSVA source instance to an IWSVA receiver instance. When you would like to copy the policies and configuration files of one IWSVA device to one or more other IWSVA destinations on a manual or recurring basis, use Configuration Replication. You can set policies to configure replication frequency and select a root account to export the configuration files from the replication source.

To set up a configuration replication policy:

1. Open the IWSVA Web console and click **Administration > IWSVA Configuration > Replication Configuration**.
2. Choose a server role, whether standalone (default), source, or receiver.

   If source, check Configuration replication source and click **Save**. A pop-up message appears to confirm a successful replicate source has been established. Click **OK**. If receiver, continue with the following steps.
3. Check Configuration receiver and enter a replication source management IP address, port, and security protocol.

   Specify the name and password of the Replication Source Administrator Account (admin) used to export the configuration files from the replicate source.The policy and configuration replication occurs hourly by default.
4. Click **Save**.

Note: Only "super admin" can perform the manual sync.

Central Log/Reporting

IWSVA uses a log source list and status available from the server. Central Log/Reporting is supported for multiple IWSVA servers. You can choose one of IWSVA servers to use as the log/report console (thereafter known as the "log server.") IWSVA will send their logs to this server. You can manage your log/report on log server using device group.

To set up Central Log/Reporting:

1. From the IWSVA menu, click Administration > IWSVA Configuration > Central Log/Reporting.
2. The default server role is Standalone. Choose a server role, whether log server or log source.
   - **Log Server**
     - **i.** If you use it as Log received server, check Log Server and click **Save**.
     - **ii.** Pop-up will be shown saying set was successful and click **OK**.
     - **iii.** Open the IWSVA Web console and click **Administration > IWSVA Configuration > Central Log/Reporting** and select device group at **Device Group Management**.
     - **iv.** To add a new group, click **Add**, then specify a group name and description, select IP address(es), and then click **Save**.
   - **Log Source**
     - **i.** If you send as log source server to other IWSVA server, check Log Source and specify the Management IP, Management Port, and administrator account password of the log receiving server.
     - **ii.** Click **Save**.

All the existing device groups are displayed in Device Group Management, and the device groups are also displayed on Logs, Reports and Dashboard screens and enable you to query logs and reports on these screens.

Scan Method

Use this screen to configure the scan methods for the data and web sites. IWSVA provides three types of scans:

- Smart Scan with Global Smart Protection Server (SPS)—Smart Scan uses Trend Micro's Smart Protection Network to scan web sites and data. Smart Scan leverages the threat signatures stored in-the-cloud to provide the latest and most updated protection.

- Smart Scan with Local Smart Protection Server (SPS)—To avoid latency introduced in cloud scans, IWSVA sends scan requests to your local smart protection server. The Local Smart Protection Server will provide more privacy and improve the processing speed. Protection is automatically updated and strengthened as more products, services and users access the network creating a real-time neighborhood watch protection service for those who use it.
- Conventional Scan—The Convention Scan uses anti-malware and anti-spyware components stored locally.

Note: To use Smart Scan, IWSVA requires continuous connection with Smart Protection Network. If IWSVA fails to connect to Smart Protection Network for three consecutive times, IWSVA automatically switches to Conventional Scan to continue providing the protection. If switching to Conventional Scan automatically, you should select **Smart Scan** from **Administration > IWSVA Configuration > Scan Method**.

PAC File Management

Use this screen to manage proxy auto-config (PAC) files, including adding, editing, copying and deleting PAC files.

For each PAC file, you can specify the file name, description and content. IWSVA will not check the PAC file content.

A sample PAC file is provided. To use the sample file, replace I*WSVA-HOSTNAME* with the actual IWSVA host name. The sample PAC file can only be edited but cannot be deleted.

Network Configuration

Network Configuration includes the following items:

- Network Interface on page 15-20
- Web Console on page 15-20
- Remote CLI on page 15-21
- SNMP Settings on page 15-21
- Static Routes on page 15-22

Network Interface

IWSVA supports multiple network interfaces that handle HTTP traffic in the Forward Proxy mode. Server hardware usually comes with multiple network interfaces and IWSVA can be configured to use multiple network interfaces in Forward Proxy deployment.

Web Console

By default, the IWSVA console is accessed through an HTTPS connection on port 8443. For improved security, Trend Micro recommends that you use a Secure Socket Layer connection (HTTPS). Web console connection can be configured on the **Administration > Network Configuration > Web Console** screen on the Web console.

Note: The default password for the default Web console private key is "adminIWSS85". If you change the Web console from Non-SSL mode to SSL mode, certificate and private key import is not required. You can enter the default password to proceed.

In bridge mode, IWSVA uses the ports specified as follows:

- **Non-SSL mode**—access the IWSVA console using a non-secure URL, for example:

  ```
  http://<IWSVA Server IP address:port>
  ```

  - **Port number**—default is 1812; can be changed to any unused port (recognized by the firewall)
- **SSL mode**—default and recommended; choose this option to enable a secure connection to the IWSVA console
  - **SSL Certificate**—to support SSL, IWSVA needs a public key and certificate; locate the certificate you will use, and upload it to the IWSVA server
  - **SSL Password**—enter the password associated with the SSL certificate, if any.
  - **Port number**—default is 8443; enter the port on which you want to open the IWSVA console, for example:

    ```
    https://<IWSVA Server IP address:port>
    ```

Remote CLI

SSH (Secure Shell) is a network protocol that allows two network devices to exchange data in a secured connection. SSH replaces Telnet which sends data (including passwords) in clear text. IWSVA allows administrators to access the CLI from a remote location using SSH only.

Use **Administration > Network Configuration > Remote CLI** screen to configure SSH on IWSVA for remote CLI access.

- **SSH: Command line access**—Select this option to enable SSH connection for remote CLI access. Clear this check box to disable SSH service.
- **Port Number**—Type the service port number for SSH. The default port number is 22.

SNMP Settings

SNMP trap notifications are especially useful for monitoring the state of the IWSVA services—IWSVA issues a trap notifying you if a service stops unexpectedly. IWSVA supports Trap Destination network management systems using either IPv4 or IPv6 addresses. IWSVA supports SNMP agent notifications for the following events:

- HTTP, FTP, and ICAP service interruptions
- Virus pattern file, Tunnel pattern file, scan engine, and URL Filtering engine updates
- Security events
- HA events

Note: If IWSVA detects that the HTTP or FTP scanning service is down, it will try twice to restart it. If the service cannot be restarted, SNMP traps will be issued to the specified destination every 30 minutes until the service restarts.

Note: IWSVA supports SNMP version 1, version 2c, and version 3 for trap notifications.

System Information Setup

Specify all the necessary system information in the System Information section of the **Administration > Network Configuration > SNMP Settings** screen.

The community that you specify in the Community Name and Default Community fields identifies the community in which the SNMP object belongs. In SNMP, every managed object belongs to a community. This provides a minimal amount of security, because designating communities can define which SNMP agents can communicate.

Access Control Setup

Specify all the necessary access control information in the Access Control section of the **Administration > Network Configuration > SNMP Settings** screen.

The fields in this section are read-only because IWSVA sends simple status and alert messages. For the Read-Only Object Identifier (OID) field, the object ID (OID) is the code for a particular message, alert, or alarm. The "object" is the actual message, alert, or alarm.

Static Routes

Configure and deploy static route settings at **Administration > Network Configuration > Static Routes**. Both IPv4 and IPv6 address routes are supported. The Web UI accepts both IPv4 and IPv6 address formats as well.

Note: Static routes can also be added during deployment and changed using the **Administration > Deployment Wizard**.

The following provides a brief description of the options in this screen:

Add—Opens the Static Routes screen that allows you to create a new static route. You can add up to 50 static routes.

- If you bind a static route to an interface, the router setting must be in the same network segment as the interface.
- If you bind a static route to a port, the router setting must be in the same network segment as the port.

Delete—Deletes a static route from the list.

Network ID—Click a Network ID to edit settings.

Netmask—Displays the subnet mask of the router for this route.

Router—Displays the IP address of the router for this route.

Interface—Displays the interface that binds to this route.

Deployment Status—Displays whether a static route is deployed successfully.

Click **Deploy** after specifying all the required settings.

Configuring Static Routes

To configure a static route:

Enter the following:

- **Network ID**—Type the destination network or host ID.
- **Netmask**—Type the subnet mask.
- **Router**—Type the IP address of the router (the next hope) for this route.
- **Interface**—Select the interface that binds to this route. The router setting must be in the same network segment as the binding interface.

Management Console

On the **Management Console** screen, the `admin` account can add/delete login accounts. Login accounts can be configured on the **Administration > Management Console > Account Administration** screen on the Web console.

The Management Console offers the following options:

- Role-based Administration on page 15-24
- Role Management on page 15-24
- Account Administration on page 15-29
- Access Control Settings on page 15-31

Role-based Administration

Use Role-based Administration to grant and control access to the IWSVA Web console. If there are several IWSVA administrators in your organization, you can use this feature to assign specific Web console privileges to the administrators and present them with only the tools and permissions necessary to perform specific tasks. You can also control access to the agent tree by assigning them one or several domains to manage. In addition, you can grant non-administrators "view only" access to the Web console.

Each user (administrator or non-administrator) is assigned a specific role. A role defines the level of access to the web console. Users log on to the Web console using custom user accounts or Active Directory accounts.

Role-based administration involves the following tasks:

1. Define user roles. For details, see Role Management on page 15-24.
   - Configure user accounts and assign a particular role to each user account. For details, see Account Administration on page 15-29.

Role Management

Role Management allows you to add or remove roles, depending on the needs. These roles include the following:

- **Administrator**—Users have complete and unrestricted access to the system. They can read and modify any settings accessible through the console including creating, deleting, and modifying user accounts. Users with Administrator rights can log into IWSVA through an SSH connection. This is the default access for new users.
- **Auditor**—Users cannot make any configuration changes; they can view configurations, logs, and reports and can also change their own passwords.
- **Reports only**—Users can only view the System Status pages and scheduled reports. They can generate logs and real-time report queries and change their own passwords.
- **Custom roles**—These are the roles manually added with complete, read-only or no access to some or all administration domains. Users can modify or view different pages depending on the access rights assigned to their role.

For more information, see Role-based Administration on page 15-24.

Menu Item Permissions

A user role determines the web console menu items accessible to a user. A role is assigned a permission for each menu item.

Permissions determine the level of access to each menu item. The permission for a menu item can either be:

- **Full access**: Allows full access to a menu item. Users can configure all settings, perform all tasks, and view data in a menu item.
- **Read-only**: Only allows users to view settings, tasks, and data in a menu item.
- **No access**: Hides a menu item from view.

Administration Menu Items Access

The following tables list the menu items available for administrators.

TABLE 15-1. Administration Menu Items

ADMINISTRATION DOMAINS	MENU ITEMS
Status Monitoring	• System Status • Dashboard
Policy Management	• Application Control • Bandwidth Control • HTTP • FTP

TABLE 15-1. Administration Menu Items

ADMINISTRATION DOMAINS	MENU ITEMS
Logs	• Log Analysis • Log Favorites • Settings
Reports	• Reports on selected users/groups
System Administration	• Updates • Notifications • Administrations **Note:** Only users using the built-in administrator account (Admin) can access User Accounts and User Roles.

Built-in User Roles

IWSVA comes with a set of built-in user roles that you cannot modify or delete. The built-in roles are as follows:

TABLE 15-2. Administration Menu Items

ADMINISTRATION DOMAINS	DESCRIPTION
Administrator	Users have complete and unrestricted access to the system. They can read and modify any settings accessible through the console, including creating, deleting, and modifying user accounts. Administrator can use this account and password to log into the CLI. This is the default access for new users.
Auditor	Users cannot make any configuration changes; they can view configurations, logs, and reports. They can also change their passwords.
Reports only	Users can only view the Dashboard and scheduled reports. They can generate logs and real-time report queries and change their own password.

Note: Accounts that have administrator privileges can log in to the terminal console through SSH.

Custom Roles

You can create custom roles if none of the built-in roles meet your requirement. Only users with the built-in administrator role can create custom user roles and assign these roles to user accounts.

Adding a Custom Role

To add a custom role:

1. From the main menu, click **Administration** > **Management Console** > **Role Management**.
2. Click **Add**.

   A new screen appears.
3. Type a name for the role and optionally provide a description.
4. Select the access rights for each administration domain at **Role Permission**. See Administration Menu Items Access on page 15-25 for access details.
5. Click **Save**.

The new role displays on the **Roles List**.

Modifying a Custom Role

To modify a custom role:

1. From the main menu, click **Administration** > **Management Console** > **Role Management**.
2. Click the role name.

   A new screen appears.
3. Modify any of the following:
   - **Name** for the role
   - Role **Description** (optional).
   - **Role Permissions**: modify the access rights for each administration domain.
4. Click **Save**.

Deleting a Custom Role

To delete a custom role:

1. From the main menu, click **Administration** > **Management Console** > **Role Management**.
2. Select the role that you want to delete.
3. Click **Delete**.

A confirmation message pops up.

4. Click **OK**.

Account Administration

Account administration allows you to add and delete accounts. It shows all the existing accounts, giving the username, a description, and assign roles,

Login Accounts

The Login Accounts page shows all the available login accounts.

- Click **Add** to create a new login account or click a username to edit an existing one.
- To delete a login account, select the check box associated with the login account and then click **Delete**.
- **Username**—The name of the user assigned to the login account.
- **Password**—Enter and confirm a secure password.
- **Description**—The field that briefly describes the login account.
- **Role**—The role assigned to the user account. Role Management on page 15-24.

Login Accounts can be configured on the **Administration > Management Console > Account Administration** screen on the Web console.

Up to 128 users can access IWSVA using assigned access rights. When in the application, users can make configuration changes that are recorded in the audit log (see Audit Log on page 15-3).

If you have a team of security administrators who are responsible for different functions and who might also have help desk privileges, then assigning them access rights can be beneficial to your organization. To manage IWSVA, these users can have different logon credentials with different privileges.

Access rights can also give you the ability to audit what is being changed in IWSVA. If you have the need to comply with certain government agency standards, then this function can be critical.

Adding a Login Account

To add a login account:

1. From the main menu, click **Administration > Management Console > Account Administration**.
2. In the Account Administration screen, click **Add**.
3. In the **Login Accounts** page, complete the necessary information:
   - **Local Account** or **LDAP Account**—Select the account type.

     Note: If LDAP is not configured in IWSVA web console, the **LDAP Account** option is disabled.

     If you select LDAP Account, the **Username** and **Password** fields will be disabled and will use the LDAP account information instead.

   - **Username**—The name of the user assigned to the login account.
   - **Password**—Should be a mixture of alphanumeric characters between 4 and 32 characters long. Avoid dictionary words, names, and dates.
   - **Description**—The field that briefly describes the login account.
   - **Role**—Select a role from the drop-down list. See Built-in User Roles on page 15-27.
4. Click **Save**.

   The new login account appears in the **Account Administration** screen.

Changing a Login Account

To change a login account:

1. From the main menu, click **Administration > Management Console > Account Administration**.
2. Click on the desired username.
3. In the Login Accounts screen, change the necessary information:
   - **Password**—Should be a mixture of alphanumeric characters between 4 and 32 characters long. Avoid dictionary words, names, and dates.
   - **Description**—The field that briefly describes the login account.

- **Role**—Select a role from the drop-down list. See Built-in User Roles on page 15-27.

4. Click **Save**.

   The changed login account appears in the **Login Accounts** screen.

Note: If an administrator account logs into the terminal console through SSH, and does not close the session, the administrator cannot modify the account directly to "Auditor" or "Reports only." A warning message will appear.

Access Control Settings

An administrator can set the access control list (ACL) to restrict access to the management console (such as the Web console, CLI, and PING requests) or to a specific IP address or IP address range.

ACL supports both IPv4 and IPv6 addresses. You can configure a rule with a single address, an address range, or a network mask.

The management ACL is disabled by default, which allows any user to access the IWSVA management console. Administrators can add one or multiple IP addresses to the management ACL. Any IP address added to the management ACL can also be deleted individually. If the list is enabled, the administrator can only connect to the IWSVA management console from an IP address displayed on the allowed IP address list.

Note: Add the IP addresses of the central managers to which IWSVA registers (such as Trend Micro Control Manager and so on) to the access list to allow them to function properly and access the necessary data from IWSVA.

To enable and configure the access control list for the management console:

1. Go to **Administration > Management Console > Access Control Settings**.
2. Select one of the following options:
   - **IP address** - to add a single IP address to the management ACL
   - **IP range** - to add a range of IP addresses to the management ACL

- **IP mask** - to add all the IP address covered by a network segment to the management ACL

Note: No more than 20 entries can be added to the management ACL.

3. Click **Add** to add your entry to the allowed list.
4. Check the **Enable Administrative Access Based on Client IP** check box.

Note: At least one IP address must be added to the management ACL before enabling this feature. Only users from the allowed IP address list can access the management console.

5. Click **Save**.
6. To delete an entry, click the **Delete** icon on the row of the entry to be deleted and confirm the deletion by clicking **Save**.

Syslog Server

When a syslog servers has been configured, logs can be redirected to them. You can add, edit, or remove syslog servers from IWSVA.

To configure a syslog server:

1. Go to **Logs > Log Settings**.
2. Click **Add** under Syslog Server, or to edit an existing syslog server, click the **Syslog Server Name**.
3. Click **Enable Syslog**.
4. Specify the server name or IP address.
5. Specify the UDP Port.
6. Indicate the log type or priority level.
7. Click **Save**.

Config Backup/Restore

The Configuration Backup & Restore page is where you can generate an IWSVA configuration file for backup. Also from this page, the configuration and policy information for the following Trend Micro products can be migrated to IWSVA 6.5 SP2:

- IWSVA 6.5
- IWSVA 6.5 SP1
- IWSVA 6.5 SP2

IWSVA supports both full and partial migration. Use full migration to restore system and application settings or to apply current configuration to an IWSVA replacement machine. Perform a partial migration if you want to replace policy- and application-level configurations. For details about "Information Not Migrated", see *Information Not Migrated* in the *Installation Guide*.

Note: 1. To perform a full migration, make sure the deployment mode, IP address, and network card(s) are the same on the two IWSVA machines.
2. OS settings, system patch information, and pattern files will not be updated after a full or partial migration.
3. IWSVA in High Availability mode only supports partial migration.

System Updates

IWSVA does not support updates for the system, but from time to time, Trend Micro makes system updates available through the Download Center at:
http://downloadcenter.trendmicro.com/

There are two kinds of system updates:

- Application patches
- OS updates

Both are handled in the same way and can be viewed in the History section of the **Administration > System Updates** screen. Only properly formatted and encrypted Trend Micro updates can be uploaded using this utility

To install a system update:

1. Get the latest update from the Trend Micro Download Center at: `http://downloadcenter.trendmicro.com/`
2. Go to **Administration > System Updates.**
3. Click **Browse** to locate the downloaded file.
4. Click **Upload**.
5. In the summary screen, click **Install**.
6. You may navigate to another screen after you receive the successful installation message.

Note: See Applying an Application Patch or Removing an Application Patch on page 16-21 for instructions on removing an application patch.

WARNING! **Updates available from other sources should never be applied to the IWSVA server.**

Note: After updating, the IWSVA server may restart.

System Maintenance

Go to **Administration > System Maintenance** to shut down or restart the system for maintenance purposes. IWSVA records the actions performed to the audit and system event logs.

Shut down—Select this option to turn off the appliance and stop the IWSVA service.

Restart—Select this option to restart the IWSVA service or the system. The IWSVA service is unavailable while the system is restarting.

Comment—Enter a reason for the selected action you want to perform. You cannot leave this field blank. The information you enter in this field is recorded in the logs.

System Event Log

The system event log contains information about state changes or errors that occurred in the system. The following types of events are recorded:

- Active updates
- Product registration
- System maintenance

To view the system event logs:

1. Click **Administration > System Event Log** in the main menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, or Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Level(s)**, select the event level(s) for which you want to view log entries. Click **Add** (or **Add All** for all grayware listed).

   To remove an event level from the right list box, click **Remove** (or **Remove All** for all levels listed).
4. Under the **Sort by** section, select a sort option (Server, Date, Level, or Source).
5. Click **Show Log**. The **System Event Log** viewing screen opens.
6. Click **Refresh** to update the display.

Product License

The Product License function allows you to register and license IWSVA. Fully activating IWSVA is a two-step process. First, you must register IWSVA with Trend Micro. After registering, a valid IWSVA activation code (AC) will be provided to license the product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only.

To activate IWSVA, you first need a Registration Key, which you acquire during product registration. It allows you to obtain an activation code. You can activate IWSVA using the Deployment Wizard or later using the IWSVA console.

License Expiration Warning

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the upcoming discontinuances. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

https://olr.trendmicro.com/registration/

Registering IWSVA

There are several ways to register IWSVA:

- *Registering as a New Customer*
- *Registering as a Registered User*

Registering as a New Customer

To register if you are a new customer:

1. Click the Trend Micro Product Registration Server link in your product at **Administration > Deployment Wizard > Product Activation**.
2. Click **Continue**.
3. Click **New Account**, select the Region-Language, and click **Next**.
4. In the Enter Registration Key screen, use the Registration Key that came with your product (Trend Micro Enterprise Protection DVD or License Certificate) and click **Continue**.
5. Select your product type and click **Continue**.
6. Select **I Accept** and click **Submit**.
7. Type your Company name, First Name, Last Name, and email address.
8. Confirm email address, select your country/Region, then click **Submit**.
9. Verify your registration information.
    a. Click **Edit** to make any changes.
    b. Click **OK**.
10. Obtain your activation code from either the confirmation page or your email.
11. Click **OK** to finish.

Registering as a Registered User

To register if you are a registered user:

1. Click the Trend Micro Product Registration Server link in your product at **Administration > Development Wizard > Product Activation**.
2. Type your login ID and password in the fields provided, and then click **Login**.

   You will be prompted to change your password the first time you log on.
3. In the **My Products** screen, click **Add Products** and type the Registration Key.
4. To edit your company profile, click **View/Edit Company Profile**.
5. Your Activation Code appears on the next screen. To receive a copy of your Activation Code at your registered email address, click **Send Now**.

Note: For maintenance renewal, contact Trend Micro sales or your reseller. Click **Check Status Online** at **Administration > Product License** to manually update the maintenance expiration date on the Product License screen.

Obtaining a Registration Key

The Registration Key can be found on:

- Trend Micro Enterprise Solution DVD
- License Certificate (that you obtained after purchasing the product)

Registering and activating your registration key entitles you the following benefits:

- Updates to the IWSVA pattern files and scan engine
- Technical support
- Easy access in viewing the license expiration update, registration and license information

Registration Keys have 31 characters and appear as follows:

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

Obtaining and Entering an Activation Code

When the activation code expires, IWSVA security updates will be disabled. In the Product License screen, you can obtain an Activation Code online, view renewal instructions, and check the status of your product.

To activate IWSVA, you need an Activation Code. This can be done in several ways.

- You can use a Registration Key to obtain an Activation Code online.

Activation Codes have 31 characters and appear like this:

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

To obtain and enter an activation code online:

1. Open the IWSVA console and then click **Administration > Product License**.
2. Obtain an activation code by registering IWSVA (click the link at the top of the page to register and then follow the on-screen instructions).
3. Click the **Enter a new code** link.
4. When prompted, type the activation code in the Activation Code field and then click **Activate**.

Updating Your License

To obtain the latest license through the Web, go to **Administration > Product License** and click **Check Online Status**.

For more renewal instructions, see:
https://olr.trendmicro.com/registration/us/en-us/instruction_renew.aspx

Renewing a Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If your Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

- To purchase renewal maintenance, contact the same vendor from whom you purchased the product. A Maintenance Agreement, extending your protection for a year, will be sent by post to the primary company contact listed in your company's Registration Profile.
- To view or modify your company's Registration Profile, log in to the account at the Trend Micro online registration Web site:

  https://olr.trendmicro.com/registration/us/en-us

Support

Using the case diagnostic tool (CDT), IWSVA generates core and/or system file(s) containing the system data held in memory when a process abnormally terminates. The Generate System Information File button is an extension of this feature, allowing you to package the current machine "state" at the click of a button.

The core and/or system file(s) that IWSVA generates contains the following information:

- **IWSVA information**—Includes the IWSVA product version, engine version, build number, and IWSVA hot fixes and service pack information. Product and integration settings are also part of this information
- **IWSVA/system logs**—Includes the IWSVA logs and debug logs, logs generated by syslogd daemon (if system logs are enabled), and core dump file
- **System/network information**—Includes the hardware configuration, operating system, build, system resource status, other applications installed, and network information
- **CDT-compliant configuration/plugins information**—Includes information about changes made to the CDT as a result of IWSVA adding a new component, such as a TMCM or MCP agent.
- **Verbose Logging** - Create verbose logs with IP-filtering.

Network Packet Capturing

The Network Packet Capturing wizard is located on the Administration > Support | Network Packet Capturing tab. Using the captured network packet, administrators or support teams can perform traffic debug or analysis.

With this feature, administrators can choose a single or multiple network interfaces on which to simultaneously capture network packet. After the capture starts, the elapsed time displays. The capture operation stops when the administrator clicks Stop capturing or when the (default) maximum file size of 10GB is reached.

Note: The default maximum file size limitation is configured in `/etc/iscan/network.ini`.

The packet capture for each interface will be save in an individual file using the naming convention of "capture-{interface}-{date:time}.pcap". For example capture-eth0-20111101:31:31:01.pcap would be the file name for the packet capture on the eth0 network interface performed on November 1, 2011.

After the network packet capture completes, all packet capture files are saved in one compressed package file named to "capture-{date}.tgz". This file displays in the downloadable list. Administrators can either download or deleted the compressed file.

Using Network Packet Capturing

Administrators can analyze traffic with this feature that allows packet captures for selected interfaces or a single interface.

To capture network packets:

1. Go to the **Administration > Support** page and click the **Network Packet Capturing** tab.
2. Select the appropriate interface(s) from the **Available** column.
3. Click **Add** or **Add All** to move the selected interfaces to the Selected column.
4. If needed, click **Remove** or **Remove All** to remove interfaces from the Selected column.
5. Click **Start Capturing**. The elapsed time displays. The capture stops when the maximum files size of 10GB is reached.
6. If necessary, click **Stop Capturing** to stop the packet capture before reaching the maximum file size.
7. When the capture finishes, select the appropriate generate file or select All.
8. Select an action:
   - Click **Download** and browse to save the capture file to a directory.

- Click **Delete** to delete the generated files and click **OK**.

Verbose Log

Verbose logging tracks all changes and settings applied using a group policy and its extension to the local computer and to users who log on to the computer. Enabling verbose logging involves adding the registry key for verbose logging.

To enable verbose logging:

1. Enter the IP address or IP range you would like to track with verbose logging.
2. Add the entry or entries to the Selected box.
3. Click **Start Capturing**.
4. Select one of the generated verbose log types to download.
5. Choose to clean (delete) the log or download it to your computer for further evaluation.

Deployment Diagnostic

Use Deployment Diagnostic files when working with Trend Micro technical support to help you diagnose the causes of your deployment problems.

While IWSVA generates system file(s), the application could encounter some conditions that prevent it from gathering all the possible diagnostic information. IWSVA gathers as much information as possible and also records any errors encountered in a log file with comprehensive messages that you can delete or download to you computer for further evaluation.

Chapter 16

Testing and Configuring IWSVA

After opening the InterScan Web Security Virtual Appliance (IWSVA) console, test the following to verify that the program is working properly. The following lists the tests described in this chapter:

EICAR Test File

The European Institute for Computer Antivirus Research (EICAR) has developed a test virus to test your antivirus appliance. This script is an inert text file. The binary pattern is included in the virus pattern file from most antivirus vendors. The test virus is not a virus and does not contain any program code.

WARNING! Never use real viruses to test your Internet security.

Download the EICAR test virus from the following URLs:

http://www.eicar.org/85-0-Download.html

https://secure.eicar.org/eicar.com

Alternatively, you can create your own EICAR test virus by typing or copying the following into a text file, and then naming the file eicar.com:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
$H+H*
```

Note: Flush the URL cache (**HTTP** > **Configuration** > **WRS/URL Cache**), the Content Cache (**HTTP > Configuration > Content Cache**), and your local browser before testing. If either cache contains a copy of the test virus, it is possible an attempt to download the file would get the file from the cache, rather than getting it from the Internet, and IWSVA would not detect the file.

Testing Web Reputation

To test IWSVA's Web Reputation feature, open a Web browser and type the following in the address field:

```
http://wrs21.winshipway.com
```

If the test is successful, you should receive an IWSVA Security Event message stating, "This URL has a Web security rating that prohibits it from being accessed."

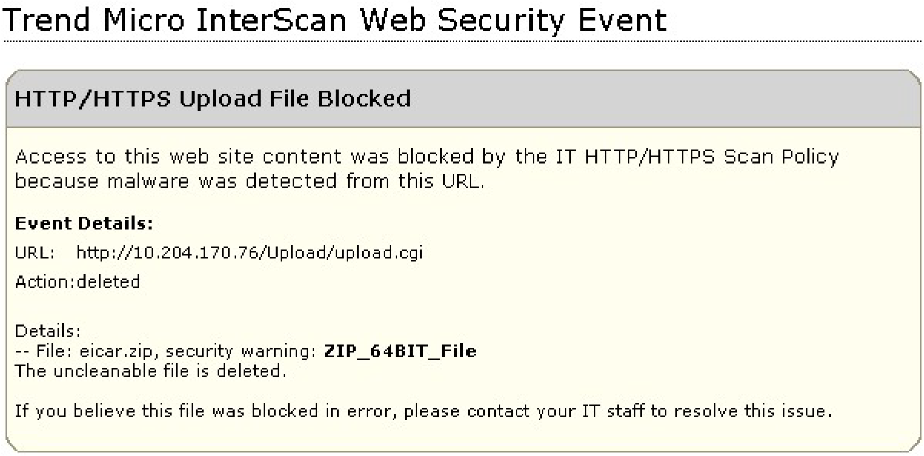
Testing Upload Scanning

The following procedure contains instructions to test the uploaded virus:

1. Open the IWSVA console and click **HTTP > Advanced Threat Protection > Policies** in the main menu. Clear **Enable virus scanning**, and then click **Save**.
2. Download the test virus (eicar.com) from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`

3. Save the test virus on your local machine.
4. Re-open the IWSVA console, under **HTTP > Advanced Threat Protection > Policies** in the main menu, select **Enable virus scanning**, and then click **Save**.
5. Upload the test virus to a Web site. A message similar to *Figure 16-1* appears in your browser.



Trend Micro InterScan Web Security Event

HTTP/HTTPS Upload File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPS Scan Policy because malware was detected from this URL.

Event Details:

URL: http://10.204.170.76/Upload/upload.cgi

Action:deleted

Details:
-- File: eicar.zip, security warning: **ZIP_64BIT_File**
The uncleanable file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

FIGURE 16-1. This warning screen shows the detection of an EICAR test virus.

Testing HTTPS Decryption Scanning

This section describes the procedure to test HTTPS decryption on IWSVA in stand-alone mode.

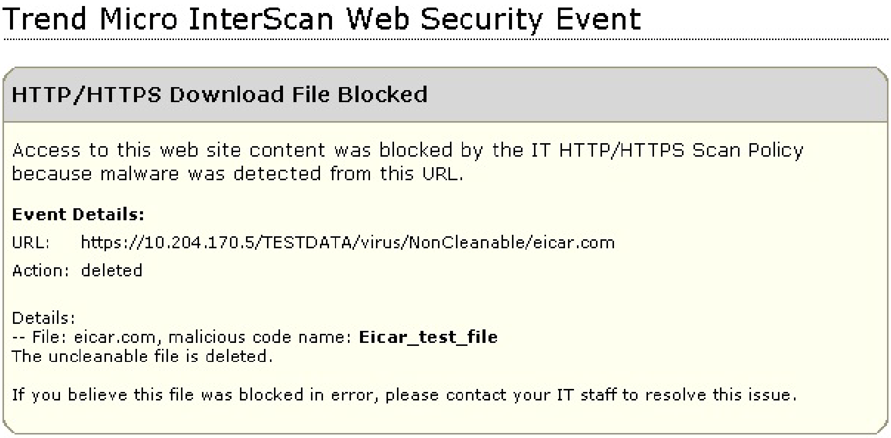
To test virus scanning of decrypted HTTPS traffic:

1. Set the Web client's HTTP proxy to point to IWSVA (for example, open Internet Explorer and click **Tools > Internet Options > Connections > LAN Settings > Use a proxy server**).
2. Open the IWSVA Web console and click **HTTP > HTTPS Decryption > Settings | Server Certificate Validation** and make sure all options are selected.
3. Click **HTTP > HTTPS Decryption > Policies** and select **Enable HTTPS Decryption**.
4. Click **Add** to create a new HTTPS decryption policy. In the Rules tab, select **Disease Vector** under Internet Security.
5. From the client machine, access the test virus file from the following URL:

   ```
   https://secure.eicar.org/eicar.com
   ```

6. Because the server certificate is not in the trusted list on IWSVA, a certificate error notification displays. Click **Visit site anyway**.

7. A security warning screen displays. The warning message varies depending on whether URL filtering is also enabled or not.



Trend Micro InterScan Web Security Event

HTTP/HTTPS Download File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPS Scan Policy because malware was detected from this URL.

Event Details:

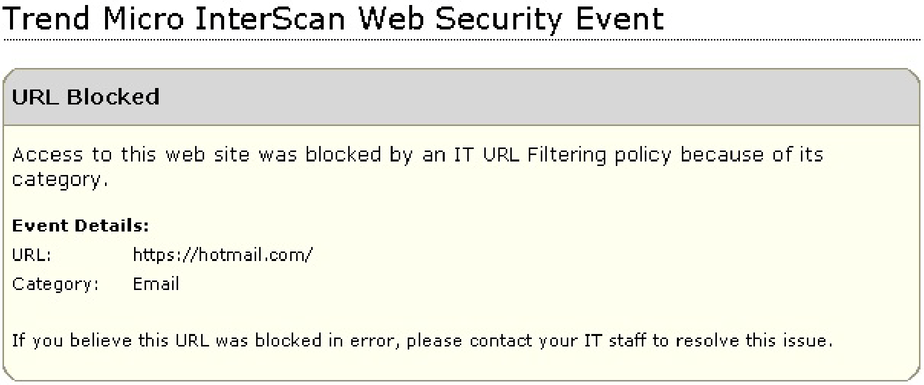
URL: https://10.204.170.5/TESTDATA/virus/NonCleanable/eicar.com

Action: deleted

Details:
-- File: eicar.com, malicious code name: **Eicar_test_file**
The uncleanable file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

FIGURE 16-2. Security warning screen if URL filtering is disabled



Trend Micro InterScan Web Security Event

URL Blocked

Access to this web site was blocked by an IT URL Filtering policy because of its category.

Event Details:

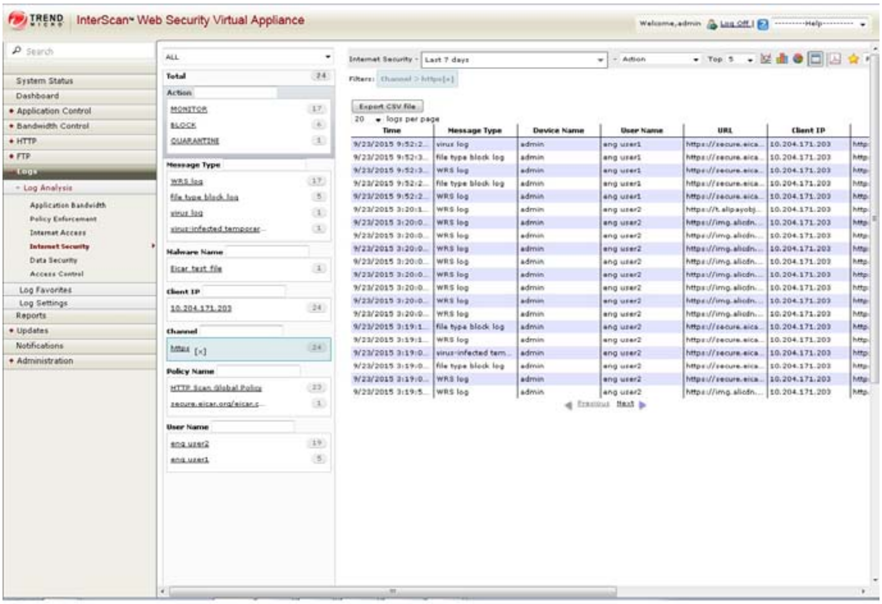
URL: https://hotmail.com/

Category: Email

If you believe this URL was blocked in error, please contact your IT staff to resolve this issue.

FIGURE 16-3. Security warning screen if URL filtering is also enabled

On the IWSVA server, you can view detailed log information in the Internet Security log by selecting the View Detailed Logs icon from the options on the top button bar.



ALL

Total 24

Action
MONITOR 17
BLOCK 6
QUARANTINE 1

Message Type
WRS log 17
file type block log 5
virus log 1
virus-infected temporar... 1

Malware Name
Eicar test file 1

Client IP
10.204.171.203 24

Channel
https [x] 24

Policy Name
HTTP Scan Global Policy 23
secure.eicar.org/eicar.c... 1

User Name
eng user2 19
eng user1 5

Internet Security - Last 7 days - Action Top 5

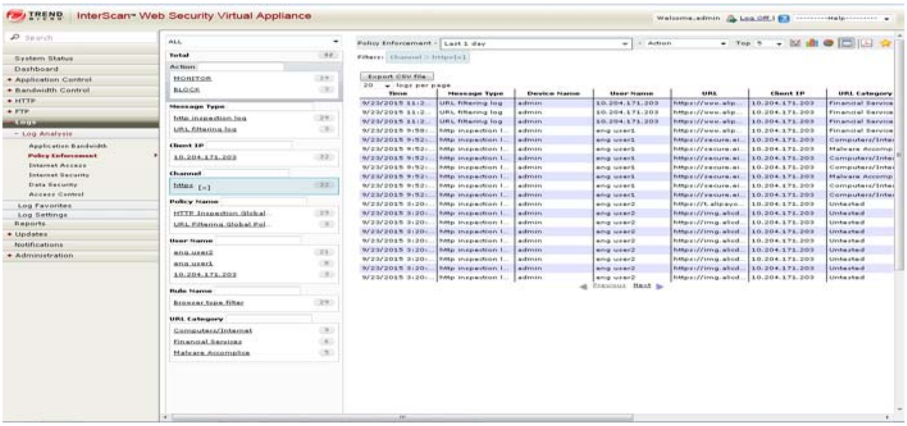
Filters: Channel > https[x]

20 logs per page

Time	Message Type	Device Name	User Name	URL	Client IP	
9/23/2015 9:52:2...	virus log	admin	eng user1	https://secure.eica...	10.204.171.203	http
9/23/2015 9:52:3...	file type block log	admin	eng user1	https://secure.eica...	10.204.171.203	http
9/23/2015 9:52:3...	WRS log	admin	eng user1	https://secure.eica...	10.204.171.203	http
9/23/2015 9:52:2...	file type block log	admin	eng user1	https://secure.eica...	10.204.171.203	http
9/23/2015 9:52:2...	WRS log	admin	eng user1	https://secure.eica...	10.204.171.203	http
9/23/2015 3:20:1...	WRS log	admin	eng user2	https://t.alipayobj...	10.204.171.203	http
9/23/2015 3:20:0...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http
9/23/2015 3:20:0...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http
9/23/2015 3:20:0...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http
9/23/2015 3:20:0...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http
9/23/2015 3:20:0...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http
9/23/2015 3:20:0...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http
9/23/2015 3:20:0...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http
9/23/2015 3:20:0...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http
9/23/2015 3:19:1...	file type block log	admin	eng user2	https://secure.eica...	10.204.171.203	http
9/23/2015 3:19:1...	WRS log	admin	eng user2	https://secure.eica...	10.204.171.203	http
9/23/2015 3:19:0...	virus-infected tem...	admin	eng user2	https://secure.eica...	10.204.171.203	http
9/23/2015 3:19:0...	file type block log	admin	eng user2	https://secure.eica...	10.204.171.203	http
9/23/2015 3:19:0...	WRS log	admin	eng user2	https://secure.eica...	10.204.171.203	http
9/23/2015 3:19:5...	WRS log	admin	eng user2	https://img.alicdn....	10.204.171.203	http

FIGURE 16-4. View the log for HTTPS decryption test in the Internet Security log screen if URL filtering is disabled

.



ALL

Total 32

Action
- MONITOR 29
- BLOCK 3

Message Type
- http inspection log 29
- URL filtering log 3

Client IP
- 10.204.171.203 32

Channel
- https [×] 32

Policy Name
- HTTP Inspection Global 29
- URL Filtering Global Pol 3

User Name
- eng user2 21
- eng user1 8
- 10.204.171.203 3

Rule Name
- browser type filter 29

URL Category
- Computers/Internet 9
- Financial Services 6
- Malware Accomplice 5

Policy Enforcement · Last 1 day · Action · Top 5

Filters: Channel = https[×]

Export CSV file

20 logs per page

Time	Message Type	Device Name	User Name	URL	Client IP	URL Category
9/23/2015 11:2...	URL filtering log	admin	10.204.171.203	https://www.alip...	10.204.171.203	Financial Service
9/23/2015 11:2...	URL filtering log	admin	10.204.171.203	https://www.alip...	10.204.171.203	Financial Service
9/23/2015 11:2...	URL filtering log	admin	10.204.171.203	https://www.alip...	10.204.171.203	Financial Service
9/23/2015 9:58:...	http inspection l...	admin	eng user1	https://www.alip...	10.204.171.203	Financial Service
9/23/2015 9:52:...	http inspection l...	admin	eng user1	https://secure.al...	10.204.171.203	Computers/Inte
9/23/2015 9:52:...	http inspection l...	admin	eng user1	https://secure.al...	10.204.171.203	Malware Accomp
9/23/2015 9:52:...	http inspection l...	admin	eng user1	https://secure.al...	10.204.171.203	Computers/Inte
9/23/2015 9:52:...	http inspection l...	admin	eng user1	https://secure.al...	10.204.171.203	Computers/Inte
9/23/2015 9:52:...	http inspection l...	admin	eng user1	https://secure.al...	10.204.171.203	Malware Accomp
9/23/2015 9:52:...	http inspection l...	admin	eng user1	https://secure.al...	10.204.171.203	Computers/Inte
9/23/2015 9:52:...	http inspection l...	admin	eng user1	https://secure.al...	10.204.171.203	Computers/Inte
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://t.alipayo...	10.204.171.203	Untested
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://img.alicd...	10.204.171.203	Untested
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://img.alicd...	10.204.171.203	Untested
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://img.alicd...	10.204.171.203	Untested
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://img.alicd...	10.204.171.203	Untested
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://img.alicd...	10.204.171.203	Untested
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://img.alicd...	10.204.171.203	Untested
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://img.alicd...	10.204.171.203	Untested
9/23/2015 3:20:...	http inspection l...	admin	eng user2	https://img.alicd...	10.204.171.203	Untested

◀ Previous Next ▶

FIGURE 16-5. View the log for HTTPS decryption test in the Policy Enforcement log screen if URL filtering is enabled

Testing FTP Scanning

The following procedure contains instructions to test your FTP virus scanning capability in standalone mode.

To test virus scanning of FTP traffic:

1. Download the test virus from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`

2. Access the FTP server through IWSVA with it working as the FTP proxy.

   For example, assume the following IP addresses: IWSVA FTP proxy server (`10.2.203.126`), FTP server (`10.2.202.168`).

   Open a command line prompt and type the following:

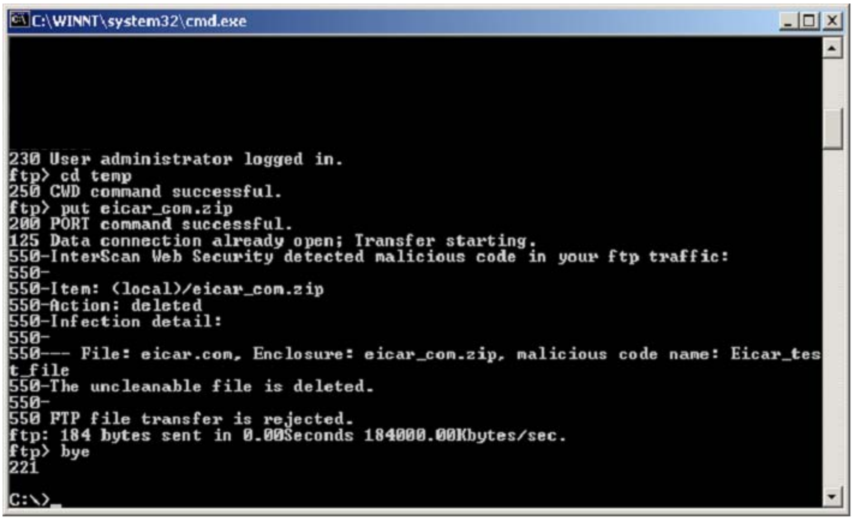
   ```
   ftp 10.2.203.126
   ```

3. Log on as `user@host`. For example, if your FTP account name is anonymous and the IP address of the FTP server is `10.2.202.168`, then log on as `anonymous@10.2.202.168`

4. Upload the test virus (for example, eicar_com.zip) by typing the following command:

   ```
   put eicar_com.zip
   ```

5. If you have configured the IWSVA FTP proxy mode correctly, IWSVA displays a message similar to the one in *Figure 16-6*.



```
230 User administrator logged in.
ftp> cd temp
250 CWD command successful.
ftp> put eicar_com.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
550-InterScan Web Security detected malicious code in your ftp traffic:
550-
550-Item: (local)/eicar_com.zip
550-Action: deleted
550-Infection detail:
550-
550--- File: eicar.com, Enclosure: eicar_com.zip, malicious code name: Eicar_tes
t_file
550-The uncleanable file is deleted.
550-
550 FTP file transfer is rejected.
ftp: 184 bytes sent in 0.00Seconds 184000.00Kbytes/sec.
ftp> bye
221

C:\>_
```

FIGURE 16-6. Warning message that shows the detection of a virus in eicar_com.zip.

Testing Application Control

IWSVA must be deployed in Forward Proxy Mode, Transparent Bridge Mode, or Transparent Bridge Mode-High Availability to use the Application Control feature.

The following procedure allows you to modify the Application Control Global Policy to block end users from accessing the Google website.

To test Application Control:

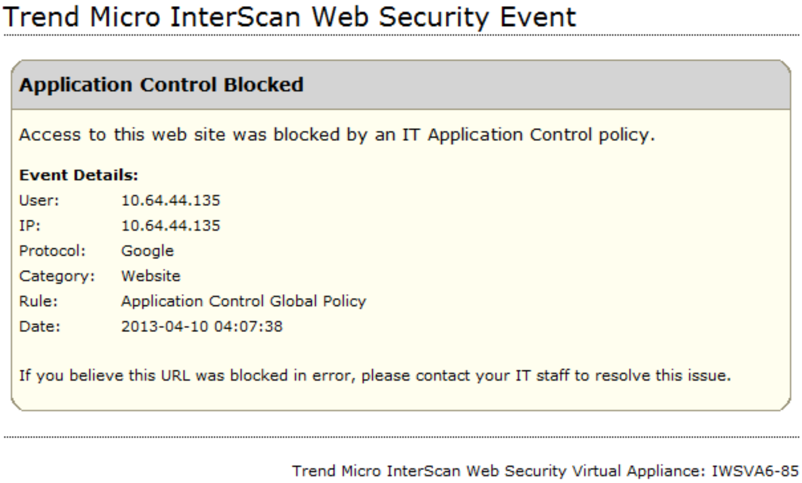
1. Open the IWSVA console and go to **Application Control > Policies**.
2. Check the **Enable Application Control** check box and click **Save**.

3. Click the **Application Control Global Policy** name to modify it.
4. Search for Google protocol listings in one of two ways:
   a. Type "Google" in the **Application Search** field and click **Search** button.

      Search result appear listing "Google" in the Web category.

   b. Scroll down to the Web category, expand the category, and find the entry for Google.
5. Select the **Block** action from the drop-down action menu in the column on the right side of the Website category name.
6. Select one of the objects in scheduled times under "Scheduling."
7. Click **Apply**.
8. Click **Save** and you return to the Application Control Policies page.
9. Click **Deploy Policies** to deploy the updated policy.
10. Open your browser and attempt to access http://www.google.com.

    Your browser displays a notification message confirming an Application Control policy breach.



Trend Micro InterScan Web Security Event

Application Control Blocked

Access to this web site was blocked by an IT Application Control policy.

Event Details:

```
User:       10.64.44.135
IP:         10.64.44.135
Protocol:   Google
Category:   Website
Rule:       Application Control Global Policy
Date:       2013-04-10 04:07:38
```

If you believe this URL was blocked in error, please contact your IT staff to resolve this issue.

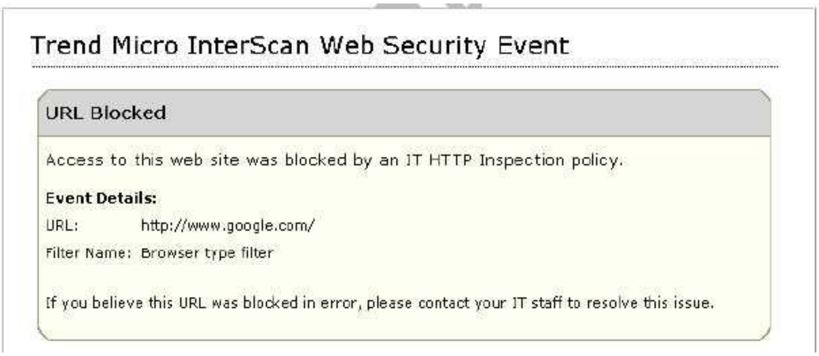
Trend Micro InterScan Web Security Virtual Appliance: IWSVA6-85

Testing HTTP Inspection

Use this procedure to test the HTTP Inspection browser-type filter which identifies requests sent from a FireFox browser according.

To test HTTP Inspection:

1. Open the IWSVA console and go to **HTTP > HTTP Inspection > Policies**.
2. Check the **Enable HTTP Inspection** check box and click **Save**.
3. Click the **HTTP Inspection Global Policy** name to access the policy for modification.
4. Select the **Block** action from the drop-down action menu above the list of HTTP Inspection filters.
5. Select one of the objects in scheduled times under “Scheduling.”
6. Click **Apply**.
7. Click **Save** and you return to the HTTP Inspection Policies page.
8. Click **Deploy Policies** to deploy the updated policy.
9. Attempt to access an http:// URL, such as http://www.google.com, with your FireFox browser. Your browser displays the notification message in *Figure 16-7*.



Trend Micro InterScan Web Security Event

URL Blocked

Access to this web site was blocked by an IT HTTP Inspection policy.

Event Details:

URL: http://www.google.com/

Filter Name: Browser type filter

If you believe this URL was blocked in error, please contact your IT staff to resolve this issue.

FIGURE 16-7. HTTP Inspection Policy Breach Notification

Testing URL Monitoring

Before testing the monitor feature in URL filtering, require users to set the Web client's HTTP proxy to point to IWSVA.

To test URL filtering:

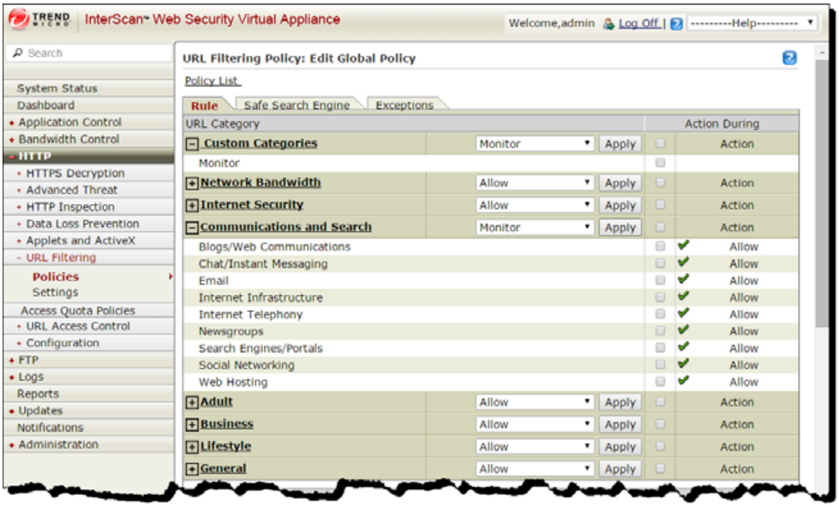
1. Open the IWSVA Web console and click **HTTP > Configuration > Custom Categories** and create a new category **"monitor"** for the following URL:

   `http://www.download.com`

2. Click **HTTP > URL Filtering > Policies** and select **Enable URL Filtering**; then, click the **URL Filtering Global Policy** name to access the policy for editing it.
3. Select one of the objects in scheduled times under "Scheduling."

Note: Create a time object under **Administration > IWSVA Configuration > Scheduled Times**.

4. Select **Monitor** and click the check box under Action for **Blogs/Web Communications/Search Engines/Portals**; then, click **Apply**.



URL Filtering Policy: Edit Global Policy

URL Category			Action During	
⊟ Custom Categories	Monitor	Apply	□	Action
Monitor			□	
⊞ Network Bandwidth	Allow	Apply	□	Action
⊞ Internet Security	Allow	Apply	□	Action
⊟ Communications and Search	Monitor	Apply	□	Action
Blogs/Web Communications			□	✓ Allow
Chat/Instant Messaging			□	✓ Allow
Email			□	✓ Allow
Internet Infrastructure			□	✓ Allow
Internet Telephony			□	✓ Allow
Newsgroups			□	✓ Allow
Search Engines/Portals			□	✓ Allow
Social Networking			□	✓ Allow
Web Hosting			□	✓ Allow
⊞ Adult	Allow	Apply	□	Action
⊞ Business	Allow	Apply	□	Action
⊞ Lifestyle	Allow	Apply	□	Action
⊞ General	Allow	Apply	□	Action

FIGURE 16-8. Rule screen configuration for URL monitor testing

5. Save and deploy this policy.
6. From a client computer, access the following Web sites during a time you have not selected as the time object:

   `http://www.download.com`

   `http://www.google.com`

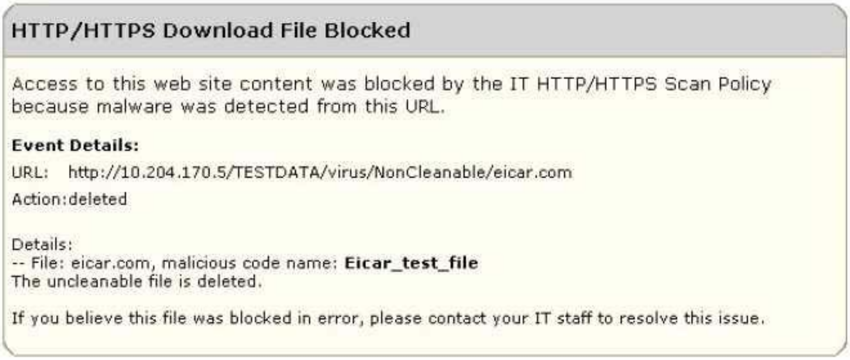
   `http://www.yahoo.com`

You should be able to access the Web sites without seeing any warning messages. To query and view URL filtering log, access the IWSVA Web console and click **Logs > Log Analysis > Internet Security**.

Testing Download Scanning

To test virus scanning when downloading using HTTP or FTP over HTTP, attempt to download the test virus from the following Web site:

`http://www.eicar.org/anti_virus_test_file.htm`



HTTP/HTTPS Download File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPS Scan Policy because malware was detected from this URL.

Event Details:

URL: http://10.204.170.5/TESTDATA/virus/NonCleanable/eicar.com

Action:deleted

Details:
-- File: eicar.com, malicious code name: **Eicar_test_file**
The uncleanable file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

FIGURE 16-9. This virus-warning screen opens if the system is set up properly.

If a client attempts to download an infected file, IWSVA blocks all other users' access to that site for four hours by default. When other clients subsequently attempt to access the same URL that contained the virus, they will see a URL blocking message instead of the virus-warning message.

To configure the default block time (in hours), change the parameter `infected_url_block_length` under the `[Scan-configuration]` section of `/etc/iscan/intscan.ini` file, and execute `/etc/iscan/S99ISproxy stop` and `/etc/iscan/S99ISproxy start` to restart the service.

To disable auto URL block, change the parameter `disable_infected_url_block` under the `[Scan-configuration]` section of `/etc/iscan/intscan.ini` file, and execute `/etc/iscan/S99ISproxy stop` and `/etc/iscan/S99ISproxy start` to restart the service.

About `disable_infected_url_block` parameter

`no`: Enables auto URL blocking

`yes`: Disables auto URL blocking

Note: Trend Micro does not recommend disabling this feature, because it decreases the security level.

Testing URL Filtering

Trend Micro recommends that you use the default settings to test URL filtering.

To test URL Filtering:

1. Click **HTTP > URL Filtering > Settings** from the main menu. Configure the work days and times.
2. Click **HTTP > URL Filtering > Policies** from the Main menu.
3. Select **Enable URL filtering** and then click **Save**.
4. Click **URL Filtering Global Policy** and select the Block action to apply to the categories that you want blocked during the time you selected.

   Keep the default settings in the Safe Search and Exception tabs.
5. Click **Save** to save any changes. Click **Deploy Policies** to make the policy effective immediately.

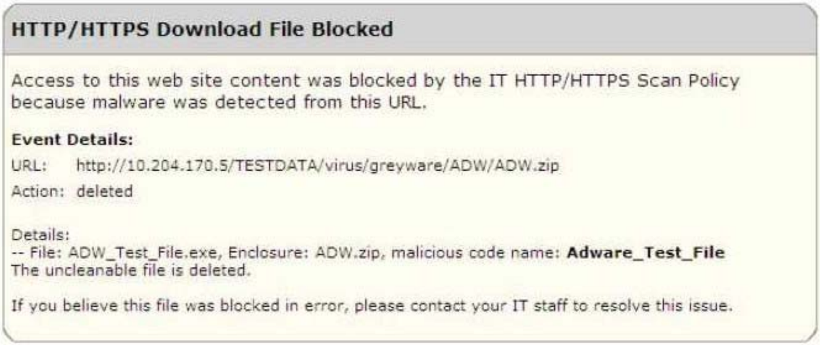
6. Open a browser and access any site that is in a category to be blocked at the time of the test. IWSVA blocks access to URLs belonging to the category that is set to be blocked.

Testing Spyware Scanning

To test spyware scanning:

1. Click **HTTP > Advanced Threat Protection > Policies**.
2. Click **Virus Scan Global Policy**.
3. Click the **Spyware/Grayware Scan Rule** tab and then select the types of spyware/grayware that should be scanned.
4. Click **Save**.
5. Click **Virus Scan Global Policy**.
6. Click the **Action** tab.
7. Under the **Uncleanable files** field, select the action setting (Delete, Quarantine, or Pass).
8. Click **Save**.
9. Click **Deploy Policies** to make the policy effective immediately.

   After a successful spyware detection, a sample message appears:



HTTP/HTTPS Download File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPS Scan Policy because malware was detected from this URL.

Event Details:

URL: http://10.204.170.5/TESTDATA/virus/greyware/ADW/ADW.zip

Action: deleted

Details:
-- File: ADW_Test_File.exe, Enclosure: ADW.zip, malicious code name: **Adware_Test_File**
The uncleanable file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

FIGURE 16-10. A sample message after detecting a spyware with action "Delete" setting

Testing Java Applet and ActiveX Scanning

Java applets and ActiveX controls are used on many Web pages to display interactive content or applications. One way to test IWSVA is to temporarily configure the global policy to block all applets and ActiveX controls, and then attempt to open Web pages that use them (to verify that the applet or object is blocked).

To test Java applet and ActiveX scanning:

1. Click **HTTP > Applets and ActiveX > Policies** from the main menu.
2. If necessary, select **Enable Applet/ActiveX security** and click **Save**.
3. Click **Applet/ActiveX Security Global Policy**.
4. On the **Java Applet Security Rules** tab, click **Block all Java applets** and then **Save**.
5. On the **ActiveX Security Rules** tab, click **Block all cabinet files** and **Block all PE format files** and then click **Save**.
6. From the **Applets and ActiveX Policies** screen, select **Deploy Policies** to make policy changes effective immediately.
7. Open a Web browser and attempt to navigate to Web sites that use Java applets and ActiveX controls, for example, for stock price tickers or games.

   IWSVA blocks the mobile code from downloading and running in your browser.

Note: Blocking all Java applets and ActiveX controls might be too restrictive for your environment because it prevents many legitimate Web sites from functioning properly. After testing, Trend Micro recommends going back to the **Applets and ActiveX Policy: Edit Global Policy** screen to change the settings back to the default or your own less-restrictive configuration.

Additional IWSVA Configurations

This section briefly introduces some common IWSVA configuration tasks.

Configuring the Separate Management Interface

In many large enterprises and/or secure networking environments, a separate network segment (also known as the management network) can be used to manage various network devices. For security reasons, the management network is not connected to the Internet and is a separate network that ordinary users are not allowed to access.

On the IWSVA server, you can enable the separate management interface that connects to the company's management network. A separate network interface must be available on the IWSVA server for the dedicate management interface. After the management interface is activated and configured on IWSVA, you can access the IWSVA Web console or CLI through the separate management interface. The following shows an example network topology:

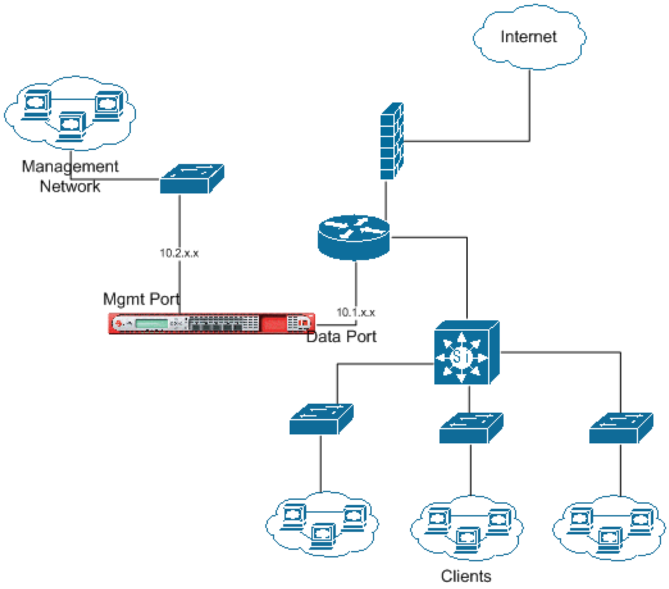


FIGURE 16-11. IWSVA management interface placement in the network

In this example, the management interface on the IWSVA is connected to the management network in the company. The clients access the Internet through the data (bridge or proxy) interface.

WARNING! **Do not configure the data (bridge/proxy) interface and the management interface in the same network environment.**

To configure the separate management interface:

1. From the main menu, click the **Administration > Network Configuration > Network Interface** page and check the **Enable Management Interface** check box.
2. From the **Ethernet interface** drop-down list, select a desired interface for the management interface.
3. Configure the IP address settings.
4. Select **Enable PING** if you want IWSVA to respond to PING requests on this interface.
5. Click **Save**. You can access the separate management interface to log into the Web console and manage IWSVA.

Tip: If the IWSVA machine is behind a router/switch in the management network, configure a static route on the management interface to access IWSVA through the Web console or SSH.

To test the separate management interface:

1. First try to log on to the Web console through the data (bridge or proxy) interface. You should be able to log on and manage IWSVA.
2. Next try accessing the Web console on the separate management interface. You should be able to log on and manage IWSVA.

Activating Remote CLI

You can enable the remote CLI feature to connect to the IWSVA server and configure settings using the CLI commands. Remote connection is secured through SSH v2 (Secure SHell) which is a network protocol that allows two network devices to exchange data in a secured connection. SSH replaces Telnet which sends data (including passwords) in clear text.

To enable remote CLI on the IWSVA server:

1. From the main menu, click **Administration > Network Configuration > Remote CLI** and choose **SSH: Command line access** to enable remote CLI access using SSH on IWSVA.
2. Type the service port number for SSH v2. The default port number is 22.
3. Click **Save**.

Specifying Advanced Threat Protection Scans

Advanced Threat Protection scanning is enabled by default. The HTTP traffic flow for clients to browse the Web and perform other HTTP operations can be enabled or disabled (see Enabling the HTTP/HTTPS Traffic Flow on page 7-2).

Specifying the User Identification Method

IWSVA supports several methods to identify clients when configuring a policy's scope (see Configuring the User Identification Method on page 8-6). The default identification method is through the client's IP address. IWSVA also supports identifying clients through their host names or MAC addresses and through their LDAP directories.

Enabling the Guest Account (LDAP only)

When using the **User/group name authentication** identification method, HTTPS decryption, HTTP virus scanning, HTTP Inspection, Data Loss Prevention, Java applets and ActiveX security, URL Filtering, and access quota policies will support configuring policies for users who are temporarily visiting your network. The guest account is disabled by default—enable it to allow guests accounts to access the Internet. To enable the guest account, IWSVA needs to be configured for User/Group name authentication (LDAP).

To enable guest accounts:

1. To enable the guest account, go to **Administration > IWSVA Configuration < User Identification tab.**
2. In the **Authentication Method** section, select **Captive Portal**, check **Allow Guest Login**, and click **Save**.

Reviewing Scanning and Filtering Policies

IWSVA is pre-configured to provide a baseline level of gateway security. Trend Micro recommends reviewing the HTTP virus scanning Global and Guest policy configurations to ensure they reflect your organization's security policies.

Additionally, if you are running the Applets and ActiveX security, URL filtering and FTP scanning modules, review those configurations and modify them accordingly.

Enabling Access Quota Policies

To limit bandwidth consumption, enable the access quota control to set a maximum amount of data that a client can retrieve or download during a given time period.

To enable access quota control:

1. Click **HTTP > Access Quota Policies** on the main menu.
2. Select **Enable access quota control**.
3. To configure access quota control for your network's guest users, click **Access Quota Policies** and configure the settings. To configure access quota control for other network users, click **Add** and configure a new policy.
4. Click **Save**.

   For the new policy to take effect immediately, click **Deploy Policies** in the **HTTP > Access Quota Policies** page.

Setting Internet Access Control Settings

The default IWSVA settings allow all non-guest clients to access the Internet. To allow a subset of your clients Internet access, configure their IP addresses on the **Access Control Settings** screen.

In addition, IWSVA can be configured to exempt some servers from scanning to speed up browsing performance when visiting trusted sites. For example, consider adding the IP address ranges of your intranet sites to the Approved Server IP list to exempt frequently visited sites from scanning and filtering.

To configure which clients are allowed to access the Internet:

1. Click **HTTP > Configuration > Access Control Settings** from the main menu.
2. On the **Client IP** tab, select **Enable HTTP Access Based On Client IP** and enter the IP/Hostname addresses that are allowed to access the Internet.
3. Enter a short description.
4. Click **Add**.
5. Click **Save**.

To configure which servers are exempt from filtering and scanning:

1. Click **HTTP > Configuration > Access Control Settings** from the main menu.
2. Click the **Approved Server IP List** tab, configure the IP addresses of servers that are exempt from HTTP scanning, URL filtering, and URL blocking.
3. Enter a short description.

4. Click **Add**.
5. Click **Save**.

Applying an Application Patch or Removing an Application Patch

From time to time, Trend Micro makes updates available through the Download Center. After downloading the latest update from the Download Center to a desktop or other computer, you can upload it to the IWSVA device where it is automatically installed.

To apply an application patch:

1. Download the latest update from http://downloadcenter.trendmicro.com
2. From the main menu, click **Administration > System Updates** and then click **Browse**.
3. Locate the update you downloaded from the Trend Micro Download Center.
4. Click **Upload** to have IWSVA copy the update to the IWSVA device and begin installing.

   Only a properly formatted and encrypted Trend Micro patch can be uploaded from this utility.

To remove an application patch:

1. From the main menu, click **Administration > System Updates**.
2. In the History section, click the **Application Patches** tab.
3. Click the **Uninstall** link beside the application patch number.
4. In the preview page that appears, verify the version of the patch you want to remove.

   You can remove the most recently installed application patch at any time.
5. Click **Uninstall**. A progress page appears. After the patch has been removed, close the window to return to the main IWSVA console.

About Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches, and service packs to address issues, enhance product performance, or add new features.

The following is a summary of the items Trend Micro might release:

- **Hot fix**: A workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore, not released to all customers. Windows hot fixes include a setup program.
- **Security Patch**: A hot fix focusing on security issues that is suitable for deployment to all customers.
- **Patch**: A group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis.
- **Service Pack**: A consolidation of hot fixes, patches, and feature enhancements significant enough to be considered a product upgrade. You can obtain hot fixes from your Technical Account Manager. Check the Trend Micro Knowledge Base to search for released hot fixes:

  - http://esupport.trendmicro.com/support/

  Check the Trend Micro Web site regularly to download patches and service packs:

  - http://www.trendmicro.com/download

  All releases include a readme file with the information you need to install, deploy, and configure your product. Read the readme file carefully before installing the hot fix, patch, or service pack file(s).

Checking the Database Connection

To check the database connection settings:

1. Click **Administration > IWSVA Configuration > Database Connection**.
2. Under **Policy Database Connection Settings**, view the database settings.
3. Click **Test Database Connection**.

Policy settings are stored in the database, and IWSVA copies the settings to a memory cache. IWSVA reloads the settings from the database into memory according to the Policy Deployment Settings (in minutes) option that specifies the interval.

To configure the Policy Deployment Settings (in minutes):

1. Open the IWSVA Web console and click **Administration > IWSVA Configuration > Policy Deployment**.
2. Under **Policy Deployment Settings (in minutes)**, type a value for the following parameters:

- Virus scan policy
- HTTPS policy
- Applet and ActiveX policy
- HTTP inspection policy
- URL filtering policy
- Access quota policy
- Application Control policy
- Bandwidth Control policy
- DLP policy

3. Click **Save**.

Changing the Management Console Password

The Web console password is the primary means to protect your IWSVA device from unauthorized changes. For a more secure environment, change the console password on a regular basis and use a password that is difficult to guess.

The administrator passwords can be changed through the Web console interface. The CLI allows you to change the Enable, Root, and any Administrator account passwords. The CLI command uses the “configure password” command to make the changes.

To change the Web console password through the CLI:

1. Log in to the CLI console and go to privileged mode.
2. Type the following command:

   ```
   configure system password
   ```

The following tips help you design a safe password:

- Include both letters and numbers in your password
- Avoid words found in any dictionary, of any language
- Intentionally misspell words
- Use phrases or combine words
- Use both uppercase and lowercase letters

To change the Web console password:

1. Open the IWSVA console and click **Administration > Management Console > Account Administration** in the main menu.
2. Click the user account for which you want to change the password.
3. From the Login Accounts page, type the new password in the **Password** field and then again in the **Confirm Password** field.
4. Click **Save**.

Configurations After Changing the Web Console Listening Port

When users enable the HTTPS Web console management mode by accessing the **Administration > Network Configuration > Web Console** screen and setting the **Port number** for SSL mode to a port (such as 8443) not used by other applications, they should also specify this SSL management port number in the **HTTP > Configuration > Access Control Settings** screen as well.

If this port number is not specified in the **Access Control Settings** screen, the consequence could be that the IWSVA progress page is blocked by IWSVA itself, when using the HTTPS Web console. In other words, when clients try to access URLs, they would see the progress bar blocked by IWSVA.

Verifying URL Filtering Settings

If you are running the URL filtering module, review the post-install tasks that follow to prepare IWSVA for your environment.

IWSVA accesses the Web Reputation database that contains URLs in over 80 categories, such as "gambling," "games," and "personals/dating." These categories are contained in logical groups.

Trend Micro recommends reviewing the URL filtering settings to ensure that the categories that qualify as company-prohibited sites reflect the values of your organization and do not affect your employees' business-related Web browsing. Before rolling out URL filtering policies, Trend Micro recommends verifying that the default categorizations are appropriate for your organization. For example, a clothing retailer might need to remove a swimsuit Web site from the “Intimate Apparel/Swimsuit” category located in the *Adult* group in order to allow legitimate market and competitor research.

Additionally, you might need to configure URL exceptions to enable employee access to specific sites that would otherwise be blocked, and review the definitions of “work time” to ensure it reflects your workplace schedule.

To review URL filtering settings:

1. Click **HTTP > URL Filtering > Policies > Policy > Exceptions** from the main menu.
2. Choose an approved URL list from the drop-down list that contains the Web sites that will be exempt from URL filtering so that they are always accessible to your clients.
3. Click **Save**.
4. Click **Administration > IWSVA Configuration > Scheduled Times** on the main menu.

Note: The default setting for “work time” is Monday to Friday, from 08:00 to 12:00, and from 13:00 to 17:00.

5. Modify these time settings according to the employee schedules in your workplace.
6. Click **HTTP > URL Filtering > Policies** from the main menu and review the category settings of the URL Filtering Guest Policy and URL Filtering Global Policy.

IWSVA Performance Tuning

If you are experiencing issues with slow browsing performance, consider the modifications described in the following section.

LDAP Performance Tuning

When running IWSVA to use the user/group name authentication identification method (LDAP), HTTP proxy performance becomes dependent upon the responsiveness of the LDAP directory server. In a worst case scenario, every HTTP request would require an LDAP query to authenticate the user's credentials, and another to retrieve group membership information for that user. These queries introduce latency in terms of the transmit/receive delay between IWSVA and the LDAP server, and add load to the LDAP server itself.

LDAP Internal Caches

To reduce the amount of LDAP queries required, IWSVA provides several internal caches:

- **User group membership cache:** This cache can store the group membership information for several hundred users. The synchronization interval for entries in this cache can be configured by the parameter `SyncInterval` under `LDAP_Setting` of the `/etc/iscan/commonldap/LdapSetting.ini` file. The default value is 1440 (24 hours). If it is set to 0, the synchronization is disabled.
- **Client IP to User ID cache:** This cache associates a client IP address with a user who recently authenticated from that same IP address. Any request originating from the same IP address as a previously authenticated request is attributed to that user, provided the new request is issued within a configurable window of time from that authentication. The caveat is that client IP addresses recognized by IWSVA must be unique to a user within that time period; therefore, this cache is not useful in environments where there is a proxy server or source NAT between the clients and IWSVA, or where DHCP frequently reassigns client IPs. To enable or disable this cache, change the `enable_ip_user_cache` setting in the `[user-identification]` section of the `/etc/iscan/intscan.ini` configuration file.
- **User authentication cache:** This avoids re-authenticating multiple HTTP requests passed over a persistent connection. When users pass the credential validation over a persistent connection, IWSVA adds an entry (two important keys in one cache entry are the client's IP address and the client's user name) in the user authentication cache so the subsequent requests over a keep-alive connection does not authenticate again. The client's IP address and client's user name serve as two forward references, or links, to the "client IP to user ID cache" and "user group membership cache," respectively. IWSVA is still able to retrieve the user's connection information from both the IP-user and user-group caches. To enable or disable this cache, change the `enable_ip_user_cache` setting in the `[user-identification]` section of

the /etc/iscan/intscan.ini configuration file. To change the TTL of this cache, change the expire_interval (in seconds) of the /etc/iscan/commonldap/LdapCache.ini configuration file. The default value is 7200 (2 hours).

When deploying IWSVA with LDAP integration, it is important to consider the additional load that authenticating HTTP requests places on the LDAP directory server. In an environment that cannot effectively use the client IP to user ID cache, the directory server needs to be able to handle queries at the same rate IWSVA receives HTTP requests.

Disable Verbose Logging When LDAP Enabled

Trend Micro recommends turning off verbose logging in the /etc/iscan/intscan.ini file, under the [http] section, “verbose” parameter, when LDAP is enabled, for server performance reasons. Verbose logging is primarily used by software developers to identify abnormal application behavior and troubleshooting. In a production deployment, verbose logging is usually unnecessary.

If verbose logging is enabled and LDAP is also enabled, IWSVA logs user authentication information and group membership information in the HTTP log in the Log folder. Logs might contain hundreds of lines per user and, therefore, significantly consume disk space, depending on the amount of internal traffic and the number of groups with which a user is associated. Verbose logging keeps the service busy by issuing I/O operations to the operating system. This might prevent the service from responding to HTTP requests in a timely fashion, and latency might occur. In an extreme bursting HTTP traffic environment, it’s possible to observe significant delays when IWSVA starts up in the verbose mode.

Appendix A

Contact Information and Web-based Resources

This appendix provides information to optimize the InterScan Web Security Virtual Appliance (IWSVA) performance and get further assistance with any technical support questions you might have.

Topics in this appendix include:

Contacting Technical Support

In the United States, Trend Micro representatives can be reached through phone, fax, or email. Our Web site and email addresses are as follows:

http://www.trendmicro.com
http://esupport.trendmicro.com/
support@trendmicro.com

General US phone and fax numbers are as follows:

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Our US headquarters are located in the heart of Silicon Valley:

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014

To obtain Trend Micro contact information for your region/country, please visit http://www.trendmicro.com

IWSVA Core Files for Support

IWSVA generates a core file containing the system data held in memory when a process is abnormally terminated.

Raw core files are created in the `/var/iwss/coredumps` directory on the IWSVA device. They are then compressed and moved to `/var/iwss/UserDumps`. You can use these files when working with Trend Micro technical support to help diagnose the cause of the problem.

To access the core files:

1. From the main IWSVA menu, click **Administration > Support**.
2. On the System Information Files tab, click **Generate System Information File**.
3. Select the Core or System File(s). (Hold down the Ctrl key to select multiple files).
4. Download the file to your computer, or delete it.

Note: To inspect the files yourself, use a program such as GDB, the GNU Project debugger.

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.

Also available in Knowledge Base are product FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

http://esupport.trendmicro.com/

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question through an email message. Response time is typically 24 hours or less.

Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

http://esupport.trendmicro.com/en-us/business/pages/virus-and-threat-removal.aspx

You are prompted to supply the following information:

- **Email**: Your email address where you would like to receive a response from the antivirus team.
- **Product**: The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Number of Infected Seats**: The number of users in your organization that are infected.
- **Upload File**: Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word “virus” as the password—then select the protected zip file in the **Upload File** field.

- **Description**: Please include a brief description of the symptoms you are experiencing. Our team of virus engineers "dissect" the file to identify and characterize any risks it might contain and return the cleaned file to you, usually within 48 hours.

Note: Submissions made through the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you click **Next**, an acknowledgement screen opens. This screen also displays a Tracking Number for the problem you submitted.

If you prefer to communicate by email, send a query to the following address:

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAV, or 877-873-6328

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide customers with up-to-the minute security information.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging risks. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA.

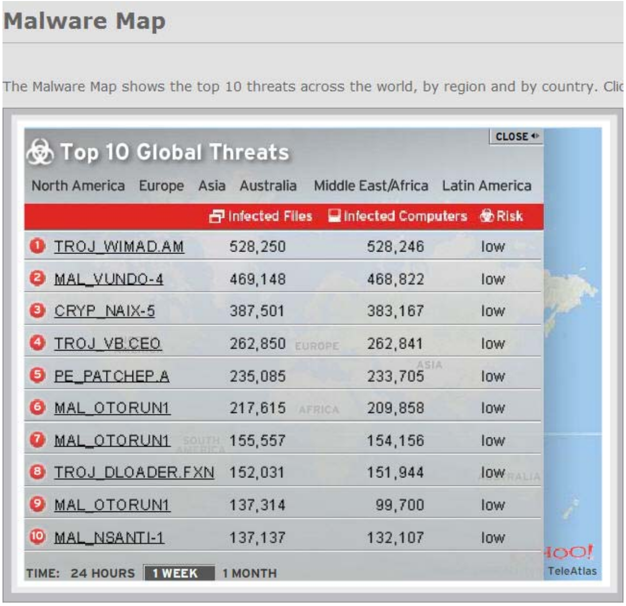
Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

http://www.trendmicro.com/vinfo/

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of risks expected to trigger in the current week, and describes the 10 most prevalent risks around the globe for the current week
- View a Malware Map of the top 10 risks around the globe



Malware Map

The Malware Map shows the top 10 threats across the world, by region and by country. Clic

Top 10 Global Threats

		Infected Files	Infected Computers	Risk
1	TROJ_WIMAD.AM	528,250	528,246	low
2	MAL_VUNDO-4	469,148	468,822	low
3	CRYP_NAIX-5	387,501	383,167	low
4	TROJ_VB.CEO	262,850	262,841	low
5	PE_PATCHEP.A	235,085	233,705	low
6	MAL_OTORUN1	217,615	209,858	low
7	MAL_OTORUN1	155,557	154,156	low
8	TROJ_DLOADER.FXN	152,031	151,944	low
9	MAL_OTORUN1	137,314	99,700	low
10	MAL_NSANTI-1	137,137	132,107	low

TIME: 24 HOURS **1 WEEK** 1 MONTH

FIGURE A-1. Trend Micro World Virus Tracking Program virus map

- Consult the Threat Encyclopedia, a compilation of known risks including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the risk, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:

- The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other risks
- The Trend Micro *Safe Computing Guide*
- A description of risk ratings to help you understand the damage potential for a risk rated Very Low or Low vs. Medium or High risk
- A glossary of virus and other security risk terminology

- Download comprehensive industry white paper
- See the Threat Meter or search the Threat Encyclopedia

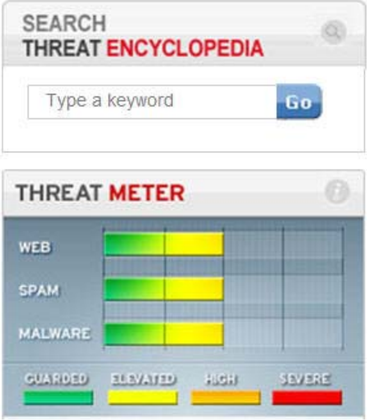


FIGURE A-2. Trend Micro Threat Information

- Subscribe, free, to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters

To open Security Information:

1. Open the IWSVA Web console.
2. Click **Security Info** from the drop-down menu at the top-right panel of the screen. The **Threat Encyclopedia** screen opens.

TrendEdge

A program for Trend Micro employees, partners, and other interested parties that provides information on unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics.

`http://trendedge.trendmicro.com`

Appendix B

Mapping File Types to MIME Content-types

The following table describes some of the file types that you can enter in the HTTP virus scanning policy **MIME content-type to skip** field to skip scanning of the corresponding MIME content-types.

Overview

Potential MIME names are not limited to *Table B-1*, which means you can input any name into the IWSVA UI skip list. (See To select which file types to scan: on page 9-55 for details.) However, the MIME type can only be skipped under the following dependencies:

IWSVA receives a file and determines:

- Is the MIME name is set to be skipped on the UI
- Is the file type (not the MIME name) is listed in the mapping table:
- If the MIME name is in the mapping tables, is MIME name is on the UI skip list?

If IWSVA finds a match, it can be skipped. If IWSVA cannot find a match, it will not be skipped.

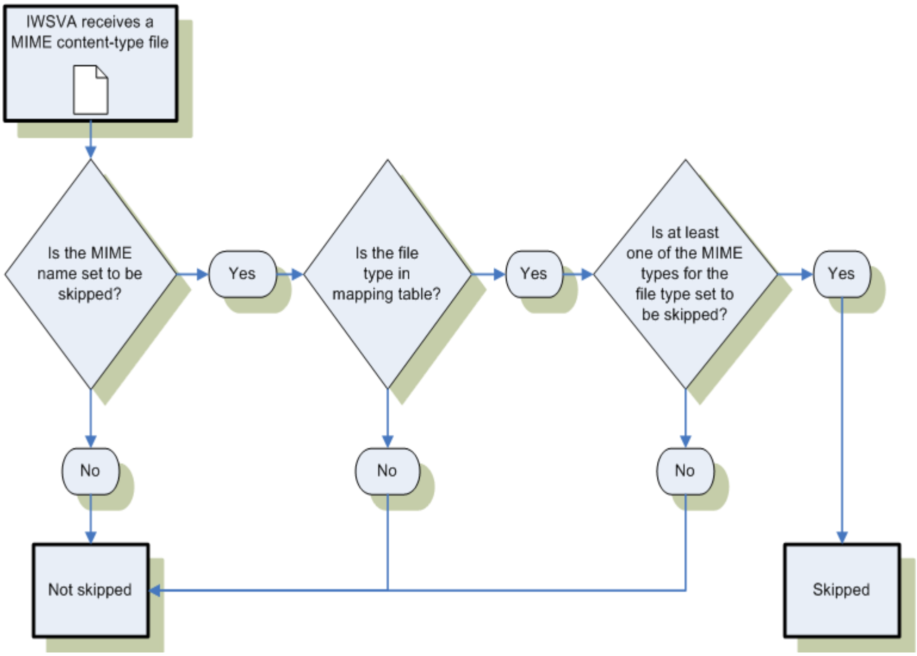

IWSVA receives a MIME content-type file
Is the MIME name set to be skipped?
Yes
Is the file type in mapping table?
Yes
Is at least one of the MIME types for the file type set to be skipped?
Yes
No
No
No
Not skipped
Skipped

FIGURE B-1. MIME Content Type Flow for Skipped Files

If an admin inputs a MIME name and the file type is unknown to IWSVA, IWSVA will skip the scanning of that file. If a MIME type is set to be skipped in IWSVA and it does not exist in the file type-MIME table, scanning will be skipped because the file type-MIME table can not list all possible MIME types for all possible file types.

If at least one of the MIME types for a file type is set to be skipped, it will also have scanning skipped because MIME names are not standard. The file type-MIME table can not list all MIME types for an known file type.

For example, the file type-MIME table contains mappings for FLV files: video/flv, video/x-flv: It does not contain "application/flv." However, some Web sites use "application/flv." IWSVA will not be able find the mapping entry for it, but IWSVA knows this is an FLV file by performing a file type check. It will skip the scan of this file.

If admin inputs "video/flv" and "application/flv" in skip list, the following check occurs:

- MIME name set to be skipped (MIME type: application/flv) >Yes >
- Check whether file type is in mapping table (file type: flv) > Yes >
- At least one of the MIME types for file type is set to skip >Yes > Skip the scan

File Type Mapping Table for MIME Content Files

TABLE B-1. File Type Mapping Table for MIME Content-Files

FILE TYPE	MIME CONTENT-TYPE
ACE Compression File	application/x-ace
ACE Compression File	application/x-compressed
Apple Sound	audio/aiff
Apple Sound	audio/x-aiff
Audio InterChange File Format from Apple/SGI	audio/aiff
Audio InterChange File Format from Apple/SGI	audio/x-aiff
Audio InterChange File Format from Apple/SGI	sound/aiff
Audio InterChange File Format from Apple/SGI	audio/rmf
Audio InterChange File Format from Apple/SGI	audio/x-rmf
Audio InterChange File Format from Apple/SGI	audio/x-pn-aiff
Audio InterChange File Format from Apple/SGI	audio/x-gsm
Audio InterChange File Format from Apple/SGI	audio/x-midi
Audio InterChange File Format from Apple/SGI	audio/vnd.qcelp
ARJ	application/arj

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
ARJ	application/x-arj
ARJ	application/x-compress
ARJ	application/x-compressed
ARJ	zz-application/zz-winassoc-arj
Advanced Streaming Format	video/x-ms-asf
Advanced Streaming Format	video/x-ms-asf-plugin
Advanced Streaming Format	video/x-ms-wm
Advanced Streaming Format	video/x-ms-wmx
Advanced Streaming Format	audio/asf
Advanced Streaming Format	application/asx
Advanced Streaming Format	application/x-mplayer2
Advanced Streaming Format	application/vnd.ms-as"
Nullsoft AVS	video/avs-video
Mime Base 64	application/base64
Macintosh MacBinary Archive	application/mac-binary
Macintosh MacBinary Archive	application/macbinary
Macintosh MacBinary Archive	application/octet-stream
Macintosh MacBinary Archive	application/x-binary
Macintosh MacBinary Archive	application/x-macbinary
BINHEX	application/binhex

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
BINHEX	application/binhex4
BINHEX	application/mac-binhex
BINHEX	application/mac-binhex40
BINHEX	application/x-binhex40
Windows BMP	image/bmp
Windows BMP	image/x-bmp
Windows BMP	image/x-bitmap
Windows BMP	image/x-xbitmap
Windows BMP	image/x-win-bitmap
Windows BMP	image/x-windows-bmp
Windows BMP	image/ms-bmp
Windows BMP	image/x-ms-bmp
SGI Image	image/x-sgi-bw
GNU BZIP2	application/x-bzip2
GNU BZIP3	application/bzip2
GNU BZIP4	application/x-bz2
GNU BZIP5	application/x-compressed
Computer Graphics Metafiles	image/cgm
COM	application/octet-stream
COM	application/x-msdos-program

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
COM	application/x-msdownload
UNIX cpio Archive	application/x-cpio
Macromedia Director Shockwave Movie	application/x-director
WordPerfect	application/wordperfect
AutoCAD DWG	application/acad
AutoCAD DWG	application/x-acad
AutoCAD DWG	drawing/x-dwg
AutoCAD DWG	image/vnd.dwg
AutoCAD DWG	image/x-dwg
Encapsulated Postscript	application/postscript
Encapsulated Postscript	image/x-eps
Encapsulated Postscript	image/eps
Encapsulated Postscript	application/x-eps
Encapsulated Postscript	application/eps
EXE	application/octet-stream
EXE	application/exe
EXE	application/x-msdownload
EXE	application/x-exe
EXE	application/dos-exe

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
EXE	vms/exe
EXE	application/x-winexe
EXE	application/msdos-windows
Free Hand Document	image/x-freehand
AutoDesk Animator (FLI or FLC)	video/x-fli
AutoDesk Animator (FLI or FLC)	video/flc
AutoDesk Animator (FLI or FLC)	video/fli
AutoDesk Animator (FLI or FLC)	video/x-acad-anim
Macromedia Flash FLV Video	video/flv
Macromedia Flash FLV Video	video/x-flv
Macromedia Flash FLV Video	flv-application/octet-stream
Frame Maker	application/vnd.framemaker
GIF	image/gif
GNU ZIP	application/gzip
GNU ZIP	application/x-gzip
GNU ZIP	application/x-gunzip
GNU ZIP	application/gzipped
GNU ZIP	application/gzip-compressed
GNU ZIP	application/x-compressed
GNU ZIP	application/x-compress

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
GNU ZIP	gzip/document
GNU ZIP	encoding/x-gzip
Windows Icon	image/ico
Windows Icon	image/x-icon
Windows Icon	application/ico
Windows Icon	application/x-ico
Windows Icon	application/x-win-bitmap
Windows Icon	image/x-win-bitmap
Amiga 8SVX Audio Interchange File Format	audio/x-aiff
Amiga 9SVX Audio Interchange File Format	image/iff
Amiga 10SVX Audio Interchange File Format	image/x-iff
Amiga 11SVX Audio Interchange File Format	application/iff
JAVA Applet	text/x-java-source
JAVA Applet	application/java-class
JAVA Applet	application/x-java-applet
JAVA Applet	application/x-java-vm
JPEG	image/jpeg
JPEG	image/jpg

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
JPEG	image/jp_
JPEG	image/pipeg
JPEG	image/pjpeg
LHA	application/x-lha
LHA	application/lha
LHA	application/x-compress
LHA	application/x-compressed
LHA	application/maclha
Compiled LISP	application/x-lisp
NT/95 Shortcut (*.lnk)	application/x-ms-shortcut
LightWave 3D Object	image/x-lwo
MAUD Sample Format	audio/x-maud
Microsoft Document Imaging	image/vnd.ms-modi
MIDI	audio/midi
Magick Image File Format	application/x-mif
Multi-image Network Graphics	video/x-mng
Multi-image Network Graphics	video/mng
MP3	audio/mpeg
MP3	audio/mpeg3
MP3	audio/x-mpeg-3

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
MPEG	video/mpeg
MPEG	video/mpg
MPEG	video/x-mpg
MPEG	video/mpeg2
MPEG	video/x-mpeg
MPEG	video/x-mpeg2a
Microsoft Cabinet	application/x-cainet-win32-x86
Windows Word	application/msword
Windows Word	application/doc
Windows Word	application/vnd.msword
Windows Word	application/vnd.ms-word
Windows Word	application/x-msw6
Windows Word	application/x-msword
Windows Excel	application/excel
Windows Excel	application/x-msexcel
Windows Excel	application/x-ms-excel
Windows Excel	application/x-excel
Windows Excel	application/vnd.ms-excel
Windows Excel	application/xls
Windows Excel	application/x-xls

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Windows Installer	application/x-ole-storage
Microsoft Access (MDB)	application/x-msaccess
Microsoft Access (MDB)	application/msaccess
Microsoft Access (MDB)	application/vnd.msaccess
Microsoft Access (MDB)	application/vnd.ms-access
Microsoft Access (MDB)	application/mdb
Microsoft Access (MDB)	application/x-mdb
Microsoft Access (MDB)	zz-application/zz-winassoc-mdb
Microsoft Office 12	application/vnd.ms-word.document.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Microsoft Office 12	application/vnd.ms-word.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.wordprocessingml.template
Microsoft Office 12	application/vnd.ms-powerpoint.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.template
Microsoft Office 12	application/vnd.ms-powerpoint.addin.macroEnabled.12

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Microsoft Office 12	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.slideshow
Microsoft Office 12	application/vnd.ms-powerpoint.presentation.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.presentation
Microsoft Office 12	application/vnd.ms-excel.addin.macroEnabled.12
Microsoft Office 12	application/vnd.ms-excel.sheet.binary.macroEnabled.12
Microsoft Office 12	application/vnd.ms-excel.sheet.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Microsoft Office 12	application/vnd.ms-excel.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.spreadsheetml.template
Microsoft Office 12	application/vnd.openxmlformats
Windows PowerPoint	application/mspowerpoint

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Windows PowerPoint	application/powerpoint
Windows PowerPoint	application/vnd.ms-powerpoint
Windows PowerPoint	application/ms-powerpoint
Windows PowerPoint	application/mspowerpnt
Windows PowerPoint	application/vnd-mspowerpoint
Windows PowerPoint	application/x-powerpoint
Windows PowerPoint	application/x-mspowerpoint
Windows Project	application/vnd.ms-project
Windows Project	application/x-msproject
Windows Project	application/x-project
Windows Project	application/msproj
Windows Project	application/msproject
Windows Project	application/x-ms-project
Windows Project	application/x-dos_ms_project
Windows Project	application/mpp
Windows Project	zz-application/zz-winassoc-mpp
Windows Write	application/mswrite
Windows Write	application/x-mswrite
Windows Write	application/wri
Windows Write	application/x-wri

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Windows Write	application/msword
Windows Write	application/microsoft_word
Windows Write	zz-application/zz-winassoc-wri
Open Document	application/vnd.oasis.opendocument.text
Open Document	application/vnd.oasis.opendocument.text-template
Open Document	application/vnd.oasis.opendocument.graphics
Open Document	application/vnd.oasis.opendocument.graphics-template
Open Document	application/vnd.oasis.opendocument.presentation
Open Document	application/vnd.oasis.opendocument.presentation-template
Open Document	application/vnd.oasis.opendocument.spreadsheet
Open Document	application/vnd.oasis.opendocument.spreadsheet-template
Open Document	application/vnd.oasis.opendocument.chart
Open Document	application/vnd.oasis.opendocument.chart-template
Open Document	application/vnd.oasis.opendocument.image

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Open Document	application/vnd.oasis.opendocument.image-template
Open Document	application/vnd.oasis.opendocument.formula
Open Document	application/vnd.oasis.opendocument.formula-template
Open Document	application/vnd.oasis.opendocument.text-master
Open Document	application/vnd.oasis.opendocument.text-web
Gravis Patch Files	audio/pat
Gravis Patch Files	audio/x-pat
Microsoft Paint v1.x	image/x-pcx
Microsoft Paint v1.x	image/pcx
Microsoft Paint v1.x	image/x-pc-paintbrush
Microsoft Paint v1.x	application/x-pcx
Microsoft Paint v1.x	application/pcx
Microsoft Paint v1.x	zz-application/zz-winassoc-pcx
Microsoft Paint v2.x	image/x-pcx
Microsoft Paint v2.x	image/pcx
Microsoft Paint v2.x	image/x-pc-paintbrush
Microsoft Paint v2.x	application/x-pcx

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Microsoft Paint v2.x	application/pcx
Microsoft Paint v2.x	zz-application/zz-winassoc-pcx
PCX	image/x-pcx
PCX	image/pcx
PCX	image/x-pc-paintbrush
PCX	application/x-pcx
PCX	application/pcx
PCX	zz-application/zz-winassoc-pcx
Palm Pilot Image	application/x-pilot-pdb
Adobe Portable Document Format (PDF)	application/pdf
Adobe Portable Document Format (PDF)	application/x-pdf
Adobe Font File	application/x-font
Macintosh Bitmap	image/pict
Macintosh Bitmap	image/x-pict
Portable Network Graphics	image/png
PPM Image	image/x-portable-pixmap
PPM Image	image/x-p
PPM Image	image/x-ppm
PPM Image	application/ppm

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
PPM Image	application/x-ppm
Postscript	application/postscript
Adobe Photoshop (PSD)	application/octet-stream
Paint Shop Pro	image/bmp
Quick Time Media	video/quicktime
Quick Time Media	video/x-quicktime
Quick Time Media	image/mov
Quick Time Media	audio/aiff
Quick Time Media	audio/x-midi
QuarkXPress Document (QXD)	application/quarkxpress
QuarkXPress Document (QXD)	application/x-quark-express
Real Audio	audio/vnd.rn-realaudio
Real Audio	audio/x-pn-realaudio
Real Audio	audio/x-realaudio
Real Audio	audio/x-pm-realaudio-plugin
Real Audio	video/x-pn-realvideo
RAR	application/rar
Sun Raster (RAS)	image/x-cmu-raster
Sun Raster (RAS)	image/cmu-raster
Real Media	application/vnd.rn-realmedia

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Microsoft RTF	application/rtf
Microsoft RTF	application/x-rtf
Microsoft RTF	text/richtext
Lotus ScreenCam Movie	application/vnd.lotus-screencam
Lotus ScreenCam Movie	application/x-lotusscreencam
Lotus ScreenCam Movie	application/x-screencam
Lotus ScreenCam Movie	video/x-scm
Lotus ScreenCam Movie	video/x-screencam
IRCAM Sound File	audio/x-sf
Sonic Foundry File	audio/sfr
Macromedia Flash	application/x-shockwave-flash
TAR	application/x-tar
TAR	application/tar
TAR	application/x-gtar
TAR	multipart/x-tar
TAR	application/x-compress
TAR	application/x-compressed
Targa Image	image/tga
Targa Image	image/x-tga
Targa Image	image/targa

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Targa Image	image/x-targa
TIFF	image/tiff
TNEF file	application/ms-tnef
TNEF file	application/vnd.ms-tne
ASCII Text	text/plain
ASCII Text	application/txt
ASCII Text	text/html
ASCII Text	text/css
UUENCODE	text/x-uuencode
VBScript	text/vbscript
VBScript	text/vbs
VBScript	application/x-vbs
Creative Voice Format (VOC)	audio/voc
Creative Voice Format (VOC)	audio/x-voc
Microsoft RIFF	audio/wav
Microsoft RIFF	application/x-cdf
Microsoft RIFF	application/x-cmx
Microsoft RIFF	image/x-cmx
Microsoft RIFF	drawing/cmx
Microsoft RIFF	application/cmx

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Webshots Picture Collection	application/x-webshots
Webshots Picture Collection	application/wbc
Windows Metafile	application/x-msmetafile
Windows Metafile	application/wmf
Windows Metafile	application/x-wmf
Windows Metafile	image/x-wmf
Windows Metafile	zz-application/zz-winassoc-wmf
PKZIP	application/zip
PKZIP	application/x-zip
PKZIP	application/x-zip-compressed
PKZIP	multipart/x-zip
PKZIP	application/x-compress
PKZIP	application/x-compressed
ACE Compression File	application/x-ace
ACE Compression File	application/x-compressed
Apple Sound	audio/aiff
Apple Sound	audio/x-aiff
Audio InterChange File Format from Apple/SGI	audio/aiff
Audio InterChange File Format from Apple/SGI	audio/x-aiff

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Audio InterChange File Format from Apple/SGI	sound/aiff
Audio InterChange File Format from Apple/SGI	audio/rmf
Audio InterChange File Format from Apple/SGI	audio/x-rmf
Audio InterChange File Format from Apple/SGI	audio/x-pn-aiff
Audio InterChange File Format from Apple/SGI	audio/x-gsm
Audio InterChange File Format from Apple/SGI	audio/x-midi
Audio InterChange File Format from Apple/SGI	audio/vnd.qcelp
ARJ	application/arj
ARJ	application/x-arj
ARJ	application/x-compress
ARJ	application/x-compressed
ARJ	zz-application/zz-winassoc-arj
Advanced Streaming Format	video/x-ms-asf
Advanced Streaming Format	video/x-ms-asf-plugin
Advanced Streaming Format	video/x-ms-wm
Advanced Streaming Format	video/x-ms-wmx

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Advanced Streaming Format	audio/asf
Advanced Streaming Format	application/asx
Advanced Streaming Format	application/x-mplayer2

Appendix C

Architecture and Configuration Files

Topics in this appendix include the following:

Main Components

The following are the main InterScan Web Security Virtual Appliance (IWSVA) modules:

- **Main Program:** Installs the Web console and the basic library files necessary for IWSVA.
- **Advanced Threat Protection:** Installs the services necessary for HTTP scanning (either ICAP or HTTP scanning) and URL blocking
- **Application Control:** Provides a security technology that automates the discovery of popular Internet applications and allows administrators to control them using policies.
- **Bandwidth Control**: Reduces network congestion by controlling communications, reducing unwanted traffic and allowing critical traffic or services the appropriate bandwidth allocation.
- **HTTP Inspection:** Allows administrators to identify behavior and filter web traffic according to HTTP methods, URLs, and headers.
- **Data Loss Prevention**: Shows all DLP policies on the system—enabled as well as disabled.
- **FTP Scanning:** Installs the service that enables FTP scanning.
- **URL Filtering:** Installs the service necessary for URL filtering.
- **Applets and ActiveX Scanning:** Installs the service necessary for checking Java applet and ActiveX object digital signatures, and instrumenting applets so their execution can be monitored for prohibited operations.
- **SNMP Notifications:** Installs the service to send SNMP traps to SNMP-compliant network management software.
- **Control Manager Agent for IWSVA:** Installs the files necessary for the Control Manager agent to enable monitoring and configuration through Control Manager.

Main Services

To start or stop any of the services in this section, you must be logged on to IWSVA as `root` using either a local terminal or SSH. The root user can only stop or start the HTTP and FTP services from within IWSVA CLI (see Enabling the HTTP/HTTPS Traffic Flow on page 7-2 and Enabling FTP Traffic and FTP Scanning on page 12-5).

No other services can be stopped or started from within IWSVA.

The following services are used by IWSVA:

- **Trend Micro IWSVA Console (java):** This service is the Web server hosting the Web console.
- **Trend Micro IWSVA for FTP (isftpd):** This service enables the FTP traffic flow and FTP virus scanning.
- **Trend Micro IWSVA for HTTP (iwssd):** This service enables the HTTP traffic flow and HTTP scanning (including FTP over HTTP). It also handles Applets and ActiveX security processing.

Note: FTP over HTTP is not supported in Transparent Bridge Mode.

- **Trend Micro IWSVA Log Import (logtodb):** This service writes logs from text files to the database.
- **Trend Micro IWSVA Notification Delivery Service (isdelvd):** This service handles administrator notifications (through email) and user notifications (through browser).
- **Trend Micro SNMP Service (snmpd):** This service sends SNMP trap notifications to SNMP-capable network monitoring devices.
- **Trend Micro Service Monitor (svcmonitor):** This service checks the health of the following daemons: HTTP, FTP, Application Control, Tomcat and WMI Daemons.
- **Trend Micro Database Service (postgres, postmaster):** This service manages the IWSVA local PostgreSQL database, which stores policy settings, reporting logs and statistics data for Summary pages.
- **Trend Micro Authentication Service (AuthDaemon):** This service receives authentication requests from iwssd daemon or appd daemon, and replies authentication results.
- **Trend Micro Syslog Service (tmsyslogd):** This service provides enterprise-class logging capabilities and sends syslog events to different servers.
- **Trend Micro Control Manager Service (En_Main):** This service permits IWSVA configuration and status reporting through Trend Micro Control Manager, if you are using Control Manager.
- **Trend Micro IWSVA for Dashboard (ismetricmgmtd):** This service collects system resource data to be used in the display of real-time dashboard metrics.

- **Trend Micro IWSVA for Application Control (appd)**: This service provides a way to control application usage by protocol and displays useful traffic statistics about inbound and outbound application traffic.
- **Trend Micro IWSVA for LDAP authentication (WMIDaemon)**: This service receives WMI query requests from AuthDaemon and returns WMI query results to AuthDaemon for transparent LDAP authentication.

Scheduled Tasks

When installing IWSVA, the setup program creates several scheduled tasks.

- **purgefile:** Runs daily at 2:00 am to delete old text log files, subject to the configured time interval to retain logs.
- **schedulereport:** Runs hourly to check if a scheduled report is configured to run.
- **schedulepr_update:** Runs daily to check if it is time to update the product registration/license.
- **schedule_au:** Runs every 15 minutes to check if it is time to update the pattern file or other program components.
- **cleanfile:** Runs hourly, to remove temporary files downloaded for scan-behind or large file scanning.
- **DbOldDataCleanup.sh:** Runs daily at 2:05 am to clean up old reporting log data in the database and cleans up the old access quota counters in the database.
- **svc_snmpmonitor.sh:** Runs every five minutes to verify that the logtodb, mail, postgres and metric daemons are running. It restarts them if they are not.
- **db_reindex.sh:** Runs daily at 28 minutes past every other hour to rebuild corrupted database indices containing any invalid data. This maintains optimum database performance.
- **db_vacuum.sh:** Runs daily at 3:58 am to perform garbage collection to free up unused space from database tables in order to maintain optimum database performance.
- **S99ISSnmpd restart**: Runs daily at 01:48 am to restart SNMP daemon.
- **tomcatchecker.sh**: Runs daily at 01:18 am/4:18 am/6:18 am/10:18 pm to check if it needs to restart tomcat service.
- **schedule_crl_update.sh**: Runs daily at 02:00 am to update Certificate revoke List (CRL).

- **IniRecover.sh**: Runs daily at 03:55 am to check if it needs to recover `/etc/iscan/intscan.ini` file.
- **log_purge.py**: Runs daily at 1:30 am to delete old text log files.
- **clear_tmpfs.py**: Runs daily at 3:00 am to clear tmpfs.
- **month_table.sh**: Run daily at 4:00 am to schedule generate month table for Log and report.
- **logpurge.sh**: Runs daily at 01:20 am to clear ***`report_log.*`*** in `/etc/iscan/log` directory.
- **archive_debug_log.py**: Runs every minute to check if it is time to archive debug log.
- **bifconnect.sh**: Run every Saturday at 1:15 am to send product information to Trend Micro Control Manager.
- **logbackup.sh**: Run daily at 12:20 am to schedule backup log.

About Configuration Files

To access configuration files, you must be logged on to the appliance as `root` using either a local terminal or SSH.

There are three types of configuration files: main, protocol module, and scanning module. All the configuration files are in the `{IWSS root}` directory; the default location for `{IWSS root}` is `/etc/iscan/`. The main configuration file is in `intscan.ini`.

- Settings specific to virus scanning are in:

  `{IWSS root}/IWSSPIScanVsapi.dsc`

- Settings that are specific to the ICAP protocol are in:

  `{IWSS root}/IWSSPIProtocolIcap.pni`

- Settings that are specific to the stand-alone proxy are in:

  `{IWSS root}/IWSSPIProtocolHttpProxy.pni`

- Settings for URL filtering scanning module are in:

  `{IWSS root}/IWSSPIUrlFilter.dsc`

- Settings specific to reporting are in:

`{IWSS root}/report.ini`

- Settings specific to botnet scanning are in:

  `{IWSS root}/IWSSPINcieScan.dsc`

- Settings for DLP scanning are in:

  `{IWSS root}/IWSSPIDlpFilter.dsc`

- Settings specific to java/activeX scanning are in

  `{IWSS root}/IWSSPIJavascan.dsc`

- Settings specific http inspection are in:

  `{IWSS root}/IWSSPISigScan.dsc`

- Settings specific ftp scanning are in:

  `{IWSS root}/IWSSPIProtocolFtp.pni`

- Settings specific application control are in:

  `{IWSS root}/appcMapping.ini`

- Settings for the URL Categorization database are in:

  `{IWSS root}/urlfxIFX.ini`

- Settings for default URL categories and their mapping information are in:

  `{IWSS root}/urlfcMapping.ini`

- Settings for the list of IP address and IP ranges of all machines allowed to access the IWSVA device are in:

  `{IWSS root}/ClientACL_http.ini (for HTTP)`

  `{IWSS root}/ClientACL_ftp.ini (for FTP)`

- Settings for rules that define what ports IWSVA forwards HTTP requests to are in:

  `{IWSS root}/HttpPortPermission_http.ini (for HTTP)`

  `{IWSS root}/HttpPortPermission_ftp.ini (for FTP)`

- Settings for rules that define what ports IWSVA allows HTTPS tunneling to are in:

  `{IWSS root}/HttpsConectACL_http.ini`

The IWSVA Web console varies depending on which modules are used. If you have been using a previous version of IWSVA, there are also many new features available in IWSVA that require new `.ini` file entries.

Protocol Handlers

Functions responsible for interpreting and processing messages in some recognized transmission protocols are encapsulated in a dynamic library referred to as a protocol handler. IWSVA provides a choice of either an ICAP protocol handler, which enables IWSVA to act as an ICAP server, or an HTTP proxy handler, wherein IWSVA acts like a direct HTTP proxy server. (The HTTP protocol handler is also used in bridge mode.) The application binary is independent of the protocol handler, allowing the same application to support different protocols with a configuration change.

Provide the complete path of the active configuration file of the protocol in the `main/protocol_config_path` entry in the `/etc/iscan/intscan.ini` file application.

Protocol handlers require their own specific configuration files, which contain entries that pertain only to that protocol. These protocol configuration files are denoted with a `.pni` filename extension.

Scanning Modules

Traffic scanning functionality is provided through dynamic libraries known as scanning modules. The first scanning module available to IWSVA provides content scanning using the scan engine.

Each scanning module has a configuration file with a `.dsc` extension. The IWSVA application locates the available scanning modules by searching for `.dsc` files in the directory that is provided in the `scan/plugin_dir` entry in the `/etc/iscan/intscan.ini` file.

Appendix D

OpenLDAP Reference

Though OpenLDAP supports Kerberos authentication, the packages to enable Kerberos authentication support are not installed by default. This appendix covers how to install and configure Kerberos support for OpenLDAP. In addition, this appendix explains how to set up your OpenLDAP directory so InterScan Web Security Virtual Appliance (IWSVA) can query it when using the user/group authentication method.

This chapter includes the following topics:

OpenLDAP Server Side Configuration

Software Package Dependencies

The following software packages are compatible with IWSVA:

- cyrus-sasl-2.1.19
- db-4.2.52.NC
- heimdal-0.6.2
- openldap-2.3.39
- openssl-0.9.7d

Configuration Files

Using OpenLDAP with IWSVA requires modifying the following configuration files:

```
/etc/openldap/ldap.conf

/etc/openldap/slapd.conf
```

Sample ldap.conf

```
#
# System-wide ldap configuration files. See ldap.conf(5) for
# details
# This file should be world readable but not world writable.


# OpenLDAP supports the ldap.conf file. You could use this file to
# specify a number of defaults for OpenLDAP clients. Normally this
# file can be found under /etc/openldap based on /etc/init.d/ldap
# start script's setting

# Set host IP address or fully qualified domain name

HOST example.peter.com
#HOST 10.2.1.1

# Set the default BASE DN where LDAP search will start off

BASE dc=peter,dc=com

# Set the default URI
```

```
URI ldap://example.peter.com

# SASL options
# specify the sasl mechanism to use. This is a user-only option.
# SASL_MECH <mechanism>
# specify the realm. This is a user-only option
# SASL_REALM <realm>
# specify the authentication identity.
# SASL_AUTHCID <authcid>
```

Sample slapd.conf

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
# Enforce all changes to follow the defined schemas loaded via
# include statements in the conf file


# NOTE 1
# All the OpenLDAP config files and backend databases are accessed
# and created by “ldap”, so if you touch these config files by
# "root", “a Permission Denied” error will occur. Please modify
# ownership accordingly.

# NOTE 2
# krb5-kdc.schema fails to work with current OpenLDAP 2.2.x distro
# krb5ValidStart, krb5ValidEnd, krb5PasswordEnd need to have
# "EQUALITY generalizedTimeMatch" inserted before the ORDERING
# statement.
# www.openldap.org/lists/openldap-bugs/200309/msg00029.html

# Enforce all changes to follow the defined schemas loaded via
# include statements in the conf file

schemacheck on

# Included schemas

include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/krb5-kdc.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/java.schema
```

```
# Directives say where to write out slapd's PID and arguments
# started with

pidfile /usr/local/var/run/slapd.pid
argsfile /usr/local/var/run/slapd.args

# Load dynamic backend modules:
# modulepath/usr/local/libexec/openldap
# moduleloadback_bdb.la
# moduleloadback_ldap.la
# moduleloadback_ldbm.la
# moduleloadback_passwd.la
# moduleloadback_shell.la

# Sample security restrictions
#Require integrity protection (prevent hijacking)
#Require 112-bit (3DES or better) encryption for updates
#Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#Root DSE: allow anyone to read it
#Subschema (sub)entry DSE: allow anyone to read it
#Other DSEs:
#Allow self write access
#Allow authenticated users read access
#Allow anonymous users to authenticate
#Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
#by self write
#by users read
#by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn. (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
access to *
by self write
by users read
by anonymous auth
by * none

# We have found this gives a useful amount of information about
# directory

loglevel 256

#Specify the number of threads used in slapd, default = 16
#Increasing or decreasing the number of threads used can
#drastically affect performance, we found 20 threads to be optimal
#for our setup, but it can be different under other operating
#systems

threads 20

#Tell slapd to close connections that have been idle for 30 seconds
#or more

idletimeout 30

# Enable LDAPv2 support. This option is disabled by default.

allow bind_v2

# Disable anonymous bind

disallow bind_anon

# Comment this section to enable simple bind

#disallow bind_simple

# NOTE 3
# SASL Configuration
# Caution: make sure you use the canonical name of the machine
# in sasl-host. Otherwise, OpenLDAP wont be able to offer GSSAPI
# authentication

# Set the SASL realm and canonical name of the host
sasl_hostexample.peter.com
sasl_realmPETER.COM

# Allow proxy authentication if it's configured

sasl-authz-policyboth

# NOTE 4
# Mapping of SASL authentication identities to LDAP entries
# The sasl-regexp line are particularly critical. They are what
# rewrite incoming connections who have SASL formatted DNs to the
# DNs that are in the directory DB. It's important to remember that
# they are processed in order, so you want to write them from most
# specific to most general

# NOTE 5
# We set the cn=.* since we are going to adopt different security
# mechanisms. If Kerberos v5 is the only one used, change wildcard
# to cn=GSSAPI,cn=auth

#sasl-regexp uid=(.*),cn=GSSAPI,cn=auth
#uid=$1,ou=people,dc=peter,dc=com

sasl-regexp uid=(.*),cn=.*,cn=auth uid=$1,ou=people,dc=peter,dc=com

# ldbm database definitions

# NOTE 6
# Correctly configuring the backend Berkeley DB is very critical
# follow the guideline at
# http://www.openldap.org/faq/data/cache/1073.html

# Cleartext passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.

databasebdb

# These options specify a DN and passwd that can be used to
# authenticate as the super-user entry of the database. The DN and
# password specified here will always work, regardless of whether
# the entry named actually exists or has the password given.
# This solves the chicken-and-egg problem of how to authenticate and
# add entries before any entries yet exist

suffix"dc=peter,dc=com"
rootdn"cn=admin,dc=peter,dc=com"
rootpwadmin

# NOTE 7
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700
# recommended.

directory/usr/local/var/openldap-data

#Tell the slapd to store the 10000 most accessed entries in memory
#Having a properly configured cache size can drastically affect
#performance

cachesize 10000
```

```
# Indices to maintain
# Some versions of OpenLDAP don't support the index of uniqueMember
# "pres" indexing allows you to see a filter that asks if the
# attribute is present in an entry
# "eq" indexing allows to ask if an attribute has an exact value
# "apporx" indexing allows to ask if an attribute value sounds like
# something
# This option is tied to --enable-phonetic compile option in
# OpenLDAP
# "sub" indexing allows to do substring search on an attribute's
# values

index default eq,pres
index objectclass  eq,pres
index cn,sn,givenname,mail   eq,pres,approx,sub
index uideq,pres
index uidNumber,gidNumber,memberUid   eq,pres
```

Tools

To create the server database and associate indices by importing an existing LDIF file:

NAME

slapadd - Add entries to a SLAPD database

SYNOPSIS

```
/usr/sbin/slapadd  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf] [-l ldif-file]
```

DESCRIPTION

Slapadd is used to add entries specified in LDAP Directory Interchange Format (LDIF) to a slapd database.

- Dump the server database to an LDIF file. This can be useful when you want to make human-readable backup of current database.

NAME

slapcat - SLAPD database to LDIF utility

SYNOPSIS

```
/usr/sbin/slapcat  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf] [-l ldif-file]
```

DESCRIPTION

slapcat is used to generate an LDAP Directory Interchange Format (LDIF) output based upon the contents of a slapd database.

- Rebuilds all indices based upon the current database contents

NAME

slapindex - SLAPD index to LDIF utility

SYNOPSIS

```
/usr/sbin/slapindex [-f slapd.conf] [-d level] [-b suffix] [-n
dbnum]
```

DESCRIPTION

Slapindex is used to regenerate slapd indices based upon the current contents of a database.

- Check the settings of slapd.conf

NAME

Slaptest – Check the suitability of the slapd conf file

SYNOPSIS

```
/usr/sbin/slaptest  [-v]  [-d  level] [-f slapd.conf]
```

DESCRIPTION

Slaptest is used to check the conformance of the slapd.conf configuration file. It opens the slapd.conf configuration file, and parses it according to the general and the backend-specific rules, checking its conformance.

- LDAP query utility

NAME

ldapsearch - LDAP search tool

SYNOPSIS

```
ldapsearch  [-D binddn] [-W]  [-w bindpasswd] [-H ldapuri] [-h
ldaphost] [-p ldap- port]  [-b searchbase] [-s base|one|sub] [-x]
[-Y mech] [-Z[Z]] filter [attrs...]
```

DESCRIPTION

ldapsearch opens a connection to an LDAP server, binds, and performs a search using specified parameters.

EXAMPLE

The command performs a query using simple plain text authentication for a matched entry with “uid=petery” and requests the mail attribute for a matched entry to be returned by the LDAP server.

```
ldapsearch -x -D "cn=admin,dc=peter,dc=com" -w admin -b
"dc=peter,dc=com" -s sub "uid=petery" mail
```

For further information, consult the manual page.

```
Verify SASL/OpenLDAP/Kerberos v5 Authentication

1. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapsearch -v -x \

-D "cn=admin,dc=peter,dc=com" -W -b "" -s base -LLL \

-H ldap://example.peter.com/ supportedSASLMechanisms

2. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapsearch -b
"dc=peter,dc=com" \

-H ldap://example.peter.com/

3. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapwhoami -H
ldap://example.peter.com
```

Appendix E

Best Practices for IWSVA

This appendix contains information about the best practices to follow for InterScan Web Security Virtual Appliance.

The topics include:

- Authenticating Multiple Users on Shared Personal Computers (Standard Authentication Method) on page E-2
- Scanning Considerations on page E-3

Authenticating Multiple Users on Shared Personal Computers (Standard Authentication Method)

Supporting multiple users on a single shared personal computer (PC) using Microsoft Active Directory server for authentication can present some challenges to IT managers and users alike. IWSVA provides authentication based on a browser challenge and can support the authentication of multiple users on a shared PC using Microsoft Internet Explorer as the default browser.

Best Practice Suggestions

Leveraging Microsoft ShellRunas Utility

- For shared PCs, you can leverage the Microsoft ShellRunas utility to force the user to authenticate each time when Microsoft Internet Explorer is started. The AD credentials are used to authenticate the user and Internet Explorer will leverage the credentials to automatically populate the user ID information in the HTTP header to allow IWSVA to identify the user for logging, reporting, and policy enforcement purposes.
- Download the MS ShellRunas utility from:

  http://technet.microsoft.com/en-us/sysinternals/cc300361.aspx
- Users must remember to shut down their IE browser sessions when they're finished using the computer. This allows Microsoft Internet Explorer to prompt the next user for their credentials. User education is critical to the success of this tool.
- Optionally, you can also modify the IP User Cache parameter to extend or shorten the cache interval for the authenticated user cache to further fine tune when users should be prompted for their authentication credentials. The default IWSVA user cache value is 2 hours (120 minutes). See the "`configure module ldap ipuser_cache interval <interval>`" CLI command for more information.

Scanning Considerations

IWSVA's malware scanning architecture is a hybrid solution that uses cloud-based malware detection methods such as Trend Micro's Smart Protection Network (SPN) and local, on-box scan technologies and signature files.

Smart Protection Network - Cloud Based Services

IWSVA's Smart Protection Network (SPN) is the industry's highest performing cloud-based malware protection service. Smart Protection Network has the following malware detection components:

- **Web Reputation Services (WRS)** is comprised of several correlated services that provide proactive detection and blocking against known bad web sites, domains, files and objects, as well as email related items - including anti-pharming and anti-phishing detection.
    - Domain reputation
    - Page reputation
    - Email reputation
    - File reputation
- **URL Filtering Service** stores its URL database in the cloud for rapid updates and protects Trend Micro's global user base without the need to download and update URL database files on the IWSVA server. This provides up-to-date URL information to every customer and accelerates the proactive protection capabilities to reduce the time between the discovery of a bad site and the time it is added to the URL database to protect all customers.
- **Feedback Loop** provides real-time information from all of Trend Micro's products to update the SPN cloud-based components and URL filtering databases. Malware detected on customer premise equipment are fed back into the cloud architecture and used to fine-tune information in real time. This provides fast proactive protection with low false positives to Trend Micro’s global customer base.

Best Practice Suggestions

Smart Protection Network (SPN) uses cloud-based services and relies on DNS queries for lookups. In order to ensure fast response and minimum latency, the IWSVA device must be configured with a primary and a secondary DNS server.

The DNS servers must be able to support the volume of DNS requests made by IWSVA. In general, before IWSVA builds up its local DNS cache, two DNS requests will be made for each URL accessed. Make sure your DNS server is installed on a server with enough resources and performance to handle the extra DNS volume.

Your DNS server should have a fast network card and be installed on a fast network switch to reduce latency.

Trend Micro recommends on-site DNS servers versus ISP provided DNS servers that are housed outside of the company's network. In general, ISP DNS servers have higher latency and do not support large numbers of DNS queries from a single IP address. Many ISP DNS servers have throttling mechanisms that limit the number of DNS requests per second and can affect IWSVA's Web Reputation Services (WRS) performance.

Try to place your DNS server as close to the IWSVA unit(s) as possible to eliminate unnecessary network hops between the devices to improve network response time and performance.

WRS and URL Filtering requests are made over HTTP port 80. Do not block the IWSVA management IP address for these ports on your firewall.

Local IWSVA Scan Engines

IWSVA provides local on-box scanning to ensure that content downloaded from the Internet is scanned for malware. Smart Protection Network's Web Reputation Service and URL Filtering services can filter a large percentage of the well-known and newly discovered malware sites and content, but local file scanning ensures that files and objects received are free of embedded viruses, worms, and other malicious code such as Trojans.

IWSVA provides the following local scan engines:

- **File Type Block** provides the ability to identify and block over 60 different file MIME types. These can include popular files such as Java applets, executable files, Microsoft Office documents, and so forth. See Mapping File Types to MIME Content-types on page B-1 for a detailed list of the supported file type.
- **Virus Scan (VSAPI)** provides signature based virus and malware scanning.

- **IntelliScan** provides the ability to identify and scan files based on their true file type, preventing users from trying to bypass the scan engines by changing the file extension or by some other form of file manipulation.
- **IntelliTrap** provides heuristics scanning to identify and protect against malware that changes or morphs from one state to another as it navigates through the network.
- **Compressed File Scanning** provides protection against malware that is hidden in highly-compressed files that are compressed many times over. Malware authors use this common delivery method to try and evade traditional anti-virus scanning software.
- **Spyware/Grayware Scanning** protects against spyware, dialers, hacking tools, password cracking applications, adware, joke programs, remote access tools, and other grayware types. This local scan engine provides protection based on spyware signatures and is used to compliment the Spyware URL category found in the URL Filtering feature. The local Spyware/Grayware scan engine is used to scan against files download or uploaded to the Internet that may be infected with spyware or grayware. Whereas the URL Filtering Spyware category is used to proactively block access to sites known to contain spyware related files and objects.
- **Applets and ActiveX Scanning** provides protection from malware embedded in Java applets and mobile code such as ActiveX applications found on many modern web sites.
- **Large File Scanning** provides administrators with a way to bypass scanning for large files that can consume a lot of system resources. Traditionally, malware authors do not embed viruses in large files because they want the malware to spread quickly without drawing a lot of attention to the file.

Best Practice Suggestions

- IWSVA's local scan services operate in a specific order to reduce the need to scan unnecessarily. IWSVA's scanning order for Internet traffic flows in the following order starting with the proactive Smart Protection Network's cloud-based services first.
  - Web Reputation Service (WRS)
  - URL Filtering Service
  - File Type Block
  - Virus Scan

  - IntelliTrap Heuristics
  - MacroTrap
  - IntelliScan True File Type
  - Applets and ActiveX
- The Virus Scan (VSAPI) scan engine consumes the most resources. Enabling Web Reputation (WRS) and subscribing to the URL Filtering service and enabling its Computer/Harmful category can greatly reduce the need to perform traditional VSAPI-based virus scans. Making these changes can reduce server resources and provide additional scalability for your environment.
- For trusted, approved-list sites and files that have a high integrity rating, you can disable malware scanning to improve performance and reduce server resource use. Use the Global Trusted URLs, Approved URL and Approved File lists in the Exception tabs to bypass scanning for trusted sites and files.
- You can configure large file scanning to skip scanning for files over a specific size. This can help reduce unnecessary scanning for larger files and lower resource use to improve capacity and performance.
- To improve user response time for larger file downloads, enable the Large File Handling's Deferred Scanning feature to "trickle" parts of the scanned file to the requesting host. This keeps the browser's file transfer status indicator alive and shows progress to the user while the file is scanned. If malware is found within the trickled file, IWSVA blocks the remainder of the file - resulting in an incomplete file that cannot be executed. For multi-media files or streaming content that uses HTTP port 80, such as YouTube content, you must enable Deferred Scanning to allow portions of the media to flow through. Selecting the "Scan Before Delivery" option blocks the streaming content until it is fully scanned and results in bad user experiences.
- For customers that need to scan the entire file before delivering it to their users, select the "Scan Before Delivery" option from the Large File Handling feature. This instructs IWSVA to buffer the file and completely scan it before delivering any portion to the user. This method is slightly slower in terms of end-user performance perception, but ensures that no portion of the infected file is allowed through.
- Keep in mind that entries placed in the Global Trusted URLs list are not scanned. If you want to scan approved list items, create an Approved List object and use this in the policy's Exception tab. The Exception Tab gives you the option of scanning approved list items in the HTTP and FTP Scan Policies.

Appendix F

WCCP Deployment & Troubleshooting

This appendix contains information about deploying and troubleshooting installation of the InterScan Web Security Virtual Appliance (IWSVA) working with Cisco's Web Cache Communication Protocol (WCCP.)

The topics include:

Introduction to WCCP

Cisco router and switches supporting Web Cache Communication Protocol (WCCP) can redirect traffic to one or more transparent proxy web cache servers. Web caches reduce network latency by enabling end users to retrieve web pages that they have accessed previously from a memory buffer or "cache" instead of from a web server.

Cisco created WCCP to control the interaction of external web cache devices with Adaptive Security Appliances. WCCP not only reduces the load on web cache devices, but it also provides load balancing and support for multiple routers and protocols. WCCP is transparent to the end user and requires no modification to the endpoint devices.

IWSVA and WCCP Overview

This appendix describes how to configure IWSVA to run in WCCP mode and communicate with a Cisco WCCP enabled device in an N-tier environment. When an IWSVA is running in WCCP mode and integrates with a Cisco WCCP device, it becomes a "web cache" even though it does not specifically serve cached content. Instead it serves as a "cache engine" for the ASA and performs web gateway functions for filtering and scanning web content.

Examples used throughout this document illustrate the configuration steps required on the IWSVA and the Cisco WCCP supported devices. Although Trend Micro cannot test and validate every Cisco device that supports WCCP, testing is performed on every IWSVA version with WCCP.

Note: IWSVA's WCCP implementation defaults to WCCP service 80 and the Dynamic WCCP service type and this is compatible for most WCCP v2 implementations. However, if your Cisco device is using a different WCCP service number other than 80 or is using the Standard WCCP service method, you will need to change the IWSVA's WCCP parameters to match. Please refer to the Additional IWSVA Tips on page F-15 for more information on how to change IWSVA's WCCP service parameters.

Examples used in this document were created with IWSVA and the following Cisco products:

- Cisco 2821 router running IOS version 12.4(13r)T
- Cisco 3750 switch running IOS version 12.2(40)SE
- Cisco ASA 5510 running version 8.4(35)k8

Deploying WCCP on Cisco 2821 Routers

Known issues and deployment requirements for Cisco routers include:

1. Cisco IOS versions 12.2(23) through 12.3(9) have been known to have WCCP connectivity issues. These versions should be avoided with IWSVA integration.
2. The router ID that is automatically selected is the highest IP address configured on the Cisco router. If the interface supporting this IP address is not directly accessible by the IWSVA device, the WCCP L2 redirection method will not function. In this case, you will need to ensure that proper route entries are configured and enabled on your routers and switches to allow IWSVA to communicate with the interface configured with the Router ID.

Deployment Example

This example uses a Cisco 2821 router running IOS 12.4(13r)T with two network segments - a private network and a public facing DMZ network.

- **Private Network**—192.168.1.0/24 - Supported on the Cisco's GigiabitEthernet 0/0 interface with 192.168.1.1 as the gateway address.
- **DMZ Network**—172.16.1.0/24 - Supported on the Cisco's GigiabitEthernet 0/1 interface with 172.16.1.5 as the gateway address.
- **IWSVA Device**—172.16.1.101 - Acts as the WCCP cache device and performs content scanning and filtering.

The private network hosts the company's client computers and the DMZ network houses the public facing servers (web, FTP, etc) and the IWSVA unit. IWSVA can access the Internet through the corporate firewall as illustrated in *Figure F-1*.

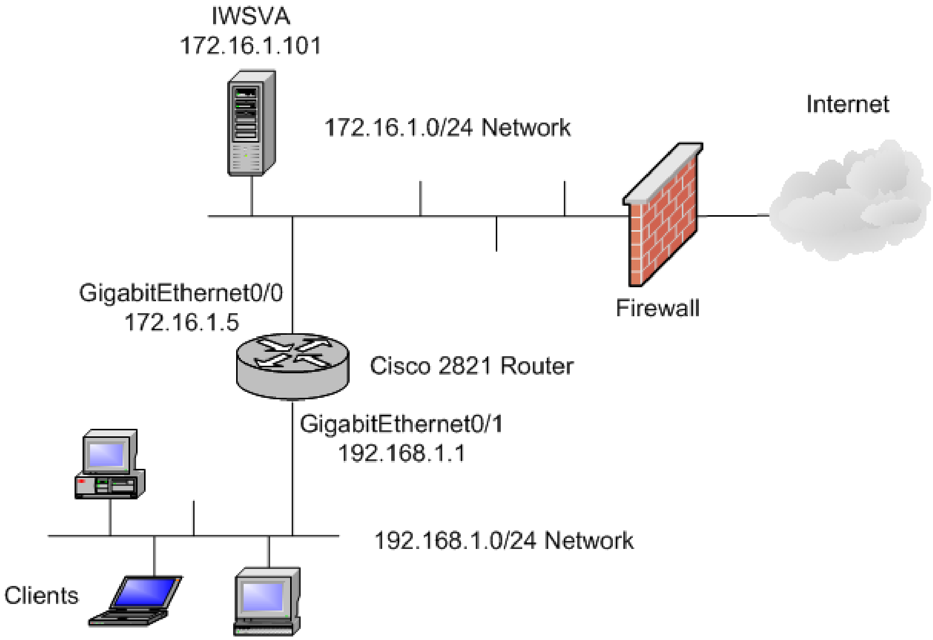


FIGURE F-1. Example Topology for Cisco 2821 Router Implementation

Configuring the Cisco 2821 Router

Log into the Cisco router with administrative permissions and perform the following configuration steps.

To configure the Cisco 2821 router:

1. Enter the Cisco router's terminal configuration mode.

```
Hostname#conf t

Hostname(config)#
```

2. Configure a redirect-list containing the client protocol(s) to be redirected to the IWSVA unit. In this example, the HTTP WWW and FTP protocols are redirected for scanning. The access-list number used in this example is 101. But this number can be different for your environment.

   ```
   Hostname (config)# access-list 101 permit tcp 192.168.1.0
   0.0.0.255 any eq www
   ```

   ```
   Hostname (config)# access-list 101 permit tcp 192.168.1.0
   0.0.0.255 any eq ftp
   ```

3. Configure a group-list containing all members of the WCCP server. In this example, we configured a group-list with the IWSVA member. WCCP forwards the protocols selected in the previous step to the IWSVA identified in this group-list. The access-list number used in this example is 22. This number can be different for your environment.

   ```
   Hostname (config)# access-list 22 permit 172.16.1.101
   0.0.0.1
   ```

4. Enable WCCP on the Cisco router. The WCCP service number used in this example is 80. By default, IWSVA always uses service number 80 with the Dynamic WCCP service. If you are using Cisco IOS 12.2 or 12.3, the WCCP version defaults to 2. In these cases, it is not necessary to configure the WCCP version. Please make sure your Cisco device is configured for the same values. The password used in this example is set to “novirus” and it must match the password configured on the IWSVA's WCCP configuration settings.

   ```
   Hostname (config)# ip wccp 80 redirect-list 101 group-list
   22 password novirus
   ```

5. Enable WCCP Outbound redirection on the interface that allows traffic to reach the public Internet. This interface does not need to be the interface where you have installed your cache device - the IWSVA in this example. In this example, the public Internet facing interface is 0/0, and the WCCP redirection is enabled as OUT on this router interface.

   ```
   Hostname (config)# interface GigabitEthernet0/0
   ```

   ```
   Hostname (config-if)# ip wccp 80 redirect out
   ```

6. Enable WCCP Inbound redirection on the interface that will be receiving traffic from the client devices. In this example, the client facing interface is 0/1 and we will enable the WCCP redirection as IN on this router interface.

   ```
   Hostname (config)# interface GigabitEthernet0/1
   ```

   ```
   Hostname (config-if)# ip wccp 80 redirect in
   ```

   Cisco 2821 routers can support GRE and the L2 forwarding methods as well as both Hash and Mask assignment methods. In the above example, the L2 forwarding method was selected along with the Mask assignment method for better performance.

Deploying WCCP on Cisco 3750 Switches

Known issues and deployment requirements for Cisco switches include:

1. Cisco IOS versions 12.2(23) through 12.3(9) have been known to have WCCP connectivity issues. These versions should be avoided with IWSVA integration.
2. WCCP entries and PBR entries use the same TCAM region. WCCP is supported only on the templates that support PBR: access, routing, and dual IPv4/v6 routing. As a result, for switches (like the 3750, 3560 series) to support WCCP, the SDM template needs to be changed to something other than "default." When TCAM entries are not available to add WCCP entries, packets are not redirected and are forwarded by using the standard routing tables.
3. The IWSVAs must be directly connected to the switch that has WCCP enabled. They should be in the same subnetwork.
4. Configure the switch interfaces that are connected to the web clients, IWSVAs, and the web server as Layer 3 interfaces (routed ports and switch virtual interfaces [SVIs]). For WCCP packet redirection to work, the servers, IWSVAs, and clients must be on different subnets.
5. Check the supported forward and assignment method by the switch, and make sure these two settings are correct in IWSVA. For example, 3560 and 3750 series just support L2 forwarding method and Mask assignment method.
6. You cannot configure WCCP and VPN routing/forwarding (VRF) on the same switch interface.
7. You cannot configure WCCP and PBR on the same switch interface.

8. You cannot configure WCCP and a private VLAN (PVLAN) on the same switch interface.

Deployment Example

This example uses a Cisco 3750 switch running IOS 12.2(40)SE with two VLAN network segments - VLAN 30 and VLAN 160.

- **VLAN 30 Network**—10.168.30.0/24 - Supports the clients on the corporate network. This VLAN has 10.168.30.254 as the gateway address.
- **VLAN 160 Network**—10.168.160.0/24 - Supports the IWSVA and other servers and has access to the public Internet through the corporate firewall. This VLAN has 10.168.160.254 as the gateway address
- **IWSVA Device**—10.168.160.54 - Acts as the WCCP cache device and performs content scanning and filtering.

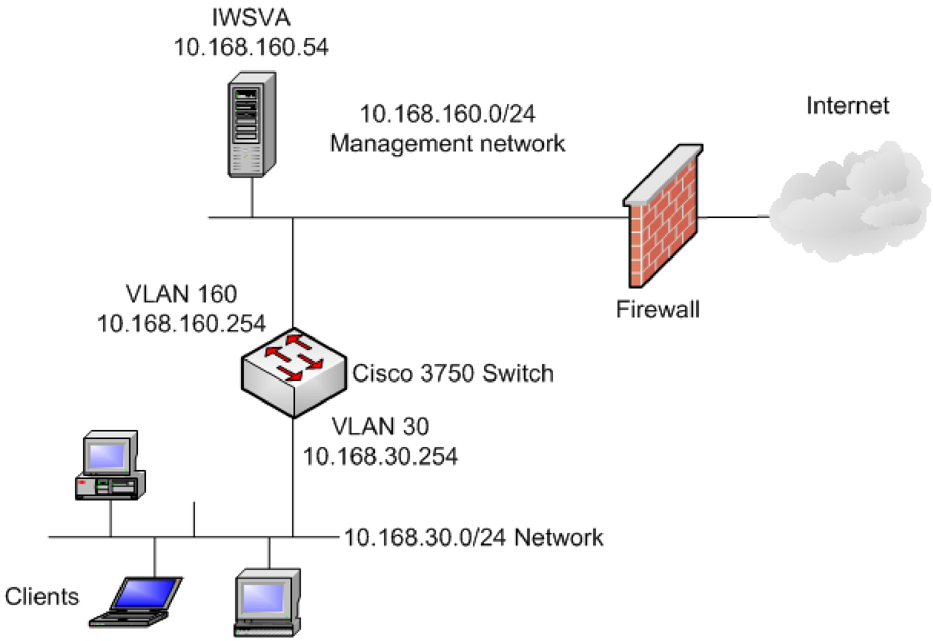


FIGURE F-2. Example Topology for Cisco 3750 Switch Implementation

Configuring the Cisco 3750 Switch

Log into the Cisco 3750 switch with administrative permissions and perform the following configuration steps.

To configure the Cisco 3750 switch:

1. Enter the Cisco switch's terminal configuration mode.

   ```
   Switch #conf t
   ```

   ```
   Switch(config)#
   ```

2. Configure an access-list containing the client VLAN(s) to be redirected to the IWSVA unit. In this example, we will redirect the 10.168.30.0/24 client subnet. The access-list used is the standard list and the WCCP80 is the identifier for this ACL. It can be different in your environment to match your naming conventions.

   ```
   Switch (config)# ip access-list standard wccp80 permit
   10.168.30.0 0.0.0.255
   ```

3. Configure a group-list containing all members for the WCCP cache. In this example, a group-list is configured with the IWSVA device's 10.168.160.54 IP address. The IWSVA device handles the inbound redirection where WCCP will forward the traffic you selected in the previous step. The group80 is the identifier for this ACL and it can be different in your environment to match your naming conventions.

   ```
   Switch (config)# ip access-list standard  group80 permit
   host 10.168.160.54
   ```

4. Enable WCCP on the Cisco switch. The WCCP service number used in this example is 80. By default, IWSVA uses service number 80 with the Dynamic service type. Please make sure your Cisco device is configured for the same values. The password used in this example is set to “novirus” and it must match the password configured on the IWSVA's WCCP configuration settings.

   ```
   Switch (config)# ip wccp 80 redirect-list wccp80 group-list
   group80 password novirus
   ```

5. Enable WCCP inbound redirection on the VLAN interface that is connected to the clients. The client side interface must be a different VLAN (subnet) from the IWSVA and the web server VLAN(s) - otherwise, proper WCCP redirection will

fail. In this example, the client side subnet is VLAN30 and the IWSVA server side subnet is VLAN160.

```
Switch (config)# interface vlan 30

Switch (config-if)# ip wccp 80 redirect in
```

6. On the IWSVA device's Web UI for WCCP configuration, make sure that the L2 forwarding method and the Mask assignment method are selected. For Cisco 3750 switches, this is the only supported configuration for these two parameters.

Deploying WCCP on Cisco ASA Devices

Known issues and deployment requirements for Cisco ASA devices include:

1. The Cisco ASA must be running version 7.2.1 or higher in order to support WCCP. Avoid using version 7.2(2) as this is known to have compatibility issues with IWSVA.
2. The Cisco ASA only supports a topology where the clients and the IWSVA device are on the same internal interface of the ASA device. This allows IWSVA to communicate directly with the client hosts without needing to go through the ASA device.
3. The Router ID that is automatically selected is the highest IP address configured on the Cisco ASA. If the Router ID happens to be on an interface that is external to the IWSVA device, such as on the DMZ interface or the external Internet facing interface, the proper routes must be defined on all necessary routing and switching devices to allow IWSVA access to the Router ID's IP address.

Deployment Example

This example uses a Cisco ASA 5510 running software version 8.4(35)k8 with two network segments—an internal and external network.

- **Internal Network**—192.168.1.0/24 - Supports the internal network where the clients reside. The internal network also houses the IWSVA device. 192.168.1.1 is the gateway address defined on the ASA's 0/1 interface.

- **External Network**—172.16.12.0/24 - Supports the external network and the path to the public Internet. 172.16.12.1 is the gateway address defined on the ASA's 0/0 interface.
- IWSVA Device—192.168.6.10 - Acts as the WCCP Cache device and performs content scanning and filtering.

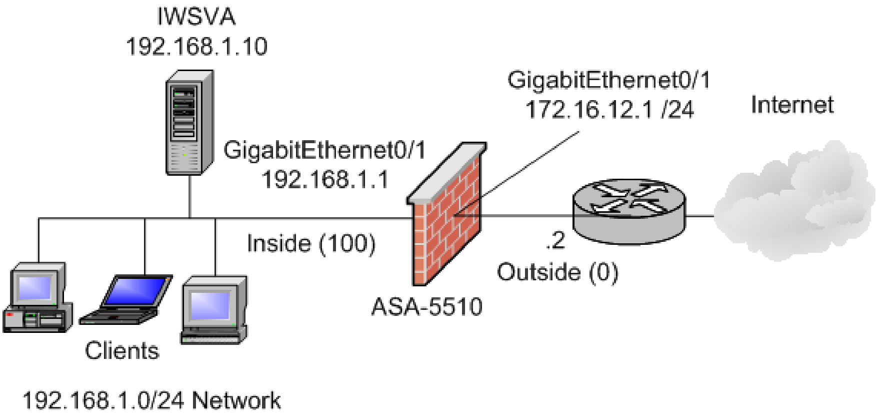


FIGURE F-3. Example topology for Cisco ASA implementation

Configuring the Cisco ASA

Log into the Cisco ASA with administrative permissions and perform the following configuration steps.

To configure the Cisco ASA:

1. Enter the Cisco ASA's terminal configuration mode.

```
ASA #conf t
```

```
ASA(config)#
```

2. Configure an access-list containing the WCCP server member(s). In our example, there is only one WCCP server which is the IWSVA device.

```
ASA (config)# access-list wccp-servers permit ip host
192.168.1.10 any
```

3. Create an access-list to allow the ASA to redirect traffic to the cache server. In our example, the 192.168.1.0/24 subnet will be redirected to the IWSVA acting as the cache server.

   ```
   ASA (config)# access-list wccp-traffic permit ip 192.168.1.0
   255.255.255.0 any
   ```

4. Configure WCCP to redirect traffic from the “wccp-traffic” filter to the “wccp-servers” device. The password used in this example is set to “novirus” and it must match the password configured on the IWSVA's WCCP configuration settings.

   ```
   ASA (config)# wccp web-cache group-list wccp-servers
   redirect-list wccp-traffic password novirus
   ```

5. Enable WCCP inbound redirection on the internal client interface. In this example, the internal client interface is called “inside”. The standard service is “web-cache” (service group id 0), which intercepts TCP port 80 (HTTP) traffic and redirects it to the cache servers.

   ```
   ASA (config)# wccp interface inside web-cache redirect in
   ```

   In this example, the GRE forwarding method and the Hash assignment were selected in the IWSVA device's WCCP configuration Web UI screen.

Configuring IWSVA with WCCP Deployment Mode

WCCP is supported on all versions of IWSVA. The configuration steps are very similar between each IWSVA version and this document will highlight the installation procedure with IWSVA.

The minor differences between IWSS and IWSVA WCCP deployments include the following:

- **Forward Method**—The IWSVA products support both GRE and L2 forwarding methods. Generally, the L2 forward method can achieve better performance over GRE, but it depends on the network topology and the Cisco device. For example, Cisco routers supporting WCCP version 1 cannot use the L2 forward method.

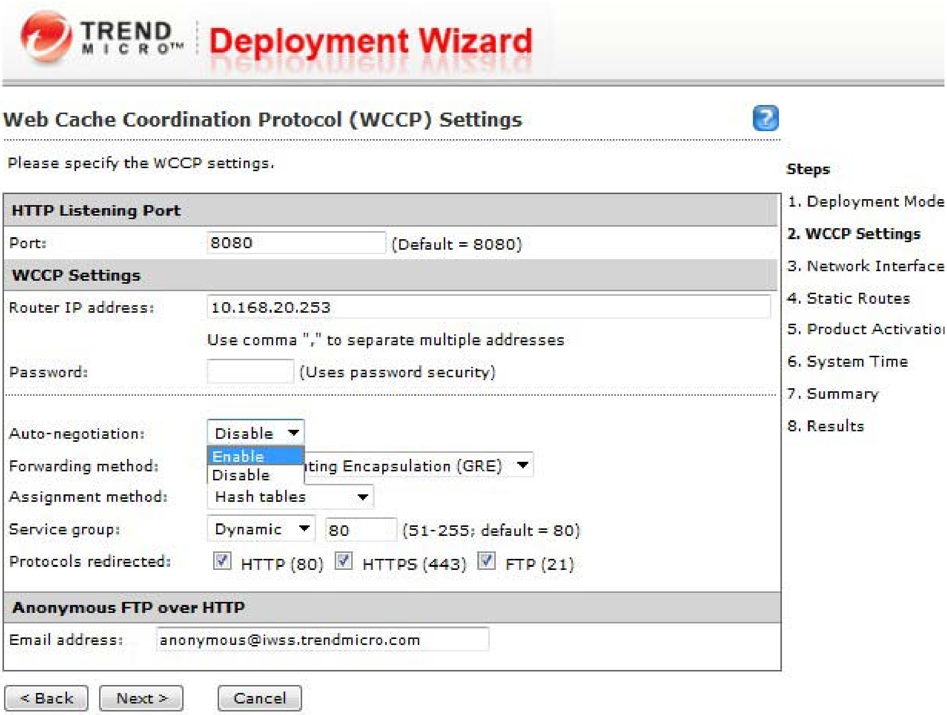
- **Router IP Address**—The Router ID of WCCP service group can have an effect on the topology design. The Router ID is treated as an IPv4 address and can also be used as the source address of any WCCP-generated GRE frames. When the GRE forward method is configured, IWSVA will use the Router ID as the source IP address of the GRE packets.

  Most Cisco routers do not allow the re-configuration of the Router ID. Cisco routers automate the selection of the Router ID by leveraging the highest reachable IPv4 address defined on the router. However, this IP address may not be the best choice when it comes to the WCCP Router ID and customers must ensure that their networking devices' route tables are updated accordingly to allow communications between the Router ID's IP address and the IWSVA device.
- **Assignment Method**—With WCCP, either the Hash or Mask assignment method can be used. The Mask assignment method is only supported with IOS versions supporting WCCP version 2. The IWSS products only support the Hash assignment method while the IWSVA products can support both the Hash and the Mask assignment methods.

Configuring WCCP on IWSVA Device

Depending on the version of IWSVA used, the WCCP configuration is done in the Deployment Wizard or in the HTTP configurations under the Proxy Deployment (older versions). The examples in this installation primer will use IWSVA to illustrate the WCCP configuration steps.

Figure 4 shows the WCCP parameters and gives an explanation of each WCCP parameter required for a basic WCCP v2 deployment with the default WCCP service 80 and Dynamic service type.



Web Cache Coordination Protocol (WCCP) Settings

Please specify the WCCP settings.

HTTP Listening Port

Port: 8080 (Default = 8080)

WCCP Settings

Router IP address: 10.168.20.253

Use comma "," to separate multiple addresses

Password: (Uses password security)

Auto-negotiation: Disable

Enable
Disable

Forwarding method: ting Encapsulation (GRE)

Assignment method: Hash tables

Service group: Dynamic 80 (51-255; default = 80)

Protocols redirected: ☑ HTTP (80) ☑ HTTPS (443) ☑ FTP (21)

Anonymous FTP over HTTP

Email address: anonymous@iwss.trendmicro.com

FIGURE F-4. IWSVA's Deployment Wizard WCCP Settings Screen

See *Table F-1* for the WCCP settings and descriptions.

TABLE F-1. WCCP Settings

PARAMETER	DESCRIPTION
Router IP address	Enter the Cisco device(s) IP addresses for the interfaces that will be redirecting traffic to the IWSVA devices for scanning and URL filtering. Multiple Cisco device IP addresses are entered and separated by commas.
Password	Used if the Cisco routers were configured with a security password for WCCP. Passwords must match between IWSVA and the Cisco device.
Forwarding Method	The WCCP forwarding methods supported are GRE and Layer2 (L2). This setting must match the forwarding type provided by the Cisco device. Generally, L2 forwarding provides slightly better performance, but is not routable and requires the clients and the IWSVA to be on the same subnet/VLAN
Assignment Method	The Mask assignment method used for the WCCP protocol. Hash table and Mask value sets are supported and the assignment method selected should match the Cisco device's abilities. Check your Cisco device's IOS version for more information on the assignment methods supported.
Service Group	The service group can be set for Standard or Dynamic and the default service group ID is 80. Change this value to match your Cisco device's service group settings.
Redirected Protocols	The protocols that are redirected from the Cisco device to the IWSVA for content scanning. Options include HTTP (80), HTTPS (443), and FTP (21).

Additional IWSVA Tips

Cisco's WCCP is a proprietary redirection technology that is unique to Cisco routers and switches. As such, its implementation can vary slightly between IOS versions running on different devices and this may require further fine tuning on the IWSVA device. This section discusses a few examples where additional fine tuning may be required to fully achieve compatibility.

IWSVA's WCCP Configuration File

IWSVA stores its WCCP configuration in the IWSSPIProtocolHttpProxy.pni file under the `/var/iwss` directory and is used by the WCCP daemon. If you need to change any WCCP parameters that are not exposed on the IWSVA WCCP web UI configuration screen, this is the configuration file you will need to modify. Trend Micro recommends configuring the WCCP function from the IWSVA Web UI under normal circumstances and only manually making changes to the `IWSSPIProtocolHttpProxy.pni` file when absolutely necessary.

Trend Micro highly recommends that you make a copy of the file beforehand. You can use the "cp" copy command to backup the file:

```
cp IWSSPIProtocolHttpProxy.pni IWSSPIProtocolHttProxy.pni_backup
```

The file can be opened and changed with an editor such as "vi". If you are new to the vi editor, you can obtain more information on its commands from any of the following web sites:

http://www.eng.hawaii.edu/Tutor/vi.html

http://www.cs.rit.edu/~cslab/vi.html

http://www.cs.colostate.edu/helpdocs/vi.html

Whenever changes are made, the file must be saved and the WCCP daemon must be restarted to activate the new changes. Restart the WCCP server daemon with the following commands:

```
/usr/iwss/S99ISWCCPd stop

/usr/iwss/S99ISWCCPd start
```

The following WCCP parameters can be manually changed from the `IWSSPIProtocolHttpProxy.pni` configuration file.

```
# Name: wccp_router
# Type: address
# Default:
# Description
# Please put one to eight IP Addresses of Cisco routers that you
# will register your IWSx to.
# Example: wccp_router=192.168.1.254,192.168.2.254
wccp_router=

# Name: wccp_address
# Type: address
# Default:
# Description
# Use this option if you require WCCP to use a specific interface
address.
# The default behavior is to not bind to any specific address.
# Example: wccp_address=192.168.1.1
wccp_address=

# NAME: wccp_forwarding_method
# TYPE: int
# DEFAULT: 1
# Description:
# WCCP2 allows the setting of forwarding methods between the
# router/switch and the cache.  Valid values are as follows:
# 1 - GRE encapsulation (forward the packet in a GRE/WCCP tunnel)
# 2 - L2 redirect (forward the packet using Layer 2/MAC rewriting)
wccp_forwarding_method=1

# NAME: wccp_return_method
# TYPE: int
# DEFAULT: 1
# Description:
# This field is reserved for the future. Any change to the value
will take
# no effect.
wccp_return_method=1
```

```
# NAME: wccp_assignment_method
# TYPE: int
# DEFAULT: 2
# Description:
# Cisco assignment method, 1 is Hash, 2 is Mask.
wccp_assignment_method=2

#wccp_std_service=standard 0
#wccp_dynamic_service=dynamic 80

# NAME: wccp_service
# TYPE: wccp_service
# DEFAULT:
# Description:
# Dynamic WCCPv2 services require further information to define the
# traffic you wish to have diverted.
# The format is:
#
#       wccp_service <id> protocol=<protocol> flags=<flag>,<flag>..
#           priority=<priority> ports=<port>,<port>..
#
#       The relevant WCCPv2 flags:
#       + src_ip_hash, dst_ip_hash
#       + source_port_hash, dest_port_hash
#       + src_ip_alt_hash, dst_ip_alt_hash
#       + src_port_alt_hash, dst_port_alt_hash
#       + ports_source, ports_defined
#
#       The port list can be one to eight entries.
wccp_service=dynamic 80 protocol=tcp flags=src_ip_hash priority=120
ports=80,21,443

# NAME: wccp_service_info
# TYPE: wccp_service_info
# DEFAULT:
# Description:
# Dynamic WCCPv2 services require further information to define the
# traffic you wish to have diverted.
# The format is:
#
#  wccp_service_info <id> protocol=<protocol> flags=<flag>,<flag>..
#           priority=<priority> ports=<port>,<port>..
#
#       The relevant WCCPv2 flags:
#       + src_ip_hash, dst_ip_hash
#       + source_port_hash, dest_port_hash
#       + src_ip_alt_hash, dst_ip_alt_hash
#       + src_port_alt_hash, dst_port_alt_hash
#       + ports_source, ports_defined
#
#       The port list can be one to eight entries.

# wccp_service_info=80 protocol=tcp flags=source_port_hash,
src_port_alt_hash priority=120 ports=80,21,443

# NAME: wccp_password
# TYPE: cyphered text
# DEFAULT:
# Description:
# MD5 service authentication can be enabled by setting
# wccp_password=<cyphered password>.
# Please note that the user should not modify this field manually.
# When the user set the password on the WebUI, the UI will use the
# encrypt the password with MD5 and save it in the configuration
file
wccp_password=

wccp_logging=0
#       0 - off, no WCCP log, error only
#       1 - on (default), write WCCP log to http.log file
```

Changing the Default WCCP Service

By default, IWSVA is setup to use WCCP service 80 and the Dynamic service type. This works well in many WCCP v2 environments, but may require modification if these values are changed on the Cisco device.

To change from the default WCCP service values:

1. Log into the IWSVA's console using the "root" level user for full administrative rights.
2. Navigate to the `/etc/iscan` directory with the **`cd /etc/iscan`** command.
3. Open the `intscan.ini` for editing. For example, you can use the **`vi intscan.ini`** command.
4. Search for the "`wccp_service`" parameter by typing **`/wccp_service`** and pressing **Enter**. The system should show the WCCP settings similar to the following. Note the default service type and number is "dynamic 80".

```
wccp_service=dynamic 80 protocol=tcp flags=src_ip_hash priority=120
      ports=80,21,443,8080
```

5. Change the `wccp_std=dynamic 80` to the new value supported by your Cisco device. For example, change it from Dynamic 80 to Standard 0 as shown in the example below. You will need to place the vi editor into insert mode with **`i`** before you can make the change.

```
wccp_std_service=standard 0 protocol=tcp flags=src_ip_hash
priority=120 ports=80
```

6. Exit the insert mode by pressing the **Esc** key. Type **`:wq`** to write and quit.
7. Restart the WCCP Server Daemon with the following commands:

```
/usr/iwss/S99ISWCCPd stop

/usr/iwss/S99ISWCCPd start
```

Note: If the Standard 0 service is used, the Cisco device can only redirect the HTTP port 80 traffic to the IWSVA device. If the Dynamic service is used, the Cisco device can redirect other ports in addition to port 80. For example, ports 80, 21, 443, and 8080 can be supported under the Dynamic service.

Advanced Concepts: Deploying WCCP for Redundancy and Fault Tolerance

There are numerous ways IWSVA can be deployed in WCCP mode. In larger environments where scalability and redundancy are desired, multiple IWSVA's can be deployed with multiple Cisco routers for load balancing and fault tolerance with WCCP version 2.

Figure 5 illustrates an example with a redundant architecture that leverages multiple IWSVA devices and multiple WCCP version 2 capable routers.

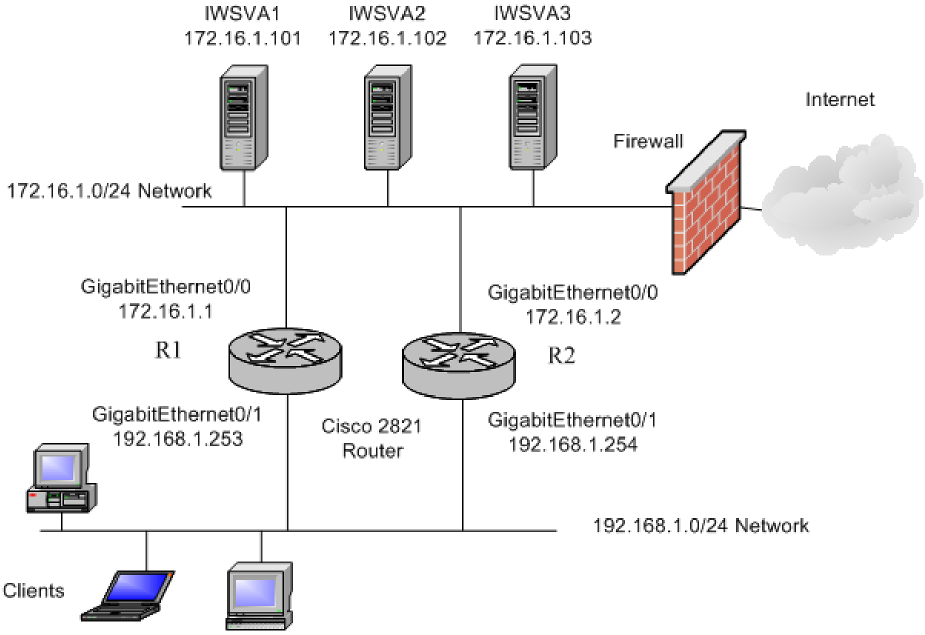


FIGURE F-5. IWSVA and Cisco Routers Deployed in High Availability Configurations

In this example, two Cisco 2821 routers running IOS 12.4(13r)T are used to redirect traffic to three IWSVA devices for URL filtering and content scanning. This customer desires load balancing across all three IWSVA devices and fault tolerance in case one of the IWSVA's is brought down. This design allows the remaining IWSVA devices to pick up the extra load so traffic processing is uninterrupted. If one of the Cisco routers is taken off line, the remaining router will automatically pick up the load and continue the traffic distribution across the IWSVA devices.

Configuring the Cisco Routers

The configuration steps and commands are similar to the Cisco 2821 router example. The completed router configurations are illustrated below for reference.

Cisco Router One

The following configuration demonstrates how WCCP is configured and enabled on the first Cisco router. The L2 Forward method and Mask assignment method are used in this example and WCCP version 2 is supported by the router's IOS version.

```
!
ip access-list standard wccp80
permit 192.168.1.0 0.0.0.255
!
ip access-list standard wccp-servers
 permit 172.16.1.101
 permit 172.16.1.102
 permit 172.16.1.103
!
ip wccp 80 redirect-list wccp80 group-list wccp-servers
!
interface GigabitEthernet0/1
ip wccp 80 redirect in
!
```

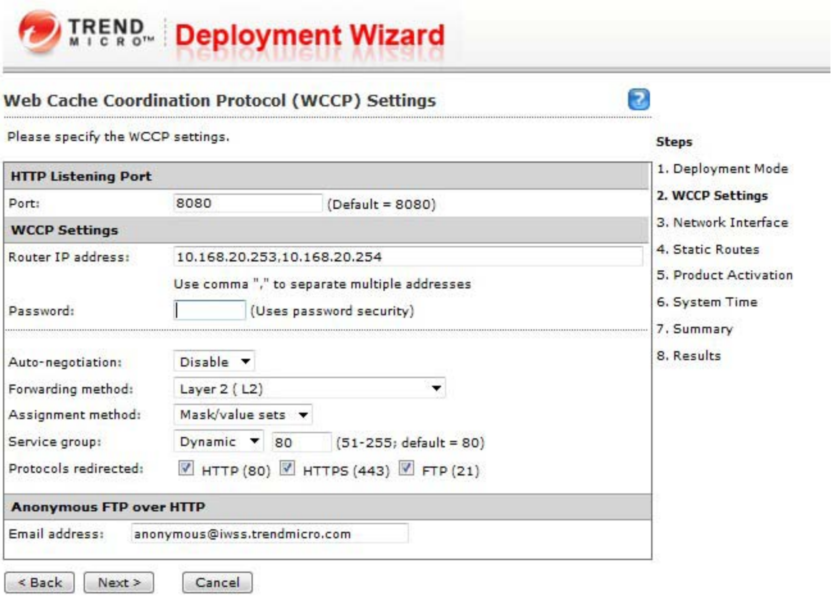
Cisco Router Two

The following configuration demonstrates how WCCP is configured and enabled on the second Cisco router. The L2 Forward method and Mask assignment method are used in this example and WCCP version 2 is supported by the router's IOS version.

```
!
ip access-list standard wccp80
permit 192.168.1.0 0.0.0.255
!
ip access-list standard wccp-servers
 permit 172.16.1.101
 permit 172.16.1.102
 permit 172.16.1.103
!
ip wccp 80 redirect-list wccp80 group-list wccp-servers
!
interface GigabitEthernet0/1
ip wccp 80 redirect in
!
```

Configuring the IWSVA Device

For this example, the three IWSVA devices are configured with the same WCCP settings. *Figure F-6* illustrates the configuration values for the WCCP settings.



Web Cache Coordination Protocol (WCCP) Settings

Please specify the WCCP settings.

HTTP Listening Port

Port: 8080 (Default = 8080)

WCCP Settings

Router IP address: 10.168.20.253,10.168.20.254

Use comma "," to separate multiple addresses

Password: (Uses password security)

Auto-negotiation: Disable

Forwarding method: Layer 2 (L2)

Assignment method: Mask/value sets

Service group: Dynamic 80 (51-255; default = 80)

Protocols redirected: ☑ HTTP (80) ☑ HTTPS (443) ☑ FTP (21)

Anonymous FTP over HTTP

Email address: anonymous@iwss.trendmicro.com

Steps
1. Deployment Mode
2. WCCP Settings
3. Network Interface
4. Static Routes
5. Product Activation
6. System Time
7. Summary
8. Results

FIGURE F-6. IWSVA's WCCP Settings Screen

In this example, the two Cisco routers' IP addresses were entered in the Router IP Address(es) field and separated by a comma. The L2 forwarding method and the Mask assignment method were selected.

Troubleshooting Cisco WCCP & IWSVA

In order to properly troubleshoot your WCCP environment, verbose logging (debug mode) of the WCCP event information may be required on the IWSVA and/or Cisco device. By default, the verbose logging is disabled. If you run into problems that you cannot solve by using this guide, contact Trend Micro's technical support team for further assistance. They may instruct you to enable verbose/debug logging on the IWSVA and/or Cisco devices to collect the necessary troubleshooting information.

Note: Running IWSVA and/or the Cisco device in debug or verbose logging modes will add latency as the product may be required to capture large amounts of data for debug purposes. You should only enable these verbose logging modes at the request of the Trend Micro technical support representative.

Enabling IWSVA's WCCP Event Logging

To enable IWSVA's WCCP logging feature:

1. Log into the IWSVA console as the "root" user.
2. Navigate to the `/var/iwss` directory by typing **`cd /var/iwss`**.
3. Open the `IWSSPIProtocolHttProxy.pni` file with an editor such as vi. For vi, type **`vi IWSSPIProtocolHttProxy.pni`**.
4. Search the file for the "wccp_logging" parameter by typing **`/wccp_logging`**.
5. Type **`i`** to put the vi editor into insert mode and change the value from 0 to **1**. This enables the IWSVA's WCCP logging function.

```
wccp_logging=1

#       0 - off, no WCCP log, error only

#       1 - on (default), write WCCP log to http.log file
```

6. Exit the insert mode with the **Esc** key and type **`:wq`** to write the file and quit the vi editor.

   The WCCP events will be saved in the HTTP log files under the `/etc/iscan/log` directory on the IWSVA device. The log files will be saved under a format that lists the date and time of the file's creation, such as: `http.log.20110325.0001`

   You can navigate to this directory and use an editor such as vi to open and view the file.

Enabling Cisco Device's WCCP Event Logging

Depending on the Cisco device you are using, how you enable the WCCP event log may be different than what is shown in this installation primer. For our example, a Cisco ASA router was use. Please refer to your Cisco router or switch's administration guide.

To enable the WCCP event logging on a Cisco device:

1. Log into the Cisco device's console using an administrative account that has configuration rights.
2. Enter the `config` mode and type the command to enable the WCCP event debug function.

   ```
   Router (config) # debug wccp event
   ```

Starting the Troubleshooting Process

If the WCCP enabled devices are not forwarding traffic to the IWSVA devices for scanning, the first thing to check is the communications between the Cisco and IWSVA devices. This section describes the various commands used in troubleshooting the communications between the Cisco device and the IWSVA acting as the cache device.

Several helpful commands provided by the Cisco device that can help verify the configuration and setup of your Cisco device includes the following.

- `show ip wccp <service id>`
- `show ip wccp <service id> view`
- `debug ip wccp event`
- `debug ip wccp packet`

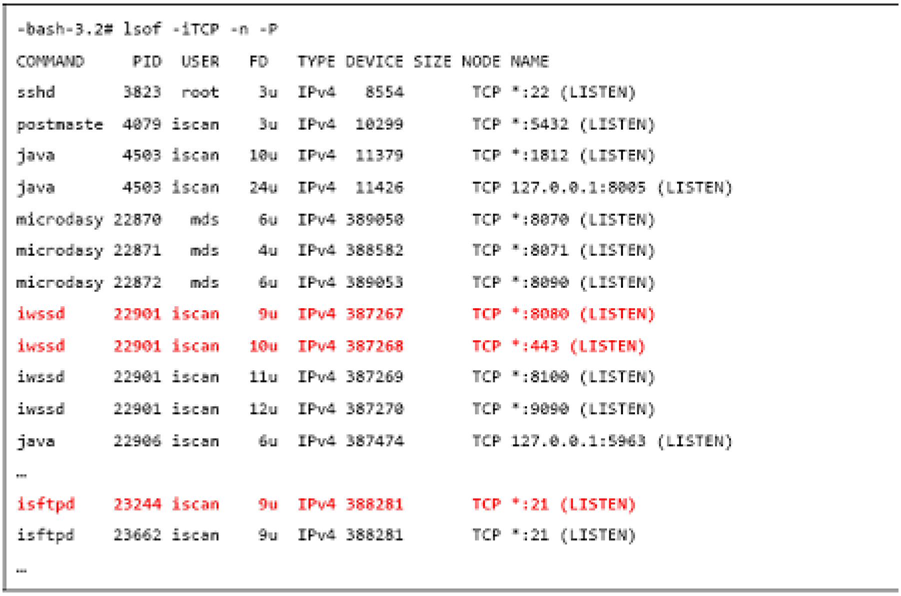
Note: The commands listed in this troubleshooting section may vary slightly between Cisco device types. The commands illustrated in this section are suited to the Cisco routing and switching devices used throughout this guide. For Cisco ASA devices, the commands vary slightly. Please refer to your Cisco administration guide for more details on these troubleshooting commands.

Checking the IWSVA Configuration

On the IWSVA device, check the following configuration parameters to ensure that communications is being performed properly on the IWSVA device.

To check the IWSVA configuration:

1. Verify that the password set for the IWSVA WCCP password parameter matches the password on the WCCP device. If the passwords are not the same, no communications between the devices can occur.
2. If the passwords match, make sure the IWSVA Scan Daemons (services) are functioning properly.
   a. On the IWSVA console, log in as the "root" user.
   b. Use the **`lsof -iTCP -n -P`** command to list the daemons and look for the **`iwssd`** and **`isftpd`** daemons to make sure they are in "LISTEN" mode



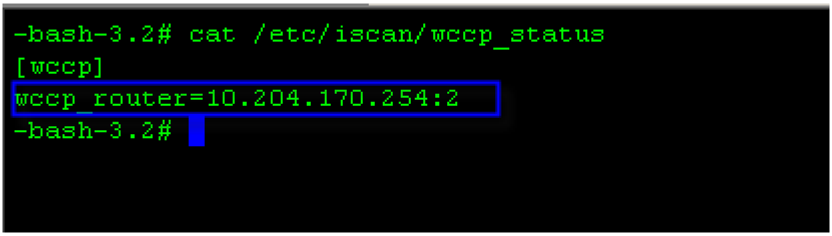
```
-bash-3.2# lsof -iTCP -n -P
COMMAND      PID  USER    FD   TYPE DEVICE SIZE NODE NAME
sshd        3823  root    3u   IPv4   8554        TCP *:22 (LISTEN)
postmaste   4079 iscan    3u   IPv4  10299        TCP *:5432 (LISTEN)
java        4503 iscan   10u   IPv4  11379        TCP *:1812 (LISTEN)
java        4503 iscan   24u   IPv4  11426        TCP 127.0.0.1:8005 (LISTEN)
microdasy 22870    mds    6u   IPv4 389050        TCP *:8070 (LISTEN)
microdasy 22871    mds    4u   IPv4 388582        TCP *:8071 (LISTEN)
microdasy 22872    mds    6u   IPv4 389053        TCP *:8090 (LISTEN)
iwssd      22901 iscan    9u   IPv4 387267        TCP *:8080 (LISTEN)
iwssd      22901 iscan   10u   IPv4 387268        TCP *:443 (LISTEN)
iwssd      22901 iscan   11u   IPv4 387269        TCP *:8100 (LISTEN)
iwssd      22901 iscan   12u   IPv4 387270        TCP *:9090 (LISTEN)
java       22906 iscan    6u   IPv4 387474        TCP 127.0.0.1:5963 (LISTEN)
…
isftpd     23244 iscan    9u   IPv4 388281        TCP *:21 (LISTEN)
isftpd     23662 iscan    9u   IPv4 388281        TCP *:21 (LISTEN)
…
```

FIGURE F-7. Daemon list showing iwssd and isftpd

3. Check the IWSVA's WCCP control connection to make sure it is running correctly.

a. On the IWSVA console, login as the “root” user.

b. Check the status value in the `/etc/iscan/wccp_status` file. If the status is set to **`2`** and the WCCP Server Daemon is running, the control connection is good. The **`cat`** command can be used to open and view the file.



```
-bash-3.2# cat /etc/iscan/wccp_status
[wccp]
wccp_router=10.204.170.254:2
-bash-3.2#
```

FIGURE F-8. **Check the WCCP control connection**

4. Check the communications between the IWSVA and Cisco device.

a. On the IWSVA unit, enable the debug-level logging for the WCCP Server Daemon:

i. Set **`wccp_logging=1`** in `IWSSPIProtocolHttpProxy.pni` file in the `/var/iwss` directory.

ii. Restart the WCCP Server Daemon with the following commands:

```
/usr/iwss/S99ISWCCPd stop
/usr/iwss/S99ISWCCPd start
```

b. Check the `http.log.current_date_time.nnnn` file in the IWSVA's `/etc/iscan/log` directory for the following log entries. You can use an editor such as "vi" to open and view the log file or use the “cat filename |more” command.

```
… <6887> WCCP: Sending WCCPv2 HERE_I_AM for service ID 80
… <6887> WCCP: Received WCCPv2 I_SEE_YOU from 10.13.9.185
… <6887> WCCP: Good Received WCCPv2 I_SEE_YOU
```

If you cannot see the first log entry with the “Here I Am” message, the WCCP transparency mode is not configured or the WCCP Server Daemon is not running.

If you cannot see the second log entry with the "I See You" message, the network device is not responding. Check its configuration or connectivity between IWSVA and the network device.

If you cannot see the third log entry confirming the "I See You", the message from the network device cannot be parsed. This may happen if you use an unsupported network device.

5. Check the control connection on the Cisco router or switch. Log into the Cisco device's console as the administrative user and perform the following diagnostic procedures:

   a. Run the **`show ip wccp <service id> view`** command to obtain a list of all routers and IWSVA systems.

      ```
      Router# show ip wccp 80 view
      WCCP Routers Informed of:
      10.13.10.17
      WCCP Cache Engines Visible:
      10.13.9.189
      WCCP Cache Engines NOT Visible:
      -none-
      ```

      If the "Cache Engines Visible" contains "-none-", there is no communications over the control connection.

   b. Run the **`show ip wccp <service_id>`** command to obtain a list of all routers and IWSVA systems. Unless another service value was selected, the default Service ID should be 80.

      ```
      Router# show ip wccp 80
      Global WCCP information:
        Router information:
          Router Identifier:       10.13.10.17
          Protocol Version:        2.0
        Service Identifier: web-cache
          Number of Cache Engines:    1
          Number of routers:          1
          Total Packets Redirected:   0
      ```

```
Redirect access-list:          -none-
Total Packets Denied Redirect:  0
Total Packets Unassigned:      0
Group access-list:             -none-
Total Messages Denied to Group:       0
Total Authentication failures:        0
```

The router identifier is the Cisco router's IP address that the IWSVA sees. This address is not necessarily the router interface that the redirected traffic uses to reach the cache, but the IP address displayed needs to be reachable by IWSVA.

The Total Packets Unassigned value is the number of packets that were not redirected due to a lack of assignment to an IWSVA device. The redirection failure can happen during the initial discovery of the IWSVA device or if the IWSVA is unavailable for short periods of time - such as being down for maintenance or services being restarted.

Checking the WCCP Registration Activity

Perform the following steps on the Cisco device to validate the WCCP registration activity.

To validate the WCCP registration activity:

1. Run the **`show ip wccp 80 view`** command to obtain a list of routers and IWSVA systems. This example assumes that the service ID is left at the default value of 80.
2. If the Cisco device is unable to “partner” with IWSVA, you will need to enable the debug capabilities to expose the WCCP activity on the Cisco device. The debug commands to enable the WCCP events and packets are:

   ```
   debug ip wccp events
   ```

   ```
   debug ip wccp packets
   ```

   You should enable the debug commands as shown in the example below after you have configured the IWSVA device and the Cisco device for WCCP. The debug will show the WCCP communication sessions between the two devices.
3. Log into the Cisco device's console as the administrative user and perform the following:

a. Router# **`debug ip wccp event`**

WCCP events debugging is on.

b. Router# **debug ip wccp packet**

WCCP packet info debugging is on

The Cisco device will display the results of the packet debug as follows:

```
Router#
2d18h: WCCP-EVNT:S00: Built new router view: 0 routers, 0 usable web caches, change
 # 00000001
2d18h: %SYS-5-CONFIG_I: Configured from console by console
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000001
2d18h: WCCP-EVNT:S00: Redirect_Assignment packet from 192.168.15.2 fails source
check
2d18h: %WCCP-5-SERVICEFOUND: Service web-cache acquired on Web Cache
192.168.15.2
2d18h: WCCP-PKT:S00: Received valid Here_I_Am packet from 192.168.15.2 w/rcv_id
00000001
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000002
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2
w/rcv_id
 00000002
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000003
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2 w/rcv_id
 00000003
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000004
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000005
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000006
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2 w/rcv_id
 00000006
```

What to Look for in the Packet Debug

Whenever the Cisco device receives a “Here I Am” packet from the cache (IWSVA), the Cisco device answers with an “I See You” packet. You should see the responses as illustrated in the previous example above if your IWSVA is communicating properly with the Cisco device.

In a production environment, there may be a lot of other chatter that may make deciphering of the debug difficult. In order to filter the debug traffic and highlight the appropriate IP address for faster troubleshooting, use an ACL to restrict the debug capture to packets that only have the IWSVA IP address as the source address.

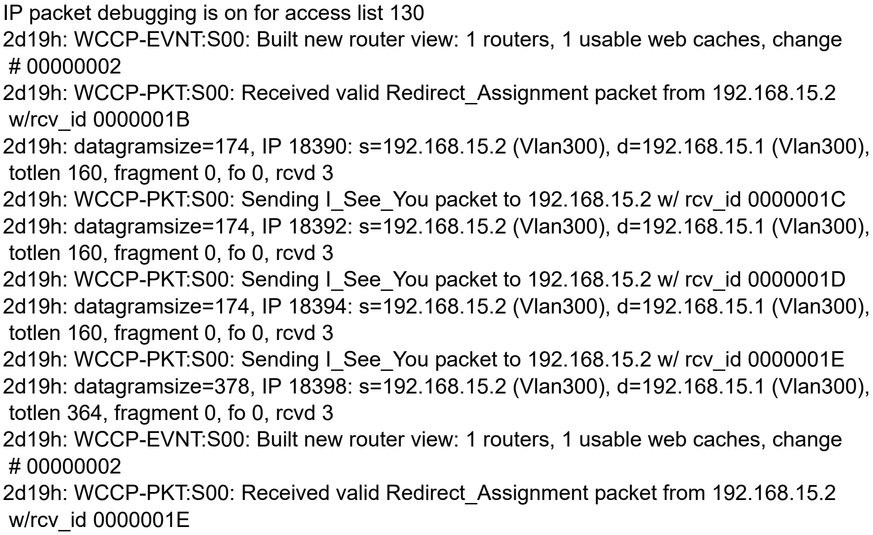
The example below shows how an ACL is used to zero in on the IWSVA IP address.

1. Execute the two commands show below to configure an ACL on the IWSVA IP address(es) and enable the debug process.

   ```
   Router(config)# access-list 130 permit ip host 192.168.15.2
   host 192.168.15.1
   ```

   ```
   Router# debug ip packet 130
   ```

   The following illustration shows an example of a filtered debug packet trace using the IWSVA IP address.



```
IP packet debugging is on for access list 130
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2
 w/rcv_id 0000001B
2d19h: datagramsize=174, IP 18390: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 0000001C
2d19h: datagramsize=174, IP 18392: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 0000001D
2d19h: datagramsize=174, IP 18394: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 0000001E
2d19h: datagramsize=378, IP 18398: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 364, fragment 0, fo 0, rcvd 3
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2
 w/rcv_id 0000001E
```

```
2d19h: datagramsize=174, IP 18402: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 0000001F
2d19h: datagramsize=174, IP 18404: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000020
2d19h: datagramsize=174, IP 18406: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000021
2d19h: datagramsize=378, IP 18410: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 364, fragment 0, fo 0, rcvd 3
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2
 w/rcv_id 00000021
2d19h: datagramsize=174, IP 18414: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000022
2d19h: datagramsize=174, IP 18416: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
```

What to Look for in the Packet Debug

If the router sees no IWSVA or WCCP activity, check the basic connectivity between the two devices. Try to ping IWSVA from the router or the router from the IWSVA device. If the pings work, verify that the configuration on the router is correct.

If the **cache acquisition** occurs but there is no packet redirection, verify that traffic actually reaches the router. Also, verify that traffic is being forwarded to the correct Cisco device interface. This was configured during the traffic redirection steps in the examples above. Note that the interception and redirection traffic goes to TCP port 80.

If the **cache acquisition** occurs and you see the redirection of packets but your clients cannot browse the Internet, check the IWSVA device's connectivity to the Internet and to your clients. From the IWSVA's console management screen, try pinging some IP addresses on the public Internet and to some of your clients on the internal network.

Checking the Packet Redirection

Perform the following steps on the Cisco device to validate the packet redirection activity to ensure that packets are being forwarded properly.

To validate the packet redirection activity:

1. Log into your Cisco device's console as the administrative user.
2. Run the **`show ip wccp 80 detail`** command to obtain the redirection statistics from the Cisco device. This example assumes that the service ID is set to the default of 80.

```
Router# show ip wccp 80 detail
```

```
WCCP Cache-Engine information:
Web Cache ID: 10.13.9.189
Protocol Version: 2.0
State: Usable
Redirection:          GRE
Initial Hash Info: 00000000000000000000000000000000
00000000000000000000000000000000
Assigned Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Hash Allotment: 256 (100.00%)
Packets Redirected: 736
Connect Time: 00:07:45
```

The Redirection parameter shows the packet redirection protocol used between the Cisco device and the cache (IWSVA). The redirection protocol can be set to Generic Routing Encapsulation (GRE) or Layer 2 (L2). GRE tunnels the communications and creates a point-to-point connection to allow devices to communicate over an IP network. L2 redirection on the other hand sends the packets directly to the cache (IWSVA) without encapsulating it first - but this requires the Cisco device and the IWSVA to be on the same Layer 2 network.

The Hash Allotment is the number of hash buckets assigned to the IWSVA. The Hex values show the Hash Allotment with Initial Hash Info and Assigned Hash Info values. The hash algorithm allows the collection and division of all the possible destination Internet addresses within a number of buckets. Each IWSVA device in the defined service group receives a percentage of the preset buckets. WCCP dynamically manages these resources according to the load and other preset conditions. If IWSVA is the only cache device defined, WCCP will assign all bucket resources to the IWSVA unit.

When the Cisco device starts the redirection of packets to the Cache Engine (IWSVA), you should see an increase in the value of the “Packets Redirected” field.

Verifying the Packet Flow on IWSVA

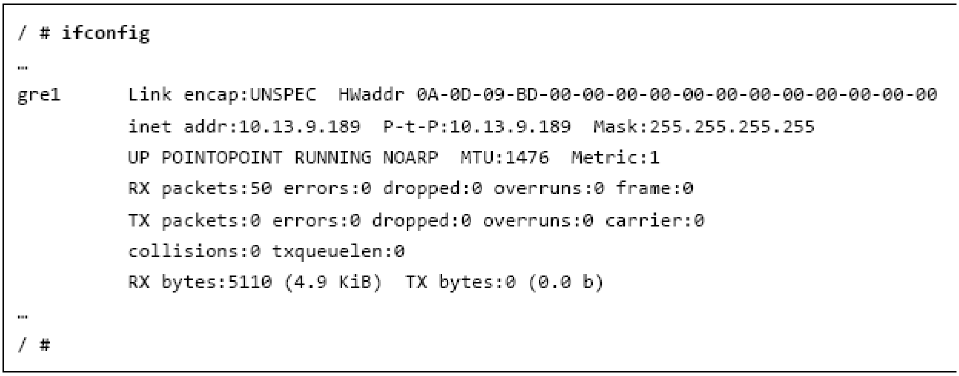
If the forward method is set to GRE and the packets are redirected from the Cisco device, but are not being received by the IWSVA scanning daemons (based on the http.log file in the `/etc/iscan/log` directory), check the following IWSVA settings.

Note: For L2 forward method deployments, skip to step 2 and proceed to step 3.

To verify the packet flow on IWSVA:

1. Log into the IWSVA console as the root user.
2. For GRE forward method deployments, use the **`ifconfig`** command to verify that the "gre1" device is operating correctly.

   ```
   - bash - 3.2# ifconfig
   ```

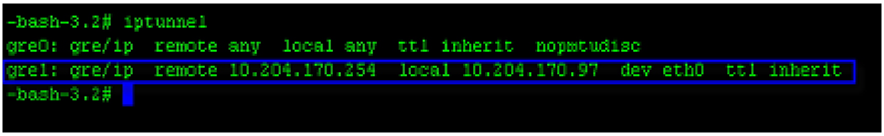


```
/ # ifconfig
…
gre1      Link encap:UNSPEC  HWaddr 0A-0D-09-BD-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.13.9.189  P-t-P:10.13.9.189  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1476  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5110 (4.9 KiB)  TX bytes:0 (0.0 b)
…
/ #
```

FIGURE F-9. Use the `ifconfig` command to verify that the "gre1" device is operating correctly

3. Use the **`iptunnel`** command to verify that the IP tunnel from the router to IWSVA is configured.

```
-bash-3.2# iptunnel
```

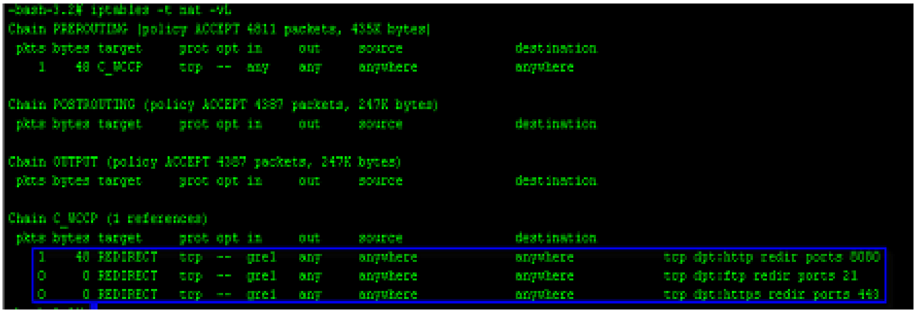


```
-bash-3.2# iptunnel
gre0: gre/ip  remote any  local any  ttl inherit  nopmtudisc
gre1: gre/ip  remote 10.204.170.254  local 10.204.170.97  dev eth0  ttl inherit
-bash-3.2#
```

FIGURE F-10. Use the `iptunnel` **command to verify that the IP tunnel is configured.**

4. Use the **`iptables`** command to verify that the IWSVA firewall is redirecting the packets to the scanning daemons.

```
-bash-3.2# iptables -t nat  -vL
```



```
-bash-3.2# iptables -t nat -vL
Chain PREROUTING (policy ACCEPT 4811 packets, 435K bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    48 C_WCCP     tcp  --  any    any     anywhere             anywhere

Chain POSTROUTING (policy ACCEPT 4387 packets, 247K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4387 packets, 247K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain C_WCCP (1 references)
 pkts bytes target     prot opt in     out     source               destination
    1    48 REDIRECT   tcp  --  gre1   any     anywhere             anywhere            tcp dpt:http redir ports 8080
    0     0 REDIRECT   tcp  --  gre1   any     anywhere             anywhere            tcp dpt:ftp redir ports 21
    0     0 REDIRECT   tcp  --  gre1   any     anywhere             anywhere            tcp dpt:https redir ports 443
```

FIGURE F-11. Use the `iptables` **command to verify that the IWSVA firewall is redirecting the packets**

5. (Optional) As an "advanced" troubleshooting step, you can use the **`tcpdump`** command to capture packets from the IWSVA firewall. This will allow you to verify that IWSVA is processing the packets correctly.

   a. To limit the amount of data that is captured with the tcpdump packet capture command, configure the Cisco router with an ACL to limit the WCCP redirection to one client. This will allow you to decrease the scope and concentrate on a single client.

   The example below shows how to restrict the WCCP redirection to one client (10.10.10.152) and start the WCCP redirection process.

   ```
   Router(config)# access-list 50 permit 10.10.10.152
   ```

```
Router(config)# ip wccp web-cache redirect-list 50
```

b. Enable the packet capture on the IWSVA using the **`tcpdump`** command. This is done from the IWSVA's console, and you must access the console as the "root" user.

```
-bash-3.2# tcpdump -s0 -w wccp.cap
```

c. After capturing enough packets, stop the packet capture, and copy the wccp.cap file to your local host.

d. Using a packet analysis tool such as Wireshark, open the wccp.cap file, and analyze the packet capture.

e. Analyze the packet capture to see that the communications between the Cisco device and the IWSVA device are working properly.

Note: Using the tcpdump packet capture utility is an advanced concept and it may not be easy to decipher the communications between the Cisco and IWSVA device. If you have troubleshot up to this step and still cannot resolve the WCCP issue, you should contact Trend Micro's customer support department for more assistance.

Appendix G

URL Filtering Category Mapping

Table G-1 shows the URL Filtering Category mapping

URL Filtering Category Mapping Table.

TABLE G-1. URL Category Mapping

ID #	CATEGORY GROUP
23=Internet Radio and TV	Network Bandwidth
72=Pay to Surf	Network Bandwidth
57=Peer-to-peer	Network Bandwidth
56=Personal Network Storage/File Download Server	Network Bandwidth
43=Photo Searches	Network Bandwidth
70=Ringtones/Mobile Phone Downloads	Network Bandwidth
71=Software Downloads	Network Bandwidth
69=Streaming Media/MP3	Network Bandwidth
77=Adware	Internet Security
80=Cookies	Internet Security
81=Dialers	Internet Security
79=Disease Vector	Internet Security
82=Hacking	Internet Security
83=Joke Program	Internet Security
86=Made for AdSense	Internet Security
78=Malware Accomplice Formerly "Virus Accomplice"	Internet Security
84=Password Cracking	Internet Security
93=New Domain	Internet Security

TABLE G-1. URL Category Mapping (Continued)

ID #	CATEGORY GROUP
94=Scam	Internet Security
73=Potentially Malicious Software	Internet Security
39=Proxy Avoidance	Internet Security
85=Remote Access Program	Internet Security
76=Spam	Internet Security
74=Spyware	Internet Security
88=Web Advertisement	Internet Security
95=Ransomware	Internet Security
42=Blogs/Web Communications (Formerly Web Communications)	Communication and Searches
51=Chat/Instant Messaging	Communication and Searches
52=Email (Formerly “Email related”)	Communication and Searches
41=Internet Infrastructure (Formerly Infrastructure)	Communication and Searches
24=Internet Telephony	Communication and Searches
53=Newsgroups	Communication and Searches
40=Search Engines/Portals	Communication and Searches
50=Social Networking	Communication and Searches

TABLE G-1. URL Category Mapping (Continued)

ID #	CATEGORY GROUP
89=Web Hosting	Communication and Searches
16=Abortion	Adult
1=Adult/Mature Content	Adult
8=Alcohol/Tobacco	Adult
11=Gambling	Adult
25=Illegal Drugs	Adult
9=Illegal/Questionable	Adult
5=Intimate Apparel/Swimsuit	Adult
26=Marijuana	Adult
6=Nudity	Adult
3=Pornography	Adult
4=Sex Education	Adult
10=Tasteless	Adult
14=Violence/Hate/Racism	Adult
15=Weapons	Adult
59=Auctions	Business
32=Brokerage/Trading	Business
21=Business/Economy	Business
31=Financial Services	Business
45=Job Search/Careers	Business

TABLE G-1. URL Category Mapping (Continued)

ID #	CATEGORY GROUP
60=Real Estate	Business
58=Shopping	Business
38=Computers/Internet	General
67=Vehicles	General
30=Activist Groups	Lifestyle
44=Alternative Journals	Lifestyle
19=Arts (Formerly Arts/ Entertainment)	Lifestyle
22=Cult/Occult	Lifestyle
29=Cultural Institutions	Lifestyle
20=Entertainment (Formerly Arts/ Entertainment)	Lifestyle
87=For Kids	LIfestyle
33=Games	Lifestyle
63=Gun Clubs/Hunting	Lifestyle
68=Humor (Formerly Humor/Jokes)	Lifestyle
55=Personal Sites	Lifestyle
47=Personals/Dating	Lifestyle
18=Recreation/Hobbies	Lifestyle

TABLE G-1. URL Category Mapping (Continued)

ID #	CATEGORY GROUP
54=Religion	LIfestyle
64=Restaurants/Food (Formerly Restaurants/Dining/Food)	Lifestyle
61=Society/Lifestyle	Lifestyle
65=Sports	Lifestyle
76=Spam	N/A
63=Sport Hunting and Gun Clubs	N/A
66=Travel	Lifestyle
38=Computers/Internet	General
27=Education	General
34=Government/Legal	General
37=Health	General
86=Made for AdSense sites (MFA)	N/A
35=Military	General
46=News/Media	General
36=Politics (Formerly Political)	General
49=Reference	General
48=Translators / Cached Pages (Formerly Translators (circumvent filtering)	General
67=Vehicles	General

TABLE G-1. URL Category Mapping (Continued)

ID #	CATEGORY GROUP
90=Untested (Formerly Unrated)	General

Appendix H

URL Filtering Category Groups

URL categories are organized into the URL filtering groups shown in *Table H-1*.

TABLE H-1. Grouping Definition for URL Categories

CATEGORY GROUP	DESCRIPTION
Adult	Websites generally considered inappropriate for children
Business	Websites related to business, employment, or commerce
Communications and Search	Websites that provide tools and services for online communications and searches.
General	Websites that do not fall into the other categories.
Internet Security	Potentially harmful websites, including those known to distribute malicious software
Lifestyle	Websites about religious, political, or sexual preferences, as well as recreation and entertainment
Network Bandwidth	Websites offering services that can significantly impact the speed of the computer's Internet connection
Custom Categories	Websites that administrators have defined for specific customized categories.

Note: For URL filtering to work correctly, the IWSVA must be able to send HTTP requests to the Trend Micro service. If an HTTP proxy is required, configure the proxy setting by choosing **Administration > Deployment Wizard**.

URL Filtering Categories

Table H-2 lists definitions of the URL filtering categories and the assigned group.

TABLE H-2. URL Filtering Category Definitions

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Adult	Abortion	Sites that promote, encourage, or discuss abortion, including sites that cover moral or political views on abortion
Adult	Adult/Mature Content	Sites with profane or vulgar content generally considered inappropriate for minors; includes sites that offer erotic content or ads for sexual services, but excludes sites with sexually explicit images
Adult	Alcohol/ Tobacco	Sites that promote, sell, or provide information about alcohol or tobacco products
Adult	Gambling	Sites that promote or provide information on gambling, including online gambling sites
Adult	Illegal Drugs	Sites that promote, glamorize, supply, sell, or explain how to use illicit or illegal intoxicants
Adult	Illegal/ Questionable	Sites that promote and discuss how to perpetrate nonviolent crimes, including burglary, fraud, intellectual property theft, and plagiarism; includes sites that sell plagiarized or stolen materials

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Adult	Intimate Apparel/ Swimsuit	Sites that sell swimsuits or intimate apparel with models wearing them
Adult	Marijuana	Sites that discuss the cultivation, use, or preparation of marijuana, or sell related paraphernalia
Adult	Nudity	Sites showing nude or partially nude images that are generally considered artistic, not vulgar or pornographic
Adult	Pornography	Sites with sexually explicit imagery designed for sexual arousal, including sites that offer sexual services
Adult	Sex Education	Sites with or without explicit images that discuss reproduction, sexuality, birth control, sexually transmitted disease, safe sex, or coping with sexual trauma
Adult	Tasteless	Sites with content that is gratuitously offensive and shocking; includes sites that show extreme forms of body modification or mutilation and animal cruelty
Adult	Violence/ Hate/ Racism	Sites that promote hate and violence; includes sites that espouse prejudice against a social group, extremely violent and dangerous activities, mutilation and gore, or the creation of destructive devices
Adult	Weapons	Sites about weapons, including their accessories and use; excludes sites about military institutions or sites that discuss weapons as sporting or recreational equipment

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Business	Auctions	Sites that serve as venues for selling or buying goods through bidding, including business sites that are being auctioned
Business	Brokerage/Trading	Sites about investments in stocks or bonds, including online trading sites; includes sites about vehicle insurance
Business	Business/ Economy	Sites about business and the economy, including entrepreneurship and marketing; includes corporate sites that do not fall under other categories
Business	Financial Services	Sites that provide information about or offer basic financial services, including sites owned by businesses in the financial industry
Business	Job Search/ Careers	Sites about finding employment or employment services
Business	Real Estate	Sites about real estate, including those that provide assistance selling, leasing, purchasing, or renting property
Business	Shopping	Sites that sell goods or support the sales of goods that do not fall under other categories; excludes online auction or bidding sites
Communications and Search	Blogs/Web Communications	Blog sites or forums on varying topics or topics not covered by other categories; sites that offer multiple types of web-based communication, such as e-mail or instant messaging
Communications and Search	Chat/Instant Messaging	Sites that provide web-based services or downloadable software for text-based instant messaging or chat

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Communications and Search	Email	Sites that provide email services, including portals used by companies for web-based email
Communications and Search	Internet Infrastructure	Content servers, image servers, or sites used to gather, process, and present data and data analysis, including web-based analytics tools and network monitors
Communications and Search	Internet Telephony	Sites that provide web services or downloadable software for Voice over Internet Protocol (VoIP) calls
Communications and Search	Newsgroups	Sites that offer access to Usenet or provide other newsgroup, forum, or bulletin board services
Communications and Search	Search Engines/ Portals	Search engine sites or portals that provide directories, indexes, or other retrieval systems for the web
Communications and Search	Social Networking	Sites devoted to personal expression or communication, linking people with similar interests
Communications and Search	Web Hosting	Sites of organizations that provide top-level domains or web hosting services
General	Computers/ Internet	Sites about computers, the Internet, or related technology, including sites that sell or provide reviews of electronic devices
General	Education	School sites, distance learning sites, and other education-related sites

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
General	Government/ Legal	Sites about the government, including laws or policies; excludes government military or health sites
General	Health	Sites about health, fitness, or well-being
General	Military	Sites about military institutions or armed forces; excludes sites that discuss or sell weapons or military equipment
General	News/Media	Sites about the news, current events, contemporary issues, or the weather; includes online magazines whose topics do not fall under other categories
General	Politics	Sites that discuss or are sponsored by political parties, interest groups, or similar organizations involved in public policy issues; includes non-hate sites that discuss conspiracy theories or alternative views on government
General	Reference	General and specialized reference sites, including map, encyclopedia, dictionary, weather, how-to, and conversion sites
General	Translators/ Cached Pages	Online page translators or cached Web pages (used by search engines), which can be used to circumvent proxy servers and Web filtering systems
General	Untested	Sites that have not been classified under a category
General	Vehicles	Sites about motorized transport, including customization, procurement of parts and actual vehicles, or repair services; excludes sites about military vehicles

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Internet Security	Adware	Sites with downloads that display advertisements or other promotional content; includes sites that install browser helper objects (BHOs)
Internet Security	Cookies	Sites that send malicious tracking cookies to visiting web browsers
Internet Security	Dialers	Sites with downloads that dial into other networks or premium-rate telephone numbers without user consent
Internet Security	Disease Vector	Sites that directly or indirectly facilitate the distribution of malicious software or source code
Internet Security	Hacking	Sites that provide downloadable software for bypassing computer security systems
Internet Security	Joke Program	Sites that provide downloadable “joke” software, including applications that can unsettle users
Internet Security	Made for AdSense sites (MFA)	Sites that use scraped or copied content to pollute search engines with redundant and generally unwanted results
Internet Security	Malware Accomplice	Sites used by malicious programs, including sites used to host upgrades or store stolen information
Internet Security	Password Cracking	Sites that distribute password cracking software
Internet Security	Scam	Scam is an attempt to defraud a person or group after first gaining their confidence, used in the classical sense of trust. It is different from either Phishing or Spam.

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Internet Security	Potentially Malicious Software	Sites that contain potentially harmful downloads
Internet Security	Proxy Avoidance	Sites about bypassing proxy servers or web filtering systems, including sites that provide tools for that purpose
Internet Security	Remote Access Program	Sites that provide tools for remotely monitoring and controlling computers
Internet Security	Spam	Sites whose addresses have been found in spam messages
Internet Security	Spyware	Sites with downloads that gather and transmit data from computers owned by unsuspecting users
Internet Security	Web Advertisement	Sites dedicated to displaying advertisements, including sites used to display banner or pop-up ads
Lifestyle	Activist Groups	Sites that promote change in public policy, public opinion, social practice, economic activities, or economic relationships; includes sites controlled by service, philanthropic, professional, or labor organizations
Lifestyle	Alternative Journals	Online equivalents of supermarket tabloids and other fringe publications
Lifestyle	Arts	Sites about visual arts, such as painting and sculpture.
Lifestyle	Cult/Occult	Sites about alternative religions, beliefs, and religious practices, including those considered cult or occult

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Lifestyle	Cultural Institutions	Sites controlled by organizations that seek to preserve cultural heritage, such as libraries or museums; also covers sites owned by the Boy Scouts, the Girl Scouts, Rotary International, and similar organizations
Lifestyle	Entertainment	Sites that promote or provide information about movies, music, non-news radio and television, books, humor, or magazines
Lifestyle	For Kids	Sites designed for children
Lifestyle	Games	Sites about board games, card games, console games, or computer games; includes sites that sell games or related merchandise
Lifestyle	Gun Clubs/ Hunting	Sites about gun clubs or similar groups; includes sites about hunting, war gaming, or paintball facilities
Lifestyle	Humor	Sites intended for humor.
Lifestyle	Personal Sites	Sites maintained by individuals about themselves or their interests; excludes personal pages in social networking sites, blog sites, or similar services
Lifestyle	Personals/ Dating	Sites that help visitors establish relationships, including sites that provide singles listings, matchmaking, or dating services
Lifestyle	Recreation/ Hobbies	Sites about recreational activities and hobbies, such as collecting, gardening, outdoor activities, traditional (non-video) games, and crafts; includes sites about pets, recreational facilities, or recreational organizations

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Lifestyle	Religion	Sites about popular religions, their practices, or their places of worship
Lifestyle	Restaurants/ Food	Sites that list, review, discuss, advertise, or promote food, catering, dining services, cooking, or recipes
Lifestyle	Society/ Lifestyle	Sites that provide information about life or daily matters; excludes sites about entertainment, hobbies, sex, or sports, but includes sites about cosmetics or fashion
Lifestyle	Sports	Sites about sports or other competitive physical activities; includes fan sites or sites that sell sports merchandise
Lifestyle	Travel	Sites about travelling or travel destinations; includes travel booking and planning sites
Network Bandwidth	Internet Radio and TV	Sites that primarily provide streaming radio or TV programming; excludes sites that provide other kinds of streaming content
Network Bandwidth	Pay to Surf	Sites that compensate users who view certain websites, email messages, or advertisements or users who click links or respond to surveys
Network Bandwidth	Peer-to-Peer	Sites that provide information about or software for sharing and transferring files within a peer-to-peer (P2P) network
Network Bandwidth	Personal Network Storage/File Download Servers	Sites that provide personal online storage, backup, or hosting space, including those that provide encryption or other security services

TABLE H-2. URL Filtering Category Definitions (Continued)

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Network Bandwidth	Photo Searches	Sites that primarily host images, allowing users to share, organize, store, or search for photos or other images
Network Bandwidth	Ring-tones/Mobile Phone Downloads	Sites that provide content for mobile devices, including ringtones, games, or videos
Network Bandwidth	Software Downloads	Sites dedicated to providing free, trial, or paid software downloads
Network Bandwidth	Streaming Media/ MP3	Sites that offer streaming video or audio content without radio or TV programming; sites that provide music or video downloads, such as MP3 or AVI files

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

TERM	EXPLANATION
“in the wild”	Describes known viruses that are actively circulating. *Also see* “in the zoo.”
“in the zoo”	Describes known viruses that are currently controlled by antivirus products. *Also see* “in the wild.”
(administrative) domain	A group of computers sharing a common database and security policy.
access (noun)	Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.
access (verb)	To read data from or write data to a storage device, such as a computer or server.
activate	To enable your software after completion of the registration process. Trend Micro products are not operable until product activation is complete. Activate during installation or after installation (in the Web console) on the Product License screen.
Activation Code	A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.
active FTP	Configuration of FTP protocol that allows the client to initiate “handshaking” signals for the command session, but the host initiates the data session.

TERM	EXPLANATION
ActiveUpdate	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files through the Internet or the Trend Micro Total Solution CD or DVD.
ActiveX	A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.
ActiveX malicious code	An ActiveX control is a component object embedded in a Web page which runs automatically when the page is viewed. ActiveX controls allow Web developers to create interactive, dynamic Web pages with broad functionality such as HouseCall, Trend Micro's free online scanner. Hackers, virus writers, and others who want to cause mischief or worse might use ActiveX malicious code as a vehicle to attack the system. In many cases, the Web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to “high.”
address	Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to “system administrator”—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.

Term	Explanation
administrator email address	The address used by the administrator of your Trend Micro product to manage notifications and alerts.
adware	Advertising-supported software in which advertising banners appear while the program is running. Adware that installs a “back door”; tracking mechanism on the user's computer without the user's knowledge is called “spyware.”
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.
antivirus	Computer programs designed to detect and clean computer viruses.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
attachment	A file attached to (sent with) an email message.
audio/video file	A file containing sounds, such as music, or video footage.

TERM	EXPLANATION
authentication	The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption or on public-key systems using digital signatures. *Also see* public-key encryption *and* digital signature.
binary	A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.
block	To prevent entry into your network.
browser	A program which allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.
cache	A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.
cause	The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.
clean	To remove virus code from a file or message.

Term	Explanation
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
cookie	A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your Web browser for later use. The next time you access a Web site for which your browser has a cookie, your browser sends the cookie to the Web server, which the Web server can then use to present you with customized Web pages. For example, you might enter a Web site that welcomes you by name.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur.
damage routine	The destructive portion of virus code, also called the payload.

TERM	EXPLANATION
De-Militarized Zone (DMZ)	From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They might be external or internal. External DMZ Ethernets link regional networks with routers.
default	A value that pre-populates a field in the Web console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
Deployment Wizard	A Web console-based wizard, which is used for ease of deployment. Deployment-related configurations have been removed from the product installation to this wizard.
dialer	A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.
directory	A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, *C:\Windows* is the Windows directory on the C drive.
directory path	The subsequent layers within a directory where a file can be found.
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message.

TERM	EXPLANATION
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called “name resolution”, uses the Domain Name System (DNS).
DOS virus	Also referred to as “COM” and “EXE file infectors.” DOS viruses infect DOS executable programs- files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.
download (noun)	Data that has been downloaded, for example, from a Web site through HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.
dropper	Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.

TERM	EXPLANATION
ELF	Executable and Linkable Format—An executable file format for UNIX and Linux platforms.
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone might use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone might send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it.
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking “I accept” during installation. Clicking “I do not accept” will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software.
Ethernet	A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network.

TERM	EXPLANATION
EXE file infector	An executable program with an .exe file extension. *Also see* DOS virus.
executable file	A binary file containing a program in machine language which is ready to be executed (run).
exploit	An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
file	An element of data, such as an email message or HTTP download.
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.

TERM	EXPLANATION
file-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
gateway	An interface between an information source and a Web server.
grayware	A category of software that might be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it might violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

TERM	EXPLANATION
group file type	Types of files that have a common theme, for example: - Audio/Video - Compressed - Executable - Images - Java - Microsoft Office
GUI	Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.
hacking tool	Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
header (networking definition)	Part of a data packet that contains transparent information about the file or the transmission.
heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
host	A computer connected to a network.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.

TERM	EXPLANATION
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
ICSA	ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry’s central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90 percent of the installed base of antivirus, firewall, IPSec, cryptography, and PC firewall products in the world today.
image file	A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, through a digital camera, or they might be generated by computer using graphics software.
incoming	Email messages or other data routed *into* your network.
installation script	The installation screens used to install UNIX versions of Trend Micro products.
instance-level settings	IWSS policies and settings which only apply to individual instances.
integrity checking	*See* checksumming.
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true-file type recognition, and scanning only file types known to potentially harbor malicious code. True-file type recognition helps identify malicious code that can be disguised by a harmless extension name.

Term	Explanation
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
Internet Bots	Web robots, or simply bots, are software applications that are often used to initiate attacks to a specific target, such as DDoS attack. They are an ever increasing threat to business networks, individuals, and the Internet in general. If they are present in the enterprise environment, they could consume a significant amount of network bandwidth and computing power. They could also incur some legal liabilities to a company.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.
interrupt	An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—*See* IP address.
IP address	Internet address for a device on a network, typically expressed using IPv4 dot notation (such as 123.123.123.123) and IPv6 colon notation.

TERM	EXPLANATION
IP gateway	A gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java applets	Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow Web developers to create interactive, dynamic Web pages with broader functionality. Authors of malicious code have used Java applets as a vehicle for attack. Most Web browsers, however, can be configured so that these applets do not execute - sometimes by simply changing browser security settings to “high.”
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet’s code is transferred to your system and is executed by the browser’s Java Virtual Machine.)
Java malicious code	Virus code written or embedded in Java. *Also see* Java file.

TERM	EXPLANATION
JavaScript virus	JavaScript is a simple programming language developed by Netscape that allows Web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently. A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user's desktop through the user's browser. *Also see* VBscript virus.
joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system.
KB	Kilobyte—1024 bytes of data.
keylogger	Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
LDAP (Lightweight Directory Access Protocol)	An internet protocol that email programs use to locate contact information from a server.
license	Authorization by law to use a Trend Micro product.

Term	Explanation
license certificate	A document that proves you are an authorized user of a Trend Micro product.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
listening port	A port utilized for client connection requests for data exchange.
load balancing	Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.
local area network (LAN)	Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building.
log storage directory	Directory on your server that stores log files.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.
macro	A command used to automate certain functions within an application.
macro virus	Macro viruses are often encoded as an application macro and included in a document. Unlike other virus types, macro viruses aren't specific to an operating system and can spread through email attachments, Web downloads, file transfers, and cooperative applications.

TERM	EXPLANATION
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.
mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
MB	Megabyte—1024 kilobytes of data.
Mbps	Millions of bits per second—a measure of bandwidth in data communications.
Media Access Control (MAC) address	An address that uniquely identifies the network interface card, such as an Ethernet adapter. For Ethernet, the MAC address is a 6 octet address assigned by IEEE. On a LAN or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as the Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type.

TERM	EXPLANATION
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
Network Address Translation (NAT)	A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you don’t have to get a registered IP address for every machine in your network.
Network Content Inspection Engine (NCIE)	An engine that can detect bots or Web robots from Trend Micro.
network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.

TERM	EXPLANATION
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
open source	Programming code that is available to the general public for use or modification free of charge and without license restrictions.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
outgoing	Email messages or other data *leaving* your network, routed out to the Internet.
parameter	A variable, such as a range of values (a number from 1 to 10).
partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
passive FTP	Configuration of FTP protocol that allows clients within your local area network to initiate the file transfer, using random upper port numbers (1024 and above).
password cracker	An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.

TERM	EXPLANATION
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
policies	Policies provide the initial protection mechanism for the firewall, allowing you to determine what traffic passes across it based on IP session details. They protect the Trusted network from outsider attacks, such as the scanning of Trusted servers. Policies create an environment in which you set up security policies to monitor traffic attempting to cross your firewall.
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer.
protected network	A network protected by IWSVA (Trend Micro™ InterScan™ Web Security Virtual Appliance).
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
public-key encryption	An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.
purge	To delete all, as in getting rid of old entries in the logs.

TERM	EXPLANATION
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.
recipient	The person or entity to whom an email message is addressed.
registration	The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen. *https://olr.trendmicro.com/registration*
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8 *Also see* Activation Code
relay	To convey by means of passing through various other points.
remote access tool (RAT)	Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.
removable drive	A removable hardware component or peripheral device of a computer.
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.

TERM	EXPLANATION
router	This hardware device routes data from a local area network (LAN) to a long distance line.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
script	A set of programming commands that, after invoked, can be executed together. Other terms used synonymously with “script” are “macro” or “batch file.”
seat	A license for one person to use a Trend Micro product.
sector	A physical portion of a disk. (*Also see* partition, which is a logical portion of a disk.)
Secure Socket Layer (SSL)	Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server might run continuously (as a daemon), waiting for requests to arrive, or it might be invoked by some higher-level daemon which controls a number of specific servers.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.

Term	Explanation
signature	*See* virus signature.
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations.
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
spam	Unsolicited email messages meant to promote a product or service.
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.

TERM	**EXPLANATION**
subnet mask	In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The subnet mask is the part of the IP address which is used to represent a subnetwork within a network. Using subnet masks allows you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. Subnet masks are a complex feature, so great care should be taken when using them. *Also see* IP address.
target (*Also see* action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
TCP	Transmission Control Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.

TERM	EXPLANATION
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last “.”. For example, host *wombat.doc.ic.ac.uk* is in top-level domain “uk” (for United Kingdom).
Total Solution CD/DVD	A CD or DVD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD or DVD is available to all Trend Micro Premium Support customers.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
Transmission Control Protocol/Internet Protocol (TCP/IP)	A communications protocol which allows computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
trigger	An event that causes an action to take place. For example, your Trend Micro product detects a virus in an email message. This might *trigger* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan Horse	A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.
true-file type	A virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).

Term	Explanation
tunnel interface	A tunnel interface is the opening, or doorway, through which traffic to or from a VPN tunnel passes. A tunnel interface can be numbered (that is, assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface. *Also see* Virtual Private Network (VPN).
tunnel zone	A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier.

TERM EXPLANATION

tunneling

A method of sending data that enables one network to send data through another network’s connections. Tunnelling is used to get data between administrative domains which use a protocol that is not supported by the internet connecting those domains.

With VPN tunneling, a mobile professional dials into a local Internet Service Provider's Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call.

When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider's site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use.

URL

Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.

TERM	EXPLANATION
VBscript virus	VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a Web page. A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser. *Also see* JavaScript virus.
virtual IP address (VIP address)	A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.
Virtual Local Area Network (VLAN)	A logical (rather than physical) grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.
Virtual Private Network (VPN)	A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling and encryption.

TERM	EXPLANATION
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads might only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
virus kit	A template of source code for building and executing a virus, available from the Internet.
virus signature	A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a computer hacker, someone who writes virus code.
Web	The World Wide Web, also called the Web or the Internet.
Web console	The user interface for your Trend Micro product.

TERM	EXPLANATION
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a “wildcard,” can be used for any number or suit in the card deck.
working directory	The destination directory in which the main application files are stored, such as /etc/iscan/IWSS.
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.
worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.
zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.
zone	A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or a physical or logical entity that performs a specific function (a function zone).