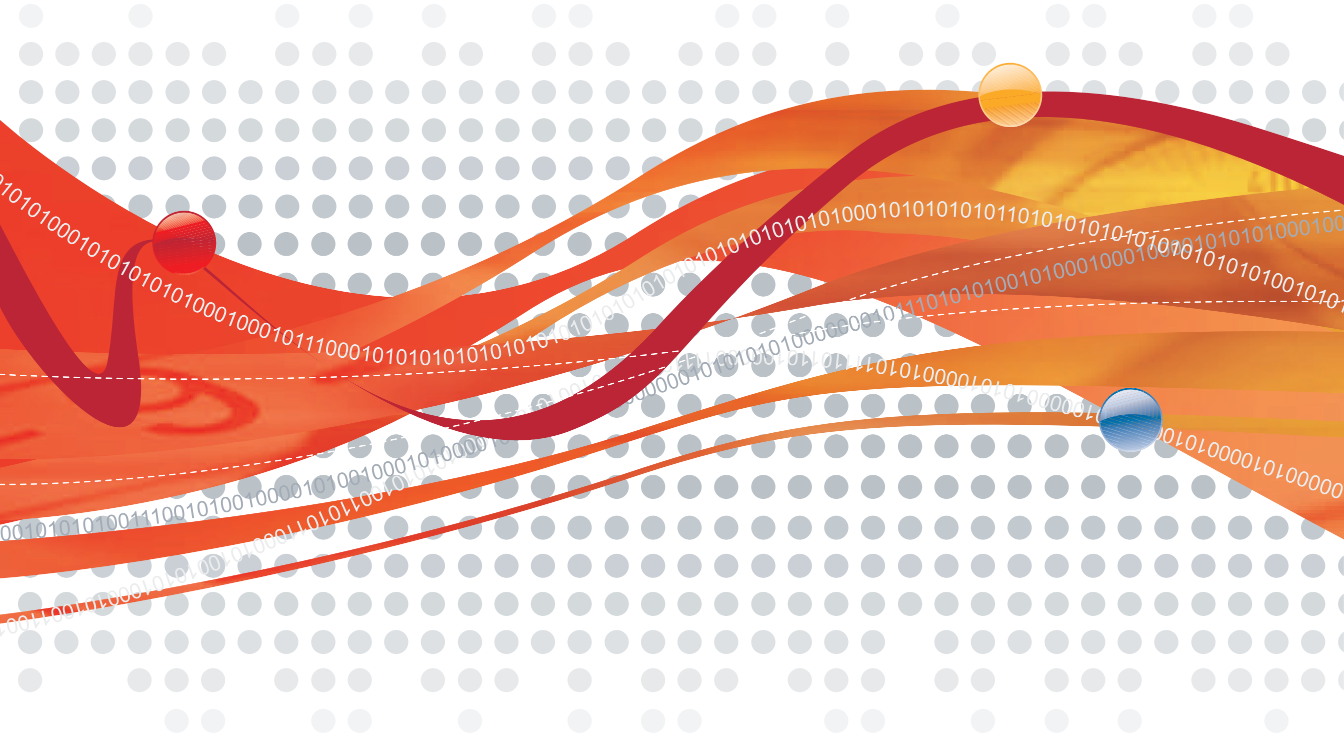
InterScan™ Web Security Virtual Appliance $^{5.1}$

Antivirus and Content Security at the Web Gateway

Installation Guide



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, review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Release Date: August 2010

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

The Installation Guide for Trend Micro™ InterScan™ Web Security Virtual Appliance is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Evaluate this documentation on the following site:

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

Contents

Preface

Chapter 1: Preinstallation Planning

Chapter 2: Deployment Primer

Chapter 3: Installing InterScan Web Security Virtual Appliance

Chapter 4: On-box Upgrade from InterScan Web Security Virtual Appliance 5.0 to 5.1

Chapter 5: Migrating to InterScan Web Security Virtual Appliance

Appendix A: Deployment Integration

Appendix B: Tuning and Troubleshooting

Appendix C: Best Practices for IWSVA Installation and Deployment

Appendix D: Maintenance and Technical Support

Appendix E: Creating a New Virtual Machine Under VMware ESX for IWSVA

Preface

Preface

Welcome to the *Trend Micro™ InterScan™ Web Security Virtual Appliance 5.1 Installation Guide*. This guide helps you to get “up and running” by introducing InterScan Web Security Virtual Appliance (IWSVA), assisting with deployment, installation, migration (if necessary), initial configuration, troubleshooting, performance tuning, and main post-installation configuration tasks. It also includes instructions on testing your installation using a harmless test virus, troubleshooting, and accessing support.

This preface describes the following topics:

- *Audience on page x*
- *IWSVA Documentation on page xii*
- *Document Conventions on page xiii*
- *About Trend Micro on page xiii*

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 and FTP protocols
- Database configuration
- VMware ESX administration experience when installing on VMware ESX

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

How to Use this Guide

This guide contains the information you need to understand and use IWSVA.

If you are an advanced user, you might want to go directly to Chapter 3, *Installing InterScan Web Security Virtual Appliance* and Appendix E, *Creating a New Virtual Machine Under VMware ESX for IWSVA*.

Chapter 1, *Preinstallation Planning*	This chapter describes the tasks you need to do before installing IWSVA. This includes planning for network traffic and HTTP and FTP service flows and ensuring that your server meets specific requirements.
Chapter 2, *Deployment Primer*	This chapter provides an overview of the different topologies in which IWSVA can be installed and helps you plan your server placement and network protection with HTTP and FTP service flows.
Chapter 3, *Installing InterScan Web Security Virtual Appliance*	This chapter describes how to obtain either a evaluation or production version of IWSVA and how to install the application.

Chapter 4, *On-box Upgrade from InterScan Web Security Virtual Appliance 5.0 to 5.1*	This chapter describes how to upgrade from IWSVA 5.0 to IWSVA 5.1 and the configurations and data retained during the upgrade.
Chapter 5, *Migrating to InterScan Web Security Virtual Appliance*	This chapter describes the different migration scenarios and how to complete a migration to IWSVA.
Appendix A, *Deployment Integration*	This appendix describes deployment scenarios for IWSVA, involving several technologies such as LDAP, Damage Cleanup Services (DCS), Cisco routers using WCCP, ICAP, and Transparent Bridge.
Appendix B, *Tuning and Troubleshooting*	This appendix describes performance tuning involving URL filtering and LDAP performance. Also, this appendix provides general troubleshooting tips and possible installation and feature issues.
Appendix C, *Best Practices for IWSVA Installation and Deployment*	This appendix describes the installation and deployment best practices that Trend Micro recommends for IWSVA
Appendix D, *Maintenance and Technical Support*	This appendix describes the maintenance agreement and the aspects of the Trend Micro Technical Support Center.
Appendix E, *Creating a New Virtual Machine Under VMware ESX for IWSVA*	This appendix describes how to create a new virtual machine for IWSVA.

IWSVA Documentation

In addition to the *Trend Micro™ InterScan Web Security Virtual Appliance 5.1 Installation Guide*, the documentation set includes the following:

- **Administrator's Guide**—this guide provides detailed information about all 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, and using logs and reports.
- **Readme file**—the Readme 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/

  DVD ISO creation document—Entitled, *How to Use the Trend Micro IWSVA ISO File*, this document describes how to create a bootable installation DVD from an ISO file.

  Online Help—Helps you configure all features through the user interface. You can access the online help by opening the Web console and then clicking the help icon. 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 management console.
- **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/support`
- **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`

Document Conventions

To help you locate and interpret information easily, the InterScan Web Security Virtual Appliance documentation uses the following conventions.

TABLE 1-1. 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
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

Preinstallation Planning

This chapter describes the following:

- *Server Requirements on page 1-2*
- *Information Needed to Install IWSVA on page 1-5*
- *Planning Network Traffic Protection on page 1-8*

Server Requirements

Operating System

A purpose-built, hardened, and performance-tuned 64-bit operating system is included with InterScan Web Security Virtual Appliance (IWSVA).

Hardware Requirements

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/document/IWSVA_Customer_Sizing_Guide_090930.pdf

Minimum Requirements:

- Single 2.0 GHz Intel ™ Core2Duo™ 64-bit processor supporting Intel™ VT™ or equivalent
- 2GB RAM
- 12GB of disk space. IWSVA automatically partitions the detected disk space as required
- Monitor that supports 1024 x 768 resolution with 256 colors or higher

Recommended Requirements:

- Dual 2.8 GHz Intel ™ Core2Duo™ 64-bit processor or equivalent for up to 4000 users
- Dual 3.16 GHz Intel ™ QuadCore™ 64-bit processor or equivalent for up to 9500 users
- 4GB RAM is recommended to support up to 4000 users
- 8GB RAM is recommended to support up to 9500 users
- 300GB of disk space or more for log intensive environments. IWSVA automatically partitions the detected disk space as per recommended Linux practices

Server Platform Compatibility

IWSVA should install and operate without issues on many brands of "off-the-shelf" server platforms. However, Trend Micro cannot guarantee 100% compatibility with all brands and models of server platforms.

To obtain a list of Trend Micro certified servers that are compatible with IWSVA, access the following URL:

`http://www.trendmicro.com/go/certified`

To obtain a general list of available platforms that should operate with IWSVA, access the following URL:

`http://wiki.centos.org/HardwareList`

Trend Micro cannot guarantee full compatibility with the hardware components from this general list.

Web Browser

To access the HTTP-based Web console, use any of the browsers in *Table 1-1*.

TABLE 1-1. Supported Web Browsers for Web Console Access

BROWSER	WINDOWS			UNIX	
	XP	Vista (64-bit)	Windows 7	RH 4.0 AS	RH 5.0 AS
IE 7.0	✓	✓			
IE 8.0	✓		✓		
Firefox 3.6	✓		✓		✓
Google Chrome 4.1			✓		

To access the Internet through IWSVA, use any of the browsers in *Table 1-2*.

TABLE 1-2. Supported Web Browsers for Internet Access

BROWSER	WINDOWS			UNIX		MAC
	XP	VISTA (64-BIT)	WINDOWS 7	RH 4.0 AS	RH 5.0 AS	OS X
IE 7.0	✓	✓				
IE 8.0	✓		✓			
Firefox 3.6	✓		✓		✓	
Safari 4.0						✓
Google Chrome 4.1			✓			

Other Requirements

- **Database Requirements:**
  - PostgreSQL v7.4.16 (included)
  - When using multiple IWSVA servers in a server farm configuration, Trend Micro recommends that you use separate server (possibly clustered) for PostgreSQL
  - 1.7GB of disk space for every three million HTTP requests per day in order to maintain the log files (calculation based on access logging enabled)
  - 256MB of RAM (based on access logging enabled, else 64MB)
- **Internet Content Adaptation Protocol (ICAP):**
  - NetApp™ NetCache™ release 6.0.1
  - Blue Coat Systems™ SGOS v5
  - Cisco ICAP servers: CE version 5.3
  - Any cache server that is ICAP 1.0 compliant

- **Directory Servers:**

  To configure policies based on Lightweight Directory Access Protocol (LDAP) users and groups, IWSVA can integrate with the following LDAP directories:

  - Microsoft Active Directory 2003 and 2008
  - Linux OpenLDAP Directory 2.2.16 or 2.3.39
  - Sun™ Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)
- **Transparent Bridge:**
  - Each transparent bridge segment supported by IWSVA requires two network interface cards.
- **Web Cache Content Protocol (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 15.1(1)T3 or above should be used
- **Other Requirements:**
- For proxy deployment modes, network clients must be able to access the HTTP port of the IWSVA server that is selected during the install.
- IWSVA server and clients must be able to communicate with each other over the corporate network.

Information Needed to Install IWSVA

You can either purchase or download a 30-day trial version of IWSVA. The 30-day trial version provides all the functionality of IWSVA.

The IWSVA setup program prompts you for required information, depending on the options chosen during installation.

Before beginning, determine the type of installation you should do:

- For new customers doing fresh installations, see Chapter 2, Deployment Primer on page 2-1 for product placement advice and Chapter 3, Installing InterScan Web Security Virtual Appliance on page 3-1.

- For customers migrating from IWSVA 5.0 to IWSVA 5.1, see Chapter 4, On-box Upgrade from InterScan Web Security Virtual Appliance 5.0 to 5.1 on page 4-1.
- For returning customer migrating from older versions of IWSVA, see Chapter 5, Chapter 5, Migrating to InterScan Web Security Virtual Appliance to migrate data and Chapter 3, Installing InterScan Web Security Virtual Appliance on page 3-1 for fresh installation instructions.

Fresh Installation

IWSVA only supports fresh installations if you are running a version of IWSVA older than 5.0. Upgrading an existing IWSS or IWSA installation is not supported. The fresh installation process formats your existing system to install IWSVA. (see Installing IWSVA on page 3-4).

Upgrade and Data Retention

For customers running IWSVA 5.0, an on-box (or in-place) upgrade is available from the Administration > Update OS page of the IWSVA server web console. Most information, configuration and logs are retained. See On-box Upgrade from InterScan Web Security Virtual Appliance 5.0 to 5.1 on page 4-1 for details.

Migration

IWSVA supports existing configuration and policy data migration from the following Trend Micro Products:

- InterScan Web Security Suite 3.1 Linux
- InterScan Web Security Suite 3.1 Windows
- InterScan Web Security Virtual Appliance 3.1
- InterScan Web Security Virtual Appliance 5.0 (same language version)
- InterScan Web Security Virtual Appliance 5.1 (same language version)

For more information about migration, see Chapter 5, Migrating to InterScan Web Security Virtual Appliance.

Type of Proxy Configuration

IWSVA supports multiple deployment modes.

- Forward proxy where clients directly connect to IWSVA.
- Upstream proxy to another existing internal proxy server
- ICAP Server to an existing ICAP 1.0 compliant cache controller
- WCCP client to a configured WCCP-enabled router of firewall
- Transparent Bridge Mode
- Reverse proxy to protect a Web server

The deployment is configured after the IWSVA installation and it can be changed using the Deployment Wizard in the Web console. Each transparent bridge segment supported by IWSVA requires two network interface cards. See Planning the HTTP Flow on page 2-5 and Planning FTP Flows on page 2-7.

Control Manager Server Information

Control Manager registration is performed through the IWSVA Web UI after the IWSVA installation is complete.

Database Type and Location

IWSVA uses the PostgreSQL database for report logs, policies, rules, and configuration settings. A local PostgreSQL installation is performed during IWSVA installation.

SNMP Notifications

If you plan to use SNMP notifications, the IWSVA setup program installs the appropriate SNMP libraries.

Web Console Password

Access to the IWSVA Web console is controlled initially through a default username and password. The default username is “admin.” The default password is adminIWSS85.

Tip: For security reasons, Trend Micro recommends that you change the default admin password after you log in to the Web console the first time.

Command Line Access

IWSVA provides a Command Line Interface (CLI) to allow configuration of the appliance using an industry standard CLI syntax. The CLI offers additional commands and functionality to manage, troubleshoot, and maintain within IWSVA. The CLI can be accessed using a local console keyboard and monitor or remotely through SSHv2.

Proxy for Internet Updates

If you have a proxy host between IWSVA and the Internet, you must configure the IWSVA's proxy settings in order to receive updates from Trend Micro. From the menu, choose **Updates > Connection Settings** to configure the upstream proxy settings. See the Administrator's Guide for more details.

Activation Codes

Activating the three IWSVA modules (core program, URL Filtering, and Applet and ActiveX Scanning) requires a single activation code. IWSVA includes one registration key for all the modules. During product registration, the Registration Key is exchanged for an Activation Code that "unlocks" the program. You can register the installation and exchange the registration key for an activation code from a link in the setup program. Alternatively, you can register and obtain an activation code before installing by visiting Trend Micro's online registration Web site at:

`http://olr.trendmicro.com`

Planning Network Traffic Protection

IWSVA can be deployed in different modes to help secure your network. (See Chapter 2, *Deployment Primer*). IWSVA supports the following deployment topologies:

- *Transparent Bridge Mode on page 1-9*
- *Forward Proxy Mode on page 1-9*

- *Reverse Proxy Mode on page 1-10*
- *ICAP Mode on page 1-10*
- *Simple Transparency Mode on page 1-10*
- *WCCP Mode on page 1-10*

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 the browser or network settings. This is the easiest deployment mode with traffic being scanned in both directions.

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

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

For further details on the Transparent Bridge Mode, see *Deploying in Transparent Bridge Mode on page 2-33*.

Forward Proxy Mode

IWSVA acts 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 Forward Proxy Mode also provides the following additional capabilities:

- Forwards all traffic to another upstream proxy server
- Integrates with an L4 switch for load balancing and simple transparency
- Integrates with a WCCP enabled switch or firewall for load balancing and simple transparency

For more details on the Forward Proxy mode, see *Deploying in Forward Proxy Mode on page 2-10*.

Reverse Proxy 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.

For more details on the Reverse Proxy Mode, see *Deploying in Reverse Proxy Mode on page 2-29*.

ICAP Mode

IWSVA acts as an ICAP proxy and accepts ICAP connections from an ICAP v1.0 compliant cache server. Cache servers can help reduce the overall bandwidth requirements and reduce latency by serving cached content locally. IWSVA scans and secures all content returned to the cache server and to the clients.

For more details on the ICAP mode, see *Deploying in ICAP Mode on page 2-23*.

Simple Transparency Mode

IWSVA's Forward Proxy 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.

For more details on the Simple Transparency Mode, see *HTTP Proxy in Simple Transparency Mode on page 2-16*.

WCCP 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.

For more details on the WCCP Mode, see *Deploying in WCCP Mode on page 2-22*.

Chapter 2

Deployment Primer

This chapter describes the following:

Identifying Your Server Placement

Before installing InterScan Web Security Virtual Appliance (IWSVA), you will need to review the IWSVA deployment modes and decide how to install IWSVA into your network environment to best meet your needs. This involves identifying where to place the IWSVA server in the network and identifying the best deployment mode for your network.

Today's enterprise network topologies typically fall into one of the following two categories:

- Two firewalls with a Demilitarized Zone (DMZ)
- One firewall without a DMZ.

The ideal location for the IWSVA server depends upon the topology in use.

Two Firewalls with DMZ

Given today's security concerns, many organizations have implemented a topology consisting of two firewalls (one external and one internal). These firewalls divide the network into two main areas:

- **The DMZ**—The DMZ is located between the external and internal firewalls. Hosts that reside in this area can accept connections from servers that are external to the organization's network. The configuration of the external firewall allows packets from external computers to reach only servers inside the DMZ.

- **Corporate LAN**—These segments are located behind the internal firewall. The configuration of the internal firewall passes traffic to machines on the corporate LAN only when the traffic originates from computers inside the DMZ.

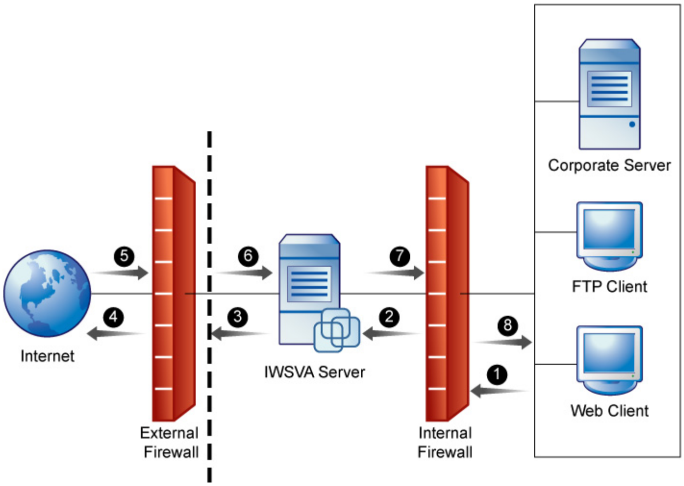


FIGURE 2-1. Two Firewalls with DMZ

This topology requires that all data inbound from the external servers (such as those on the Internet) first pass through a server in the DMZ. It also requires that certain types of data (for example HTTP and FTP packets), outbound from internal segments, pass through a server in the DMZ. This forces the use of proxies such as IWSVA.

One Firewall with No DMZ

Some organizations have a firewall, but no DMZ. When using the "no DMZ" topology, place the IWSVA server behind the firewall.

- Because the IWSVA server is not isolated from the corporate LAN, there is one less hop between external machines and machines on the corporate LAN. As shown in the diagram, this results in two less steps for processing a request, one outbound and one inbound.

- The firewall configuration allows connections to machines on the corporate LAN. For security, the firewall must limit the types of data that can reach machines on the LAN. For example, the firewall might allow HTTP data from the Internet to reach only the IWSVA server.

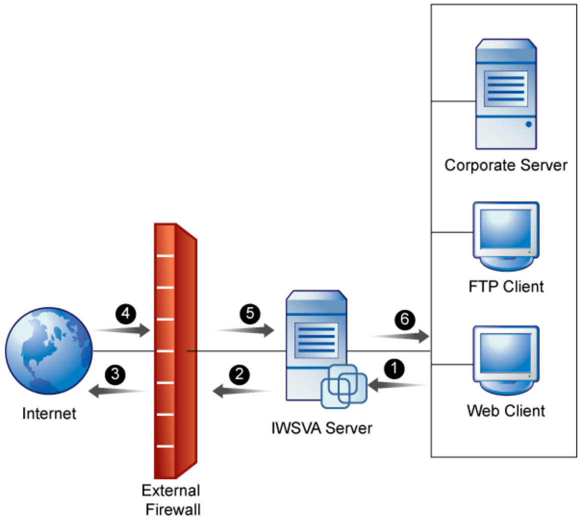


FIGURE 2-2. One Firewall with DMZ

Planning HTTP and FTP Service Flows

Network Traffic

To enforce the network traffic protection using IWSVA, an additional solution (hardware, software, or configuration) must be introduced that redirects the HTTP and FTP traffic to IWSVA. This solution includes the following:

- Reconfiguring client settings
- Using a Layer 4 switch
- Using an ICAP-enabled proxy
- Using WCCP
- Using a local Squid cache

See Appendix A, Deployment Integration starting on page A-1 for more details.

HTTP and FTP Service Flows

Each HTTP and FTP configuration has implications for configuring IWSVA, configuring the network, and for network security.

Create a flow plan for the HTTP and FTP services by doing the following:

- Understand each IWSVA service's purpose and function
- Determine each service's valid data sources. For example, does the HTTP service receive requests directly from the HTTP browsers, or indirectly through an ICAP proxy device?
- Determine which ports to use for the service. For instance, by default, the HTTP proxy service uses port 8080, and the FTP service uses port 21. However, if another application or service is using port 8080, the administrator must configure the HTTP proxy service to use a different port.
- Determine each service's valid data destinations. For example, does the HTTP proxy service send validated requests directly to the Web site? Or, does the HTTP proxy service send the validated request to an upstream HTTP proxy?
- Add in any service-specific considerations. For instance, the HTTP service flow might include an ICAP device, but the FTP service flow does not.

Using the information gathered in the previous paragraphs, administrators can determine which one of the possible flows is best to use for the installation.

Planning the HTTP Flow

The first step in planning the HTTP flow for IWSVA is choosing the way the HTTP traffic is processed by IWSVA (the deployment mode):

- HTTP Proxy
- ICAP device
- WCCP device
- Transparent Bridge
- Simple Transparency
- Reverse Proxy

The flow involving an ICAP or WCCP device is very different from the flows that do not involve ICAP or WCCP devices.

There are seven possible flows:

Transparent Bridge Settings

- **Transparent Bridge mode** — Use the transparent bridge mode when clients' computers are not configured to use the IWSVA server as their proxy, but still need to connect to the Internet through IWSVA.

Forward Proxy Settings:

- **Standalone mode** — Use this flow when ICAP devices are not being used with IWSVA, and IWSVA connects directly to the Internet.
- **Dependent mode** — Use this flow when ICAP devices are not being used with IWSVA, and IWSVA cannot connect directly to the Internet, but must instead connect through another HTTP proxy. This is can be accomplished in one of the following ways:
  - Proxy-ahead mode
  - Proxy-behind mode (not recommended)
  - Double-proxy mode
- **Forward Proxy with Transparency —** Use this mode when using an L4 (Load Balancing) switch.
- **WCCP** — Use the WCCP protocol in conjunction with WCCP enabled devices with IWSVA

Reverse Proxy Settings:

- **Reverse proxy mode —** Use this flow to protect a Web server with a proxy server by placing the HTTP proxy between the Internet and the Web server. (Used by ISPs and ASPs to protect the upload traffic against viruses and by organizations with complex Web sites that need a centralized point of access control.)

ICAP Proxy Settings:

- **ICAP protocol mode** — Use the ICAP protocol flow to use ICAP devices with IWSVA

Each configuration has implications for configuring IWSVA, configuring the network, and for network security.

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.

IWSVA supports HTTPS decryption and scanning in the following modes:

- Transparent bridge
- WCCP
- Forward proxy

Planning FTP Flows

There are two possible FTP flows: stand-alone and dependent. They are similar to the stand-alone and dependent-mode flows for HTTP service. Each requires a different configuration and has its own implications including:

- **Stand-alone**—the IWSVA server acts as an FTP proxy server between the requesting client and the remote site, brokering all transactions
- **Dependent**—IWSVA works in conjunction with another FTP proxy server within a LAN

FTP Proxy in Stand-alone Mode

To scan all FTP traffic in and out of the LAN, set up the FTP scanning module so that it “brokers” all such connections. In this case, clients FTP to the IWSVA server, supply the log on credentials to the target site, and then allow the IWSVA FTP server to make the connection. The remote site transfers the files to IWSVA FTP. Before delivering the files to the requesting clients, the IWSVA FTP server scans the files for viruses and other security risks.

The implications for the FTP stand-alone flow are:

- IWSVA must have access to the target FTP servers
- There is one less step in the flow, compared to the FTP proxy mode

To configure FTP clients to use this flow:

- Set the IWSVA server as a FTP proxy
- Set the username to be `username@targetftp-server`, instead of the normal username

Note: IWSVA FTP works with most firewalls, usually requiring only a modification to the firewall to open a port for the FTP proxy.

FTP requests follow this sequence:

1. The FTP client sends a request to the IWSVA FTP service.
2. The IWSVA FTP service validates the request (for example, the file type is not blocked). If the request is valid, the IWSVA FTP service attempts to connect to the appropriate FTP server on the Internet. If the connection succeeds, the IWSVA FTP service sends the request to the target FTP server.
3. The FTP server on the Internet responds to the request, ideally with the requested file.
4. The IWSVA FTP service scans the returned data for unwanted content. If it finds any unwanted content, it returns an appropriate message to the FTP client. Otherwise, it returns the requested data to the FTP client.

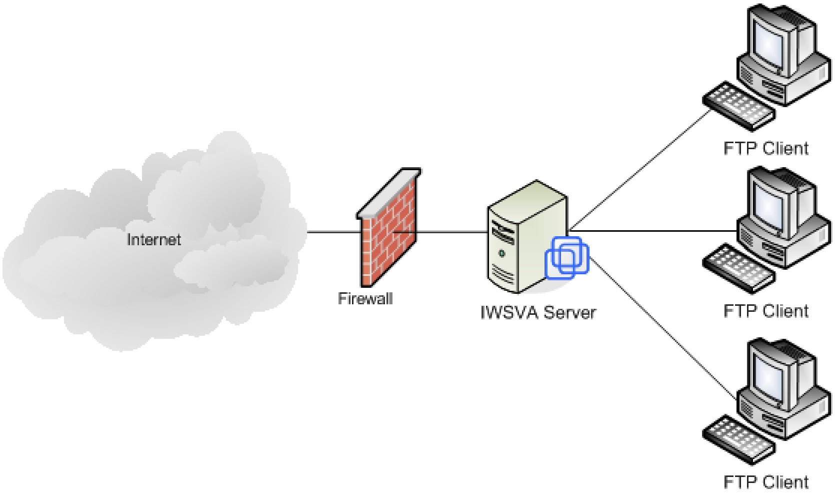


FIGURE 2-3. FTP Proxy in Standalone Mode

FTP Proxy in Dependent Mode

You can also install IWSVA FTP on a dedicated machine between an upstream proxy and the requesting clients. Using this setup adds other FTP features (for example, access blocking, logging, and filtering) to supplement the existing FTP proxy.

IWSVA's FTP-proxy mode, shown in *Figure 2-4*, is analogous to the dependent-mode flow of the HTTP service. Because it carries a performance penalty of an extra hop and extra processing by the other FTP proxy server, only use this mode if your organization does not allow the IWSVA Server to access the Internet directly.

If the other FTP proxy server uses a store-and-forward technique, the performance penalty is more noticeable on large files because the other FTP proxy first downloads the file and passes it on to the IWSVA FTP service. Additionally, the other FTP proxy must have sufficient free disk space to hold all transfers in progress.

Unlike the HTTP dependent-mode service, which has the possible benefit of cached requests, most FTP proxy servers do not cache requests.

FTP Dependent Mode also protects FTP servers from upload and download threats.

FTP requests follow this sequence:

1. The FTP client sends a request to the IWSVA FTP service.
2. The IWSVA FTP service validates the request (for example, the file type is not blocked). If the request is valid, the IWSVA FTP service relays it to the other FTP proxy or the FTP server being protected by IWSVA.
3. The FTP server on the Internet responds to the request, ideally with the requested file.
4. The IWSVA FTP service scans the returned data for unwanted content. If it finds any unwanted content, it returns an appropriate message to the FTP client. Otherwise, it returns the requested data to the FTP client.

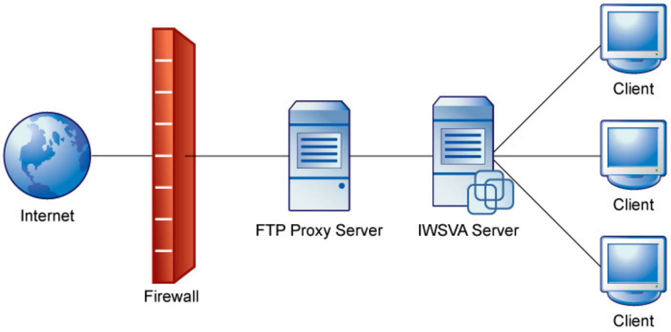


FIGURE 2-4. FTP Proxy in Dependent Mode

Deploying in Forward Proxy Mode

Overview of Forward Proxy Mode

There are two kinds of Forward Proxy: transparent and non-transparent. Transparent proxy can be achieved by a Layer 4 switch (Simple Transparency) or a WCCP-enabled switch (WCCP mode).

IWSVA configured in forward proxy mode provides the following configuration options to enable client protection:

- *Reconfiguring Client Settings on page 2-11*
- *Using a Layer 4 Switch on page 2-12*
- *Using a WCCP-enabled Switch or Router on page 2-14*

Additionally, when IWSVA is configured in this mode, all traffic can be configured to be sent to an additional upstream proxy server if applicable.

The configuration options are explored in the table that follows to provide information that will help you decide which deployment configuration to use.

During the IWSVA installation, select to install IWSVA in the Forward Proxy Mode to support this configuration.

Reconfiguring Client Settings

HTTP clients (browser or proxy servers) can be configured to contact IWSVA as a proxy. This configuration change ensures that the client's Web traffic is forwarded to IWSVA. The HTTP scanning service must be enabled in the HTTP Proxy mode to process this traffic.

FTP clients must contact IWSVA instead of the destination server, and use a modified handshake to supply the FTP server address. The FTP scanning module must be installed and configured in the standalone mode to process this traffic.

TABLE 2-1. Reconfiguring the Client Settings

ADVANTAGE	LIMITATION
No additional hardware required	Administrator have to control the settings for all computers. (Guest computers can have difficulties.)

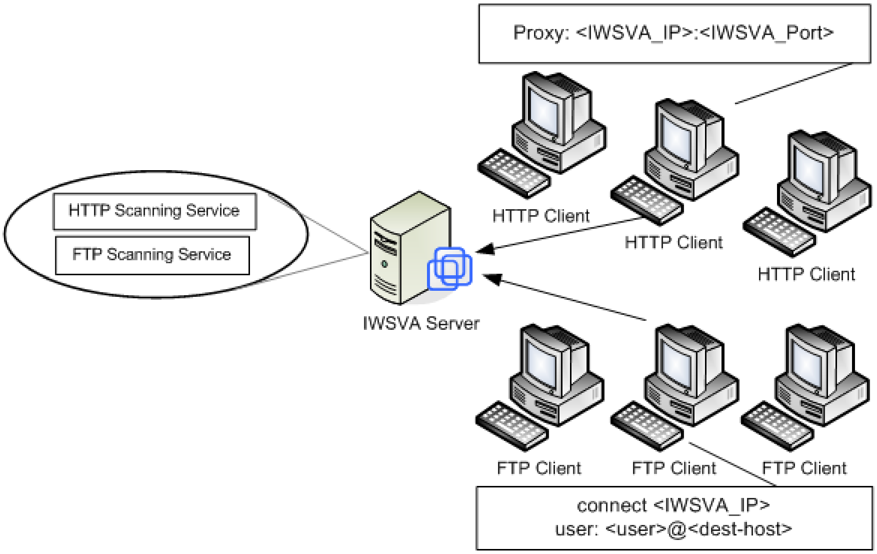


FIGURE 2-5. Reconfiguring the Client Settings

Using a Layer 4 Switch

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 the "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 addresses and host names; configuring policies based on LDAP is not possible.
- FTP over HTTP is not available; therefore, links to ftp:// URLs might not work if your firewall settings do not allow for FTP connections. Alternatively, links to ftp:// URLs might work, but the files will not be scanned.

- Simple transparency is not compatible with some older Web browsers when their HTTP requests do not include information about the host.
- HTTP requests for servers that use a port other than the HTTP default port 80 are redirected to IWSVA. This means SSL (HTTPS) requests are typically fulfilled, but the content is not scanned.
- Do not use any source NAT (IP masquerade) downstream of IWSVA, because IWSVA needs to know the IP address of the client to clean.
- A DNS server is needed for DCS to resolve the client machine name from its IP address in order to perform a cleanup.

A Layer 4 switch can be used to redirect HTTP traffic to IWSVA. The HTTP Scanning Service must be enabled in the HTTP Proxy mode.

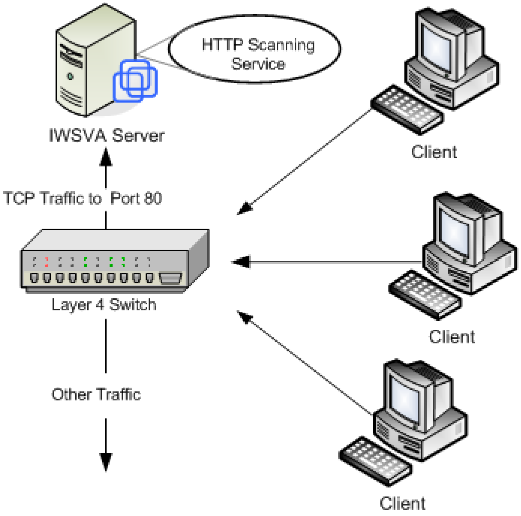


FIGURE 2-6. Using a Layer 4 Switch

During the installation, ensure that the check box that enables transparency to support this deployment mode is checked.

TABLE 2-2. Using a Layer 4 Switch

ADVANTAGES	LIMITATIONS
Transparent to clients	Traffic interception must be port-based (not protocol-based) for one port. If the non-standard port is used for HTTP, it bypasses the switch.
Simple to establish	The switch-based redirection cannot be used for the FTP traffic.
	No LDAP support

Using a WCCP-enabled Switch or Router

IWSVA supports WCCP v2.0 and forwarding methods based on GRE and L2 (layer 2).

When using WCCP transparency, FTP downloads are also scanned. With the ability to support WCCP v2.0, IWSVA is able to participate in a cluster of IWSVA devices to provide a load balancing WCCP Web security platforms.

Advantages of using WCCP:

- Transparency for the client side
- Scalable

Limitations of using WCCP:

- Cisco proprietary

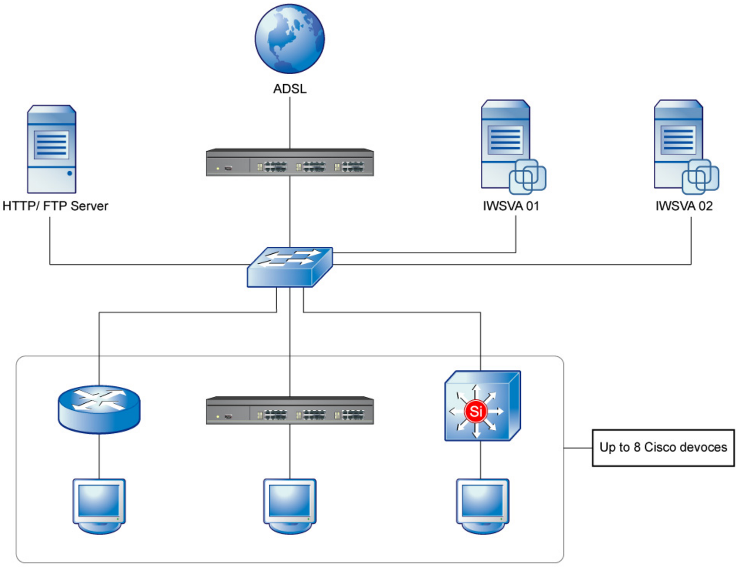


FIGURE 2-7. IWSVA deployment in a WCCP environment

Planning the HTTP Flow Using the Forward Proxy Mode

For complete details on implementing the Forward Proxy Mode, see *Forward Proxy Mode on page 1-9*.

HTTP Proxy in the Standalone 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. 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.

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

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP service.
2. The HTTP service validates the request, if the URL is not blocked. If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction. If the URL is valid, the HTTP service attempts to connect to the applicable Web server.
3. The contacted Web site returns a response from the Web server to the HTTP service.
4. The HTTP service scans the content for unwanted data and returns the appropriate response to the client.

TABLE 2-3. HTTP Proxy in Standalone Mode

ADVANTAGE	LIMITATION
Simple to install and manage.	Slow connection reaches maximum allowed connections limit.

HTTP Proxy in Simple Transparency Mode

Multiple IWSVA servers can be installed to balance your network traffic and scanning load. In this installation example, a Layer 4 switch receives clients requests and then forwards them to the IWSVA servers.

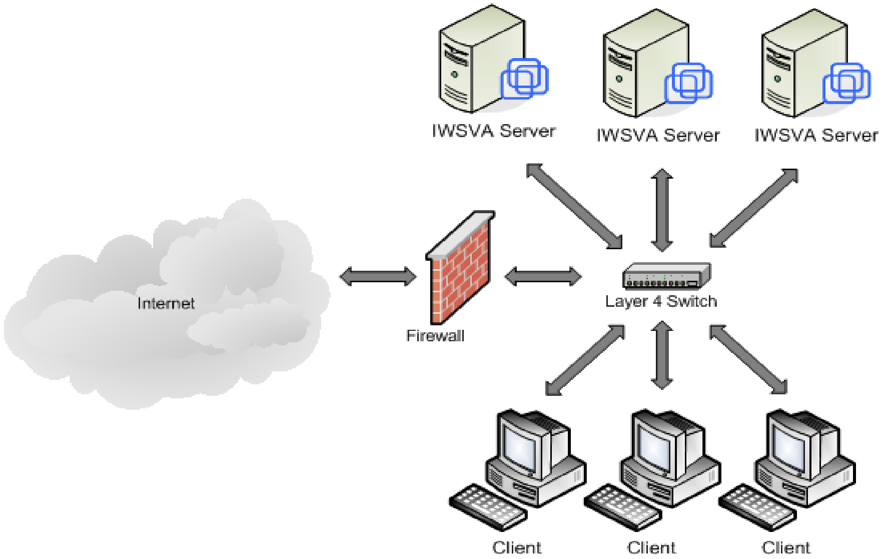
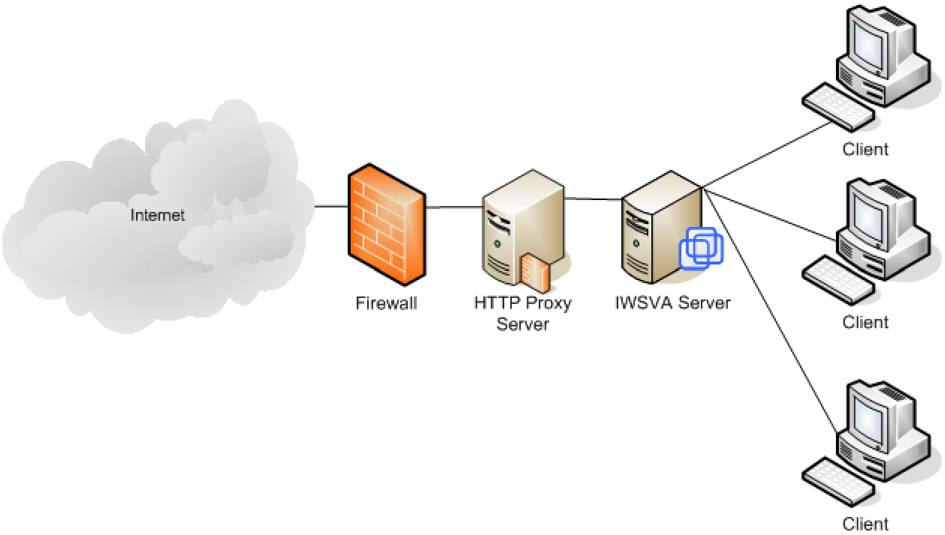


FIGURE 2-8. Use a Layer 4 switch to load balance between IWSVA servers in simple transparent mode

HTTP Proxy in Dependent Mode (Proxy Ahead)

For HTTP browsers to use this flow, configure the browsers to proxy through the IWSVA server, by default at port 8080.



HTTP Proxy in Dependent Mode (Proxy Ahead

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP service.
2. The HTTP service validates the request.
   - If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to an upstream HTTP proxy server.
3. The upstream proxy server performs its processing, then forwards the request to the Web site on the Internet.
4. The contacted Web site returns a response (ideally a Web page) to the HTTP proxy server.
5. The HTTP proxy server performs its processing on the returned data, then forwards the response data to the IWSVA HTTP service.

6. The HTTP service scans the content for unwanted data and returns an appropriate response to the HTTP client.

TABLE 2-4. HTTP Proxy in Dependent Mode (Proxy Ahead)

ADVANTAGES	LIMITATIONS
Proxy server controls timing and content availability behavior.	IWSVA has to scan every response-even when cached.
It is more secure—configuration changes will affect cached objects.	
IWSVA does not wait for the downloading of already cached objects.	

HTTP Proxy in Dependent Mode (Proxy Behind)

The proxy behind flow consists of a caching proxy placed between the HTTP client and the IWSVA server without using ICAP. Organizations typically use this flow to increase performance, as with ICAP.

WARNING! **Two security trade-offs exist for this potential performance enhancement:**

1. If the cache contains data with a virus, for which there was no pattern when the data hit the cache, the IWSVA HTTP service cannot prevent the spread of the virus.

2. Similarly, if a policy regarding valid content changes, or unauthorized users request data that exists in the cache (for authorized users), the HTTP service cannot prevent subsequent unauthorized access to this data.

Instead of using the proxy-behind flow, Trend Micro recommends that administrators use an ICAP caching device. This solution provides the performance enhancements of caching without the security issues of proxy-behind topology.

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP proxy server.
2. The proxy server forwards the request to IWSVA.
3. IWSVA validates the request using URL Filtering/URL Access Control:
    - If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
    - If the URL is valid, the HTTP service forwards the request to the Web server on the Internet.
4. The contacted Web server returns a response (ideally a Web page) to IWSVA.
5. IWSVA performs its processing on the returned data (virus, spyware, ActiveX scanning), then forwards the appropriate response/data to the proxy server.
6. The Proxy server caches the data (if cacheable), then delivers the response/data to the HTTP client.

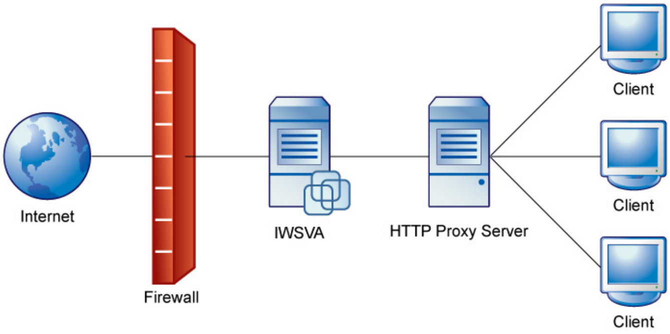


FIGURE 2-9. HTTP Proxy in Dependent Mode (Proxy Behind)

TABLE 2-5. HTTP Proxy in Dependent Mode (Proxy Behind)

ADVANTAGES	LIMITATIONS
No configuration changes required on the clients.	Configuration changes or pattern updates on IWSVA do not affect cached objects.

TABLE 2-5. HTTP Proxy in Dependent Mode (Proxy Behind) (Continued)

ADVANTAGES	LIMITATIONS
Cached objects are downloaded by clients directly from the Proxy server, which minimizes delays.	

HTTP Double Proxy in Dependent Mode

Double proxy configuration requires two caching proxies. The first proxy is placed between the HTTP client and the IWSVA server, and other one is placed between the IWSVA server and the Internet. This is typically used to get the advantages of the two configurations of the dependent modes: Proxy-ahead and Proxy-behind.

Web page requests follow this sequence:

1. The Web client sends a request to the first proxy server.
2. The first proxy server forwards the request to IWSVA.
3. IWSVA validates the request using URL Filtering/URL Access Control:
    - If the URL is invalid (blocked) the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
    - If the URL is valid, the HTTP service forwards the request to the second proxy server.
4. The second proxy server performs its processing, then forwards the request to the Web server on the Internet.
5. The contacted Web server returns a response (ideally a Web page) to second proxy server.
6. The second proxy server caches the data (if cacheable), then delivers the response/data to IWSVA.
7. IWSVA performs its processing on the returned data (Virus, Spyware, ActiveX scanning), then forwards the appropriate response/data to the first proxy server.

8. The first proxy server caches the data (if cacheable), then delivers the response/data to the HTTP client.

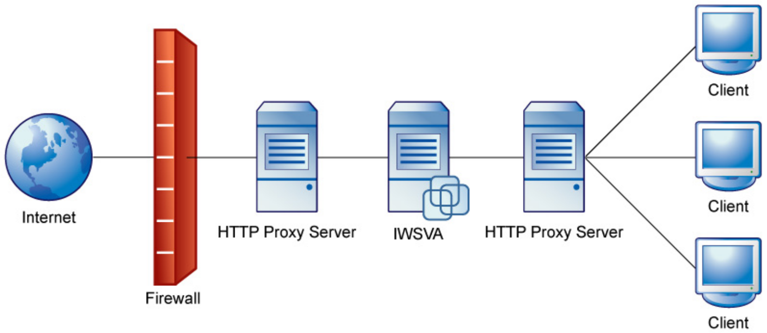


FIGURE 2-10. HTTP Double Proxy in Dependent Mode

TABLE 2-6. HTTP Double Proxy in Dependent Mode

ADVANTAGES	LIMITATIONS
Proxy server controls timing and content availability behavior.	Costs more—additional proxy servers are needed.
IWSVA does not wait for the downloading of already cached objects.	
No configuration change required on the clients.	

Deploying in WCCP Mode

HTTP Proxy in WCCP Mode (Single and Multiple IWSVA Servers)

IWSVA configured in the WCCP Mode processes Web page requests in the following sequence:

1. The Web client sends a request to the Web server.
2. The router intercepts the request and forwards the request to IWSVA.

3. IWSVA establishes a connection with the Web client.
4. IWSVA forwards the client requests to the Web server and establishes a connection with the Web server.
5. IWSVA begins sending data between the Web client and the Web server.
6. If the data has no virus, then IWSVA sends the data to the Web client.
7. If the data has a virus, then IWSVA sends the blocked page to the Web client.

Deploying in ICAP Mode

Overview of ICAP Mode

Internet Content Adaptation Protocol (ICAP) is designed to forward an HTTP response or request to third-party processors and collect the results. The component that sends the ICAP request is called the *ICAP-client*. A component that processes the request is called an *ICAP-server*.

When IWSVA is configured in ICAP mode, it processes requests from any ICAP-compliant client. Officially, Trend Micro supports the following ICAP version 1.0 implementations: NetCache, Blue Coat, Cisco Content Engines (CE), and Squid.

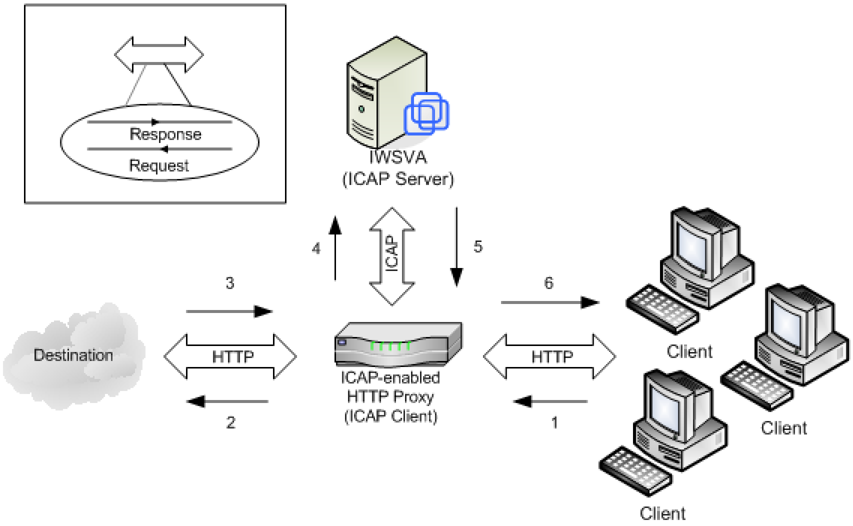


FIGURE 2-11. Using an ICAP-enabled Proxy

TABLE 2-7. ICAP-enabled Proxy

ADVANTAGES	LIMITATIONS
ICAP allows scanning of only new and necessary content.	Up front cost of ICAP equipment.
Reduced and selective scanning enhances performance	Adds extra steps in the IWSVA installation process.
Increased resource efficiencies reduce the number of IWSVA server hardware needed.	Requires management.

Planning the HTTP Flow Using the ICAP Mode

For complete details on implementing the ICAP Mode, see *ICAP Mode on page 1-10*.

HTTP Proxy in ICAP Mode (Single and Multiple IWSVA Servers)

This section discusses the flow of a typical HTTP GET request using both an ICAP device and IWSVA servers. In these flows, IWSVA interacts with the ICAP device, in response to ICAP rules. This is very different from other flows where IWSVA receives URL requests from HTTP clients. To use these flows for HTTP browsers, configure the browsers to use the ICAP device as the HTTP proxy.

Using ICAP devices can enhance performance in two ways:

- **Caching good data**—If the data is clean, the ICAP device caches the data. Subsequent requests require only four steps, not eight. (ICAP must still ask IWSVA to check the policies to validate that the users making the subsequent requests can browse the data, have not exceeded their quota, and so on.)
- **Clustered IWSVA servers**—When multiple IWSVA servers are used, the ICAP device load balances the requests between the servers. This is vital for enterprise environments where the demand for scanning incoming pages can overwhelm a single IWSVA server. With ICAP, the ICAP device performs load balancing, and receives maximum performance from the available IWSVA servers.

Note: Non-ICAP environments can receive similar benefits by using multiple IWSVA servers. However, the administrator must utilize additional load balancing technology.

When IWSVA is configured in ICAP mode, it processes requests from any ICAP-compliant client. Trend Micro supports the following ICAP client implementations:

- NetCache
- Blue Coat
- Cisco Content Engines
- Squid

Although IWSVA performs the same filtering of URLs and scanning of data for unwanted content, the ICAP flow is so different from the other flows that it requires a completely different communications protocol. Administrators indicate which protocol (ICAP or non-ICAP) to use during post-installation configuration.

The figures that follow show the HTTP flow with single and multiple IWSVA servers. (Both images assume the requested data is not in the ICAP device's cache.) The ICAP service determines which IWSVA server receives the request in a multi-server environment.

IWSVA configured in ICAP Mode processes Web page requests in the following sequence:

1. An HTTP client makes a request for a URL, sending the request to the ICAP caching proxy device.
2. The ICAP device, based on its configuration, determines that the request must be forwarded to an IWSVA server. If multiple servers are available, it alternates in round-robin fashion for load balancing.
3. The IWSVA server validates the URL.
   - If the URL is not blocked, IWSVA sends the response to the ICAP device.
   - If the URL is invalid (blocked), IWSVA directs the ICAP device to send an appropriate response to the HTTP client and the transaction is complete.
4. If the URL is valid, the ICAP server requests the page from the Web site on the Internet.
5. The Web site on the Internet returns the requested page (or some other appropriate response).
6. If the page is returned, the ICAP device, based on its configuration, determines that an IWSVA server must scan the data. Again, if multiple servers are available, it alternates in round-robin fashion for load balancing.
7. The IWSVA server scans the results and returns an appropriate response to the ICAP device, based on whether the data is clean or contains unwanted content.
8. If the data is clean, the ICAP device returns said data to the HTTP client, and the ICAP device retains a copy of the data to satisfy future requests. If the data contains unwanted content, the ICAP device returns an appropriate error message (dictated

by IWSVA) to the HTTP client, and the ICAP device does not retain a copy for future requests.

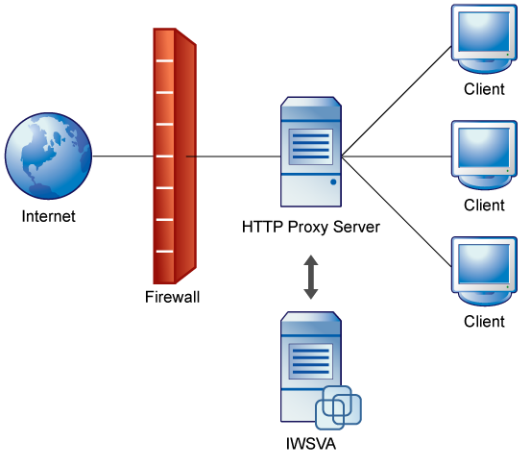


FIGURE 2-12. HTTP Proxy in ICAP Mode (Single IWSVA Server)

IWSVA ICAP Mode with Multiple Servers

If there is already a content cache server on your network, then Trend Micro recommends installing the ICAP HTTP handler. The following diagram shows the installation topology for IWSVA ICAP with multiple servers. For multiple IWSVA ICAP servers to work properly, their corresponding pattern, scan engine version, and `intscan.ini` files must be identical.

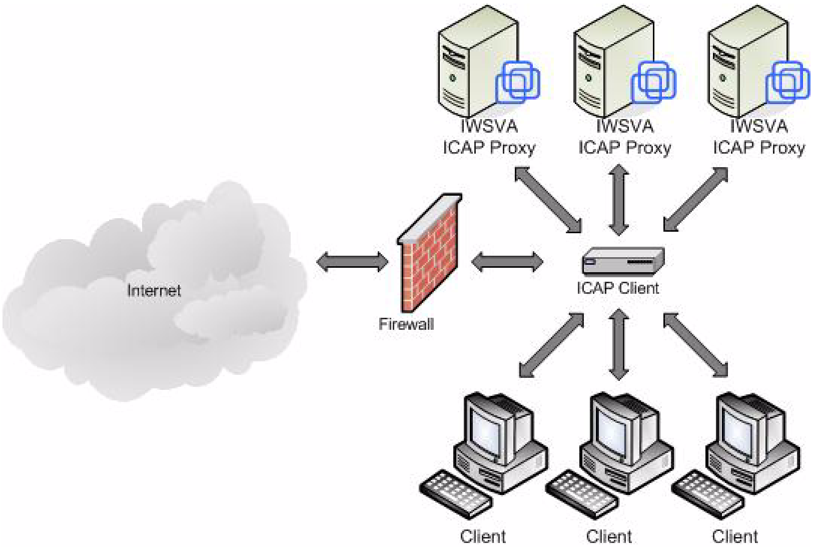


FIGURE 2-13. HTTP Proxy in ICAP Mode (Multiple IWSVA Servers)

TABLE 2-8. HTTP Proxy in ICAP Mode

ADVANTAGES	LIMITATIONS
No configuration changes required on the clients.	Configuration changes on IWSVA affects cached objects.
Cached objects are downloaded by clients directly from the Proxy server, which minimizes delays, and improves performance.	
Load-balancing is possible after some configuration to the clients.	

Deploying in Reverse Proxy Mode

Overview of Reverse Proxy Mode

IWSVA is usually installed close to clients to protect them from security risks from the Internet. However, IWSVA also supports being installed as a reverse proxy to protect a Web server from having malicious programs uploaded to it. In Reverse Proxy Mode, IWSVA is installed close to the Web server that it protects. In this mode, IWSVA protects a Web server with the proxy server. The HTTP proxy is placed between the Internet and the Web server. This is useful when the Web server accepts file uploads from clients, or to reduce the load of each Web server by balancing the load among multiple Web servers. ASPs/ISPs can use IWSVA as an HTTP proxy to protect the upload traffic against viruses, and organizations with complex Web sites need it as a centralized point of access control.

IWSVA receives clients requests, scans all content and then redirects the HTTP requests to the real Web server. This flow is especially useful for Web sites involved in e-commerce transactions, distributed applications that exchange data across the Internet, or other situations where clients upload files to the Web server from remote locations.

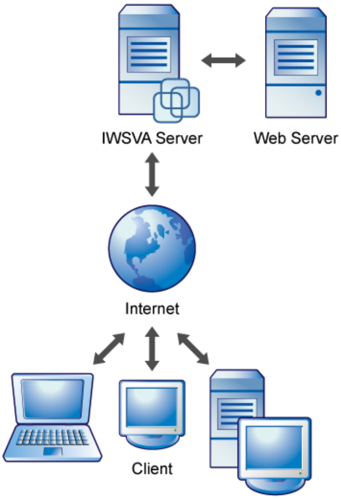


FIGURE 2-14. Reverse proxy protects Web server from clients

Planning the HTTP Flow Using Reverse Proxy Mode

For complete details on implementing the Reverse Proxy Mode, see *Reverse Proxy Mode on page 1-10*.

HTTP Reverse Proxy in Dependent Mode

In reverse proxy mode, the HTTP proxy acts as the Web server to the client systems. The proxy receives all requests and transfers them to the real Web server. Consequently, all HTTP traffic goes through the HTTP proxy, enabling the proxy to scan the content and block any infected transactions.

Note: Administrators should be aware of the following:
- The URL-filtering feature makes no sense in this configuration; only antivirus scanning and URL-blocking are useful.
- In the reverse proxy mode, the Web server's access log is useless. To analyze the connections for the Web site, you must use the IWSVA access log.
- Ideally, the reverse proxy server should be placed behind a firewall, but in many cases, the proxy is connected directly to the Internet, where it is more vulnerable to direct attacks. When a reverse proxy is configured without a firewall, administrators should take all appropriate precautions in securing the operating system hosting IWSVA.

IWSVA configured in Reverse Proxy Mode processes Web page requests in the following sequence:

1. Clients initiate the Web request.
2. The request is received by Trend Micro™ InterScan™ Web Security Virtual Appliance, and configured to listen on port 80.
3. Trend Micro™ InterScan™ Web Security Virtual Appliance scans the content, then forwards it to an actual Web server.
4. The Web server delivers the requested page back to IWSVA.
5. Trend Micro™ InterScan™ Web Security Virtual Appliance rewrites the page headers, and sends on the request.

6. The modified page returns to the requestor.

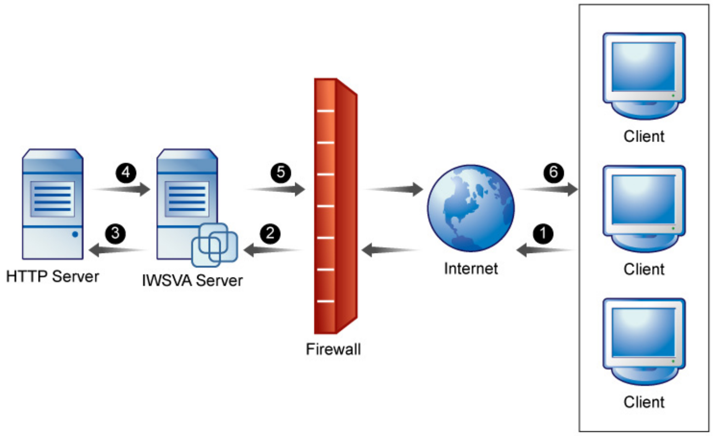


FIGURE 2-15. HTTP Reverse Proxy in Dependent Mode

TABLE 2-9. HTTP Reverse Proxy in Dependent Mode

ADVANTAGES	LIMITATIONS
IWSVA scans all objects before they are cached.	New engines, patterns, and configurations will not affect cached objects.
	The access logging feature of IWSVA is compromised.

Deploying in Transparent Bridge Mode

Overview of Transparent Bridge Mode

In the Transparent Bridge Mode, IWSVA acts as a bridge between two network devices (switch, router, or firewall) and transparently scans HTTP(s) and FTP traffic. Transparent Bridge Mode is the simplest way to deploy IWSVA into an existing network topology and does not require modifications to clients, routers, or switches. IWSVA acts as a "bump in the wire" and scans for malware. Two network cards are required for IWSVA to be configured in Transparent Bridge Mode.

The benefit of the Transparent Bridge Mode is that client's HTTP(s) 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.

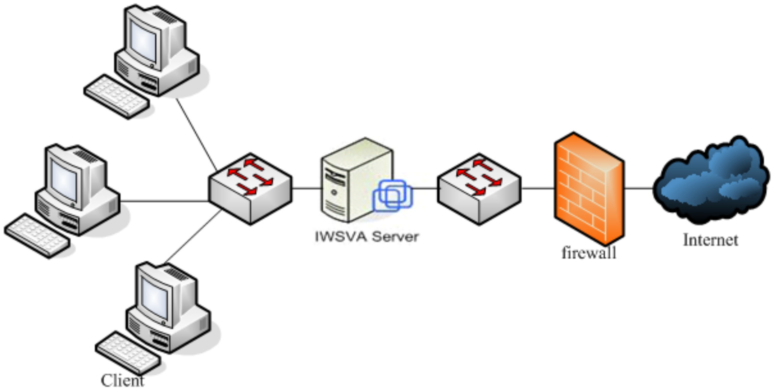


FIGURE 2-16. Typical bridge mode deployment

Planning the HTTP Flow Using Transparent Bridge Mode

For complete details on implementing the Forward Proxy Mode, see *Transparent Bridge Mode on page 1-9*.

IWSVA configured in Transparent Bridge Mode processes a Web page requests in the following sequence:

1. The Web client sends a request to the Web server.
2. IWSVA accepts the connection from client and sends the request to the Web server.
3. IWSVA establishes a connection with the Web client.
4. IWSVA establish the connection with the Web server and gets data from the Web server.
5. If the data contains no viruses, then IWSVA sends the data to the Web client.
6. If the data contains a virus, then IWSVA sends the blocked page to the Web client.

Chapter 3

Installing InterScan Web Security Virtual Appliance

This chapter explains the following:

- *Operating System Requirements on page 3-2*
- *Component Installation on page 3-2*
- *Obtaining IWSVA on page 3-3*
- *Installing IWSVA on page 3-4*
- *Logging in to IWSVA for the First Time on page 3-12*
- *Post-Installation Notes on page 3-12*

Operating System Requirements

InterScan Web Security Virtual Appliance (IWSVA) provides a purpose-build, hardened and performance tuned 64-bit operating system as part of the installation process. This dedicated operating system installs with IWSVA to provide a turn-key solution—a separate operating system such as Linux, Windows, or Solaris is not required.

Component Installation

During installation, the following Trend Micro components are automatically installed:

- **Main Program**—Management console and the basic library files necessary for IWSVA.
- **HTTP Scanning**—Service necessary for HTTP scanning (either ICAP or HTTP proxy) and URL blocking.
- **FTP Scanning**—Service necessary for FTP scanning.
- **URL Filtering**—Service necessary for URL filtering.
- **Applets and ActiveX Scanning**—Service necessary for scanning Java applets and ActiveX controls.
- **IntelliTunnel Security**—Services to block communication provided by certain Instant Message (IM) protocols and certain authentication connection protocols.
- **SNMP Notifications**—Service to send SNMP traps to SNMP-compliant network management software.
- **Control Manager Agent for IWSVA**—Files necessary for the Control Manager agent. You need to install the agent if you are using Control Manager (Trend Micro's central management console).
- **Command Line Interface**—A custom CLI shell to manage IWSVA from the command line, either by TTY or SSH.

During installation, the following open-source application is installed for convenience, but is not enabled by default:

- **Squid**—To provide optional content caching.

Obtaining IWSVA

IWSVA is supported on the following platforms:

- Bare Metal installation (dedicated off-the-shelf server platform without an operating system)
- VMware ESX 3.5/4.0 or ESXi 3.5/4.0 as a virtual machine

Trend Micro recommends that you evaluate the method of installation that best suits your environment.

You can install IWSVA from the Trend Micro Enterprise Solutions DVD or download the installation ISO from the Trend Micro IWSVA download location (http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=250&regs=NABU&lang_loc=1). The DVD is available to purchase and contains the installation files and all documentation.

Using the Trend Micro Enterprise Solutions DVD

To complete this installation, you need to create a bootable installation DVD that contains the IWSVA ISO file.

Procedure:

1. To create the installation media, insert the Trend Micro Enterprise Solution disk into the DVD drive on the computer where ISO images can be created.
2. Copy the IWSVA ISO image from the Trend Micro Enterprise Solutions Media onto the local hard drive.
3. Eject the Enterprise Solutions DVD and place a blank DVD disk into the DVD writer.
4. Burn the IWSVA ISO image to the blank DVD.
5. Insert the newly created IWSVA Installation DVD into the target server where you would like to install IWSVA.
6. Reboot the server and boot from the IWSVA installation DVD to begin the installation process.

Note: The file on the Enterprise DVD and on the Trend Micro Evaluation site is an ISO image. The ISO image allows you to create an IWSVA installation DVD to install the product.

Downloading an Evaluation Version

Procedure:

1. Go to the Trend Micro download Web page and download IWSVA.
   `http://www.trendmicro.com/download/product.asp?productid=86`
2. Download the IWSVA ISO.
3. Burn the IWSVA ISO image to the blank DVD.
4. Insert the newly created IWSVA Installation DVD into the target server where you would like to install the IWSVA application.

   WARNING! **IWSVA does not support installation using an external USB DVD drive.**

5. Reboot the server and boot from the IWSVA installation DVD to begin the installation process.

Note: The ISO image needs to be copied and then burned onto a blank DVD in order to create the IWSVA installation DVD (See the DVD ISO creation document, *How to Use the Trend Micro IWSVA ISO File.*)

Installing IWSVA

IWSVA only supports new installations or migrations from specific versions. In-place upgrades of an existing IWSS or IWSA installation is not supported.

IWSVA supports migrating existing configuration and policy data from IWSS 3.1 (Linux or Windows), IWSVA 3.1, IWSVA 5.0, and IWSVA 5.1 products (see Migration on page 1-6). Existing log and report files are not migrated. If you need to retain existing IWSx 3.1 log and report information, perform the necessary backup of these files before proceeding with the installation and migration.

The IWSVA installation process formats your existing system to install IWSVA. The installation procedure is basically the same for both the Bare Metal and the VMware ESX virtual machine platforms. The Bare Metal installation simply boots off of the IWSVA installation DVD to begin the procedure and the VMware installation requires the creation of a virtual machine before installation. The additional VMware virtual machine configuration is described in Appendix E, *Creating a New Virtual Machine Under VMware ESX for IWSVA on page E-1*.

WARNING! **Any existing data or partitions are removed during the installation process. Backup any existing data on the system (if any) before installing IWSVA.**

IWSVA also installs a copy of the open source content caching application called *Squid*. It is disabled by default but you can enable this free open-source utility through the IWSVA administration Web UI. Trend Micro provides Squid content caching for convenient and easy installation. Support for Squid is provided by the Squid open-source community.

Trend Micro Disclaimer: Trend Micro IWSVA preinstalls Squid and provides the basic configuration and statistical reports to help reduce the complexity of installing and configuring Squid to function with IWSVA. Squid is disabled by default and must be enabled by the customer through the IWSVA administration user interface after installation has been completed. Support for Squid is obtained through open source channels and it is the responsibility of the customer to become acquainted with Squid's benefits and functionality before enabling.

Additional information, documentation, and support on the Squid application can be found at the official Squid Web Proxy Cache Web site: `www.squid-cache.org`. Trend Micro will not provide support for Squid's features, but will provide support for the setup and integration of Squid and IWSVA through its supplied configuration commands.

To install IWSVA:

1. Start the IWSVA installation.

Installing on a Bare Metal Server

Insert the IWSVA Installation DVD (which was created from the IWSVA ISO image) into the DVD drive of the desired server.

Note: Because IWSVA does not support external USB CD/DVD drives, a “Cannot find kickstart file on DVD-ROM” warning message displays when installing IWSVA. You can safely ignore this warning message.

IWSVA does not support installation using an external USB DVD drive.

Installing on a VMware ESX Virtual Machine

a. Create a virtual machine on your VMware ESX server.

See Appendix E, *Creating a New Virtual Machine Under VMware ESX for IWSVA on page E-1*.

b. Power on the virtual machine that was created to boot from the IWSVA installation ISO.

Note: If your computer boots from an ISO image (such as ISOLINUX), you need to press [ENTER] at the bootloader prompt to continue with the IWSVA installation process.

Installation Steps for both a VMware ESX Virtual Machine and a Bare Metal Server

Note: IWSVA does not need a network connection during installation, but it must connect with the Internet when using the Deployment Wizard after the installation completes.

A page appears displaying the IWSVA Installation Menu. The options on this menu are as follows:

- **Install IWSVA**: Select this option to install IWSVA onto the new hardware or virtual machine.
- **System Recovery**: Select this option to recover an IWSVA system in the event that the administrative passwords cannot be recovered.
- **System Memory Test**: Select this option to perform memory diagnostic tests to rule out any memory issues.
- **Exit Installation**: Select this option to exit the installation process and to boot from the local disk.

2. Select **Install IWSVA**.

   The license acceptance page appears. From this page, you can access the readme (**Readme** button).

3. Click **Accept** to continue.

   A page appears where you choose a keyboard language.

4. Select the keyboard language for the system and then click **Next**.
5. Select the driver(s) used for installation and then click **Next**.

   The IWSVA installer scans your hardware to determine if the minimum specifications have been met and then displays the results illustrated as follows. If the host hardware contains any components that do not meet the minimum specifications, the installation program highlights the nonconforming components and the installation stops.

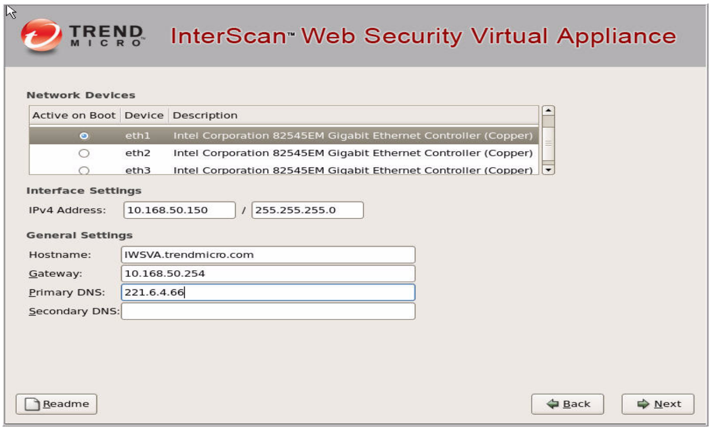
6. Click **Next** to continue.

   A page appears where you specify network devices, hostname, and miscellaneous settings. If you choose to set the hostname manually, the Miscellaneous Settings will be available to you.

Note: You must assign a valid hostname to the IWSVA server for it to function properly.

7. Select the network devices and input the corresponding IP addresses.

Note: After installing the IWSVA OS, you can access the IWSVA web console using the NIC you select, then run the Deployment Wizard to complete the necessary configuration. Also, you can use the Deployment Wizard to change the existing network settings.



Network Devices

Active on Boot	Device	Description
●	eth1	Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
○	eth2	Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
○	eth3	Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)

Interface Settings

IPv4 Address: 10.168.50.150 / 255.255.255.0

General Settings

Hostname: IWSVA.trendmicro.com

Gateway: 10.168.50.254

Primary DNS: 221.6.4.66

Secondary DNS:

FIGURE 3-1. Page to specify network devices, hostname, and miscellaneous settings

8. Configure the network settings as required for IWSVA and then click **Next**.
9. Specify the time zone for IWSVA on the time zone page.

   Use the drop-down list to display the supported time zones or point to your location using the time zone map.
10. Click **Next**.
11. Specify passwords for the root account and the enable account.

    IWSVA uses three different levels of administrator types to secure the system.

    Passwords for accounts must be a minimum of six characters and a maximum of 32 characters. For best security, create a highly unique password only known to you. You can use both upper and lower case alpha characters, numerals, and any special characters found on your keyboard to create your passwords.

- **Root Account:** The Root account is used to gain access to the operating system shell and has all rights to the server. This is the most powerful user on the system.
- **Enable Account:** The Enable account is used to gain access to the command line interface's privilege mode. It has all rights to execute any CLI command.
- **Admin Account:** The Admin account is the default administration account used to access the IWSVA Web and CLI management interfaces. It has all rights to the IWSVA application, but no access rights to the operating system shell. It has a default username ("admin") and password, which is adminIWSS85.

Note: The Admin Account is not displayed here. It is setup with a default password at the end of the installation process. Although the Admin Account is not displayed or prompted during the installation process, it is part of the three-admin account system employed by IWSVA. after the initial installation is complete, please log in IWSVA web console change admin account password.

As you type the passwords, the password strength meter on the right indicates how strong the selected password is. For the best security, Trend Micro recommends using a strong, unique password.

12. Click **Next**.

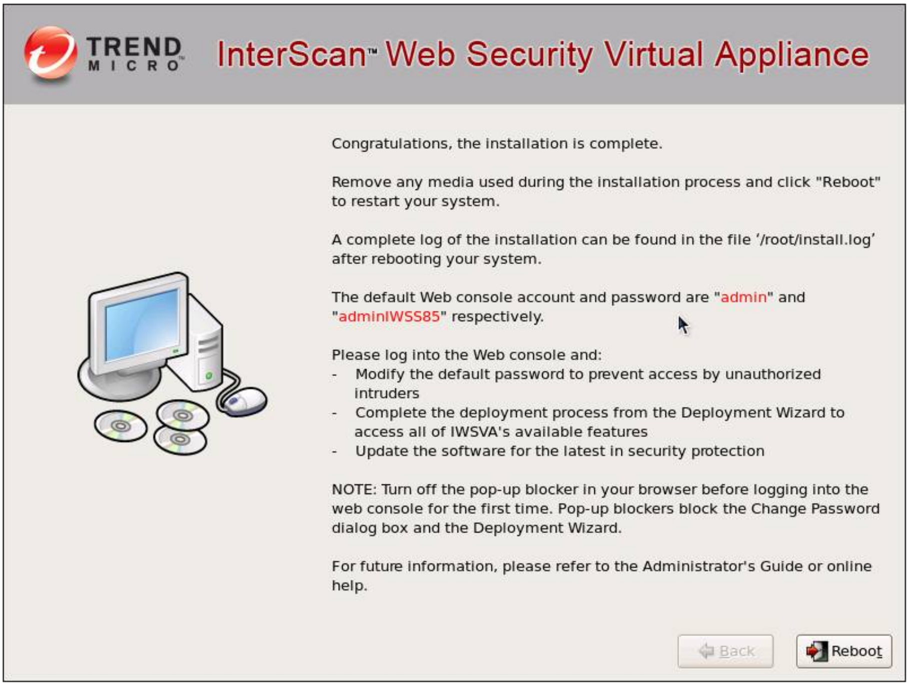
    A page appears where you accept all the configuration settings.

13. Confirm that the selected values are correct and then click **Next**.

    The installation process prompts you to begin the installation. Selecting **Continue** erases any data on the hard disk partition and formats the hard disk. If you have data on the hard disks that you would like to keep, cancel the installation and backup the information before proceeding.

14. Click **Continue**.

    A page appears that provides the formatting status of the local drive for the IWSVA installation. When formatting completes, the IWSVA installation begins.



Congratulations, the installation is complete.

Remove any media used during the installation process and click "Reboot" to restart your system.

A complete log of the installation can be found in the file '/root/install.log' after rebooting your system.

The default Web console account and password are "admin" and "adminIWSS85" respectively.

Please log into the Web console and:
- Modify the default password to prevent access by unauthorized intruders
- Complete the deployment process from the Deployment Wizard to access all of IWSVA's available features
- Update the software for the latest in security protection

NOTE: Turn off the pop-up blocker in your browser before logging into the web console for the first time. Pop-up blockers block the Change Password dialog box and the Deployment Wizard.

For future information, please refer to the Administrator's Guide or online help.

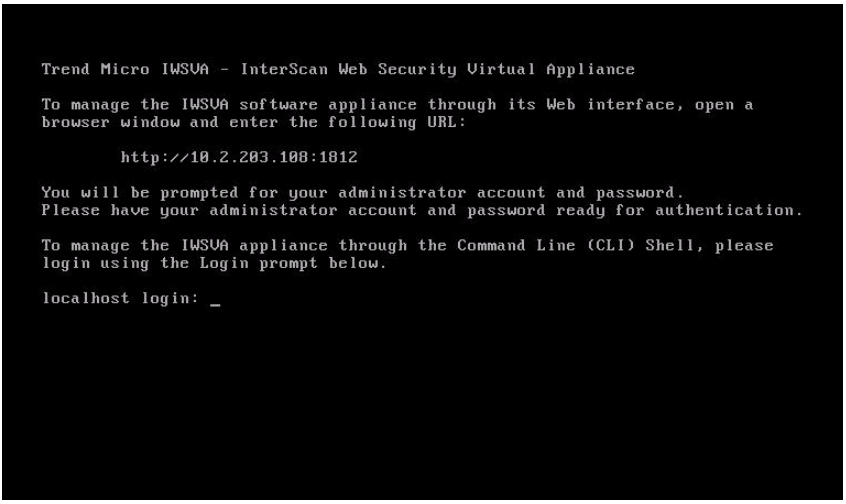
FIGURE 3-2. Summary screen contains default password.

After the installation is complete a summary screen appears. The installation log is saved in the `/root/install.log` file for reference.

15. Click **Reboot** to restart the system.

- **For a bare metal installation:** The DVD automatically ejects. Remove the DVD from the drive to prevent reinstallation.
- **For a virtual machine installation:** Trend Micro recommends disconnecting the DVD-ROM device from the virtual machine now that IWSVA is installed.

After IWSVA reboots, the initial CLI log in screen appears. (See *Figure 3-3*.)



```
Trend Micro IWSVA - InterScan Web Security Virtual Appliance

To manage the IWSVA software appliance through its Web interface, open a
browser window and enter the following URL:

        http://10.2.203.108:1812

You will be prompted for your administrator account and password.
Please have your administrator account and password ready for authentication.

To manage the IWSVA appliance through the Command Line (CLI) Shell, please
login using the Login prompt below.

localhost login: _
```

FIGURE 3-3. The initial CLI log in screen

Note: During installation, you might receive the following messages:

```
for crash kernel (0x0 to 0x0) not within permissible range
powernow-k8: bios error -no psb or acpi_pss objects
```

Both of these messages are normal. The latter message indicates that the system BIOS is not reporting or presenting any PSB or ACPI objects or hooks to the Linux kernel. Either the CPU or BIOS does not support PSB or ACPI objects or hooks or they are simply disabled.

16. Prepare to log into the IWSVA web console by disabling the pop-up blocker in your browser.

Note: Pop-up blockers block the Change Password dialog box and the Deployment Wizard which are launched during the first-time login.

17. Log in to the IWSVA Web console to launch IWSVA.

See Logging in to IWSVA for the First Time on page 3-12 for details.

Logging in to IWSVA for the First Time

After IWSVA has restarted, you can log in to the appliance either through the CLI or the Web management interface.

- For the CLI interface, type in your administrator username and password at the console login prompt.

> **Note:** Turn off the pop-up blocker in your browser before logging into the web console for the first time. Pop-up blockers block the Change Password dialog box and the Deployment Wizard.

- For the Web management interface, on your workstation (not IWSVA) open a new Web browser and then type in the URL (`http://<IWSVA 5.1IP address>:1812`) indicated in the initial CLI banner. You will need the IWSVA administrator account and password to log in. The default administrator account name is "admin" and the default password is adminIWSS85.

Post-Installation Notes

After IWSVA reboots and the initial CLI is available:

- The Deployment Wizard launches when you first log into the Web console. Use the Deployment Wizard to complete your installation. (See the Administrator's Guide, Chapter 2.)
- Trend Micro recommends that you update your scan engine and virus pattern files immediately after registering and activating the product. (See the Administrator's Guide, Chapter 3.)

Chapter 4

On-box Upgrade from InterScan Web Security Virtual Appliance 5.0 to 5.1

This chapter describes the following:

About Upgrading

The on-box (or in-place) upgrade from IWSVA 5.0 to IWSVA 5.1 provides an easy method for IWSVA administrators to upgrade from the IWSVA web console. After upgrading, the related configurations set through the web console and CLI, as well as data generated by IWSVA 5.0 will be kept in IWSVA 5.1, such as text and database logs, and configuration information. Hidden settings introduced through hot fixes may be lost.

If a power failure interrupts the upgrade process, administrators can recover the system to the status before upgrade without losing data.

Previous versions of IWSVA required exporting system configuration information, re-installing the new version, and importing the configuration information. The new upgrade method eliminates this step and retains all critical data and log information.

Note: The on-box upgrade is available only when upgrading from IWSVA 5.0 to IWSVA 5.1. For upgrades to IWSVA 5.1 from pre-IWSVA 5.0 versions, see Installing InterScan Web Security Virtual Appliance on page 3-1 and Migrating to InterScan Web Security Virtual Appliance on page 5-1.

Retained Data and Configurations

The on-box upgrade retains all critical data and configuration information. Exceptions are listed in:

- Data Not Retained on page 4-2
- Configurations Not Retained on page 4-3

Data Not Retained

The following unnecessary data will not be retained:

- Patterns and engines of AU
- Core dump files and system information files generated from the Administration > Support page of the IWSVA web console.
- Installed patch information configured at Administration > System Patch.
- OS version information configured at Administration > Update OS.

Configurations Not Retained

All critical configuration information is retained, except the following security certificate information from the scanning modules:

- HTTPS decryption certificate authority (See HTTP >HTTPS Decryption >Settings)
- Applet re-signing certificate (See HTTP > Applets and ActiveX > Settings)

WARNING! This above information must be backed up before beginning the on-box upgrade process. Paths shown are for IWSVA 5.0.

Administrators must manually import these certificate exceptions after IWSVA 5.1 installs successfully.

With the integrated Squid support in IWSVA 5.1, Squid is supported in upstream mode when enabled from the management UI. This allows IWSVA to scan all cached content before delivery to the users and ensures that all content is safe and secure. If you have Squid enabled with a previous IWSVA version, please be aware that downstream mode and its related CLI configuration commands are no longer available in IWSVA 5.1. Please use the web console to enable Squid caching in upstream mode.

Note: The IWSVA 5.0 Activation Code will be used.

On-box Upgrade from IWSVA 5.0 to IWSVA 5.1

To perform the on-box upgrade, IWSVA 5.1 delivers an upgrade package in the form of an OS patch. To download the upgrade package, visit: http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=result_page&clkval=drop_list&catid=4&prodid=86

Note: Trend Micro recommends backing up your existing settings on IWSVA 5.0 before applying the on-box upgrade patch.

To backup the existing IWSVA 5.0 settings:
- Access the IWSVA 5.0 web console.
- Select **Administration > Config Backup/Restore.**
- Click **Export**.The screen displays a progress bar. When the export process finishes, a results page displays the status. If configuration export is successful, IWSVA opens a dialog box to prompt you to save the configuration file to a local disk.
- Save the file to a local drive on your computer.

To perform an on-box upgrade from IWSVA 5.0 to IWSVA 5.1:

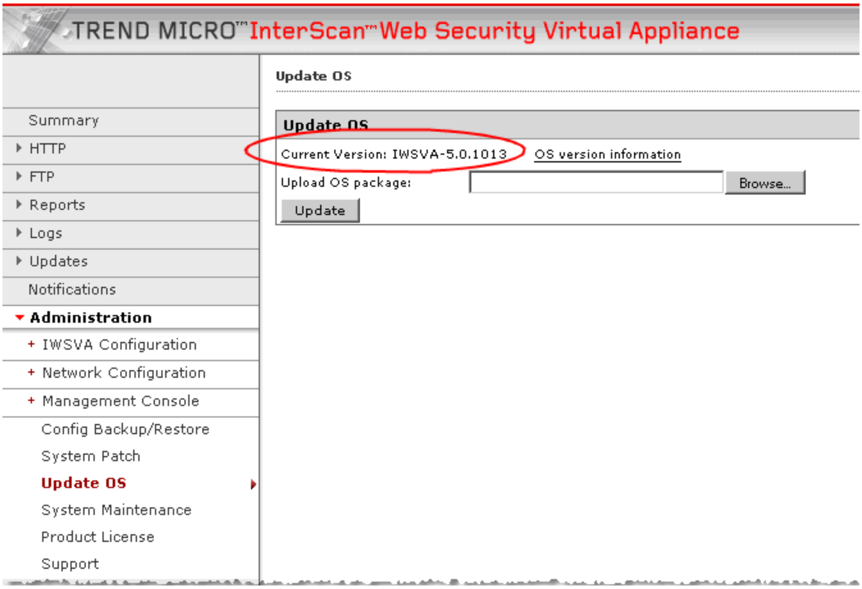
1. Log in as an administrator to the IWSVA 5.0 web console.
2. Verify that IWSVA is not registered to Trend Micro's Advanced Reporting and Management (ARM) product. IWSVA + ARM customers must unregister the IWSVA 5.0 appliances from the ARM web management console before proceeding.

   Note: If the IWSVA 5.0 appliance you are upgrading is registered to the ARM reporting module, you must unregister it from the ARM management interface before the upgrade and re-register it again after the upgrade.

3. Prepare to upload certificates after the upgrade completes.

   If you uploaded private or 3rd party certificates to IWSVA, make sure you have these ready after the upgrade. You will need to re-import them into the IWSVA 5.1 appliance. To review and backup your settings, follow the links below for each certificate type.

   - HTTPS decryption CA configured at **HTTP > HTTPS Decryption > Settings**
   - Applet re-signing certificate at **HTTP > Applets and ActiveX > Settings**
4. Go to **Administration > Update OS** in the IWSVA 5.0 web console.
5. Verify that you are running IWSVA 5.0.XXX. The version number is shown at the top of the Update OS page. (See *Figure 4-1*.)



Current Version: IWSVA-5.0.1013

FIGURE 4-1. Verify IWSVA 5.0.XXXX is the current version.

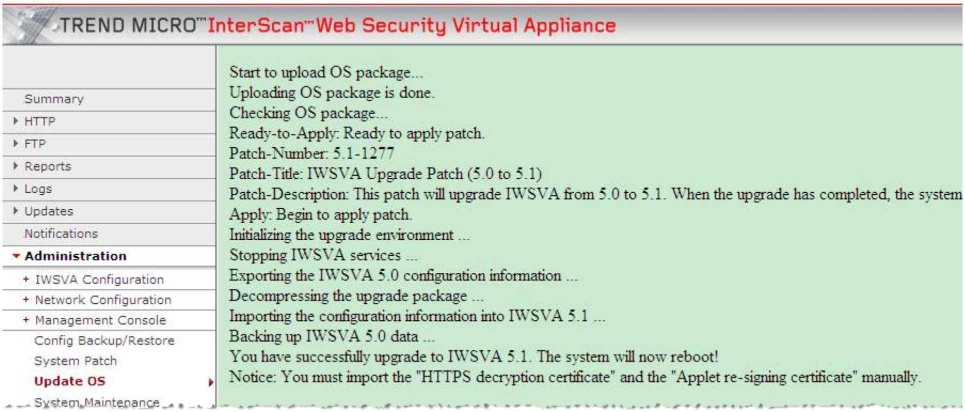
6. Download the IWSVA 5.1 upgrade package from the download page on the Trend Micro website to the host that will be performing the update.

   Download site:
   http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=result_page&clkval=drop_list&catid=4&prodid=86

Note: The OS patch mechanism checks the patch package and copies the upgrade/rollback scripts to /var/upgrade_tool.

7. Click **Browse...** to locate the upgrade package.
8. Click **Update** to transfer and install the IWSVA 5.1 upgrade package.

The upgrade process starts and the status of each upgrade process displays. See *Figure 4-2*.



```
Start to upload OS package...
Uploading OS package is done.
Checking OS package...
Ready-to-Apply: Ready to apply patch.
Patch-Number: 5.1-1277
Patch-Title: IWSVA Upgrade Patch (5.0 to 5.1)
Patch-Description: This patch will upgrade IWSVA from 5.0 to 5.1. When the upgrade has completed, the system
Apply: Begin to apply patch.
Initializing the upgrade environment ...
Stopping IWSVA services ...
Exporting the IWSVA 5.0 configuration information ...
Decompressing the upgrade package ...
Importing the configuration information into IWSVA 5.1 ...
Backing up IWSVA 5.0 data ...
You have successfully upgrade to IWSVA 5.1. The system will now reboot!
Notice: You must import the "HTTPS decryption certificate" and the "Applet re-signing certificate" manually.
```

FIGURE 4-2. Progress messages display during upgrade.

When the upgrade finishes, IWSVA automatically restarts to enable the new features. The reboot process takes several minutes to complete.

Note: - If for any reason the upgrade was unsuccessful and an error message displays, follow the procedure in the System Recovery for Power Failure during an Upgrade on page 4-10.
- If you see a message similar to "???.admin.update_os.upload_done???" displayed on the console, this is IWSVA's installer confirming the upgrade patch filename and is a normal part of the installation display.
- You may encounter the following error message: "There is not enough free disk space. The minimum requirement is 2Gb." If so, delete any TMP files or CDT files on IWSVA to make more space available.

9. After IWSVA restarts, refresh the web console to log on to IWSVA 5.1.

Note: For existing customers who upgrade from IWSVA 5.0 to 5.1, the administrator passwords are retained and the Deployment Wizard is not launched automatically to guide you through the configuration process. These steps occur only for new installations.

10. If needed, access the upgrade log information at: `/var/upgrade_tool/upgrade.log`

Post-upgrade Processes

After upgrading to IWSVA 5.1, some additional procedures may be required to restore certificate information and to re-register the IWSVA appliance to the ARM management server.

To restore certification and register to ARM:

1. Allow the reboot to complete from the upgrade procedure.
2. Manually restore the following configurations:

a. HTTPS decryption CA configured at **HTTP > HTTPS Decryption > Settings**. (See *Figure 4-3*.)

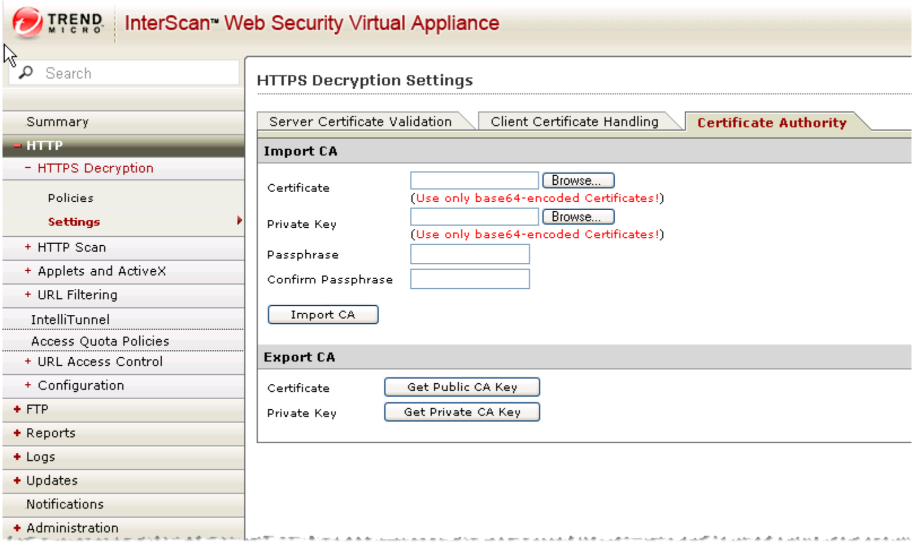
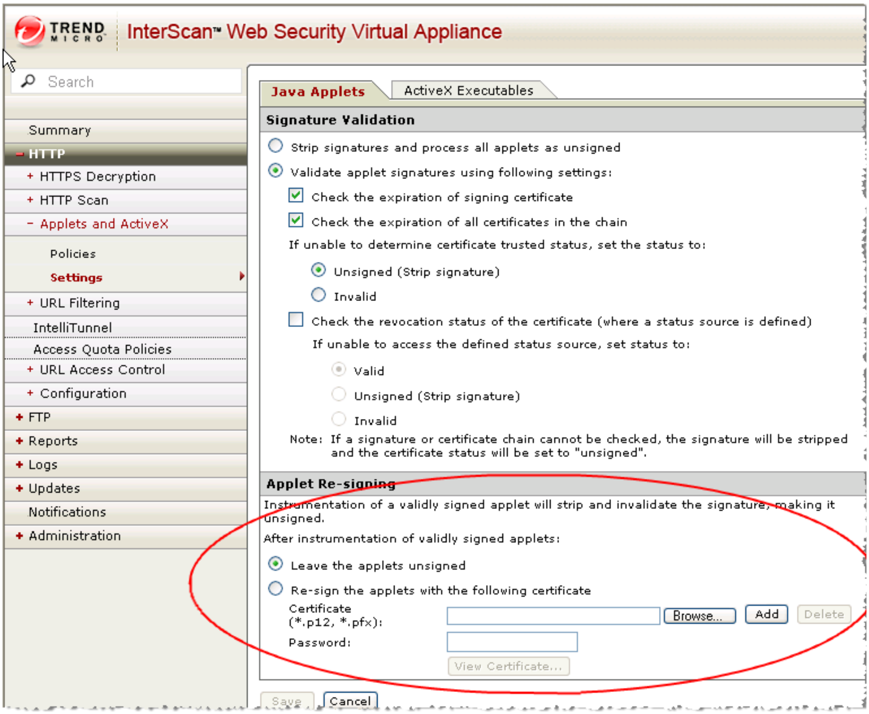


FIGURE 4-3. Re-import the HTTPS Decryption CA

b. Applet re-signing certificate at **HTTP > Applets and ActiveX > Settings**. (See *Figure 4-4*.)



Signature Validation

○ Strip signatures and process all applets as unsigned

● Validate applet signatures using following settings:

☑ Check the expiration of signing certificate

☑ Check the expiration of all certificates in the chain

If unable to determine certificate trusted status, set the status to:

● Unsigned (Strip signature)

○ Invalid

□ 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

○ Unsigned (Strip signature)

○ Invalid

Note: If a signature or certificate chain cannot be checked, the signature will be stripped and the certificate status will be set to "unsigned".

Applet Re-signing

Instrumentation of a validly signed applet will strip and invalidate the signature, making it unsigned.

After instrumentation of validly signed applets:

● Leave the applets unsigned

○ Re-sign the applets with the following certificate

Certificate (*.p12, *.pfx): [Browse...] [Add] [Delete]

Password:

[View Certificate...]

[Save] [Cancel]

FIGURE 4-4. Re-import the Applet Re-signing Certificate

3. (Optional) Register IWSVA 5.1 to ARM, if it was previously registered to IWSVA 5.0 and unregistered before upgrading.

   This is performed through the ARM management interface with the **Gateway Devices > Device Registration** option.

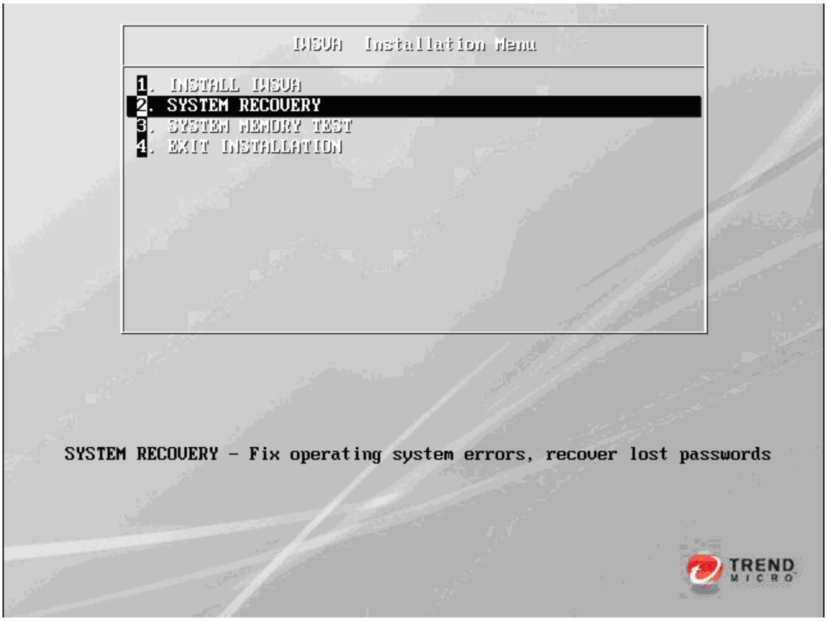
System Recovery for Power Failure during an Upgrade

If the upgrade fails because of a power failure, you can restore the IWSVA 5.0 system from the IWSVA console. All data and logs will be retained.

A failed upgrade process causes the IWSVA appliance to reboot.

To execute the recovery:

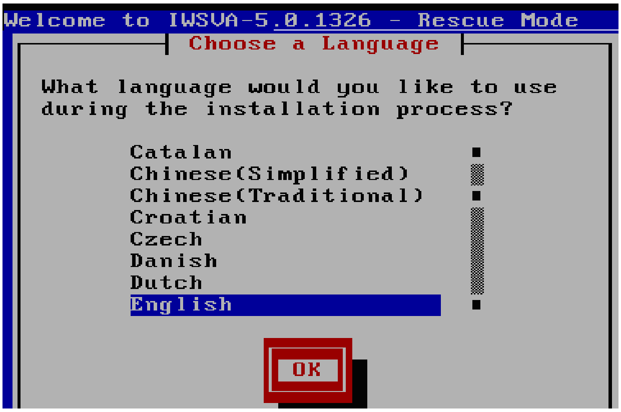
1. Select the System Recovery option from the IWSVA Installation Menu.



SYSTEM RECOVERY - Fix operating system errors, recover lost passwords

FIGURE 4-5. Enter the system recovery mode.

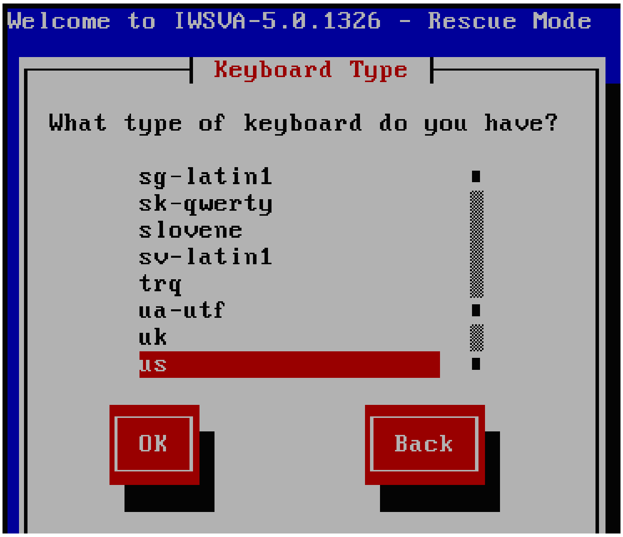
2. Select the appropriate **language** and press **Enter**.



```
Welcome to IWSVA-5.0.1326 - Rescue Mode

Choose a Language

What language would you like to use
during the installation process?

Catalan
Chinese(Simplified)
Chinese(Traditional)
Croatian
Czech
Danish
Dutch
English
```

FIGURE 4-6. Select a language for the installation process.

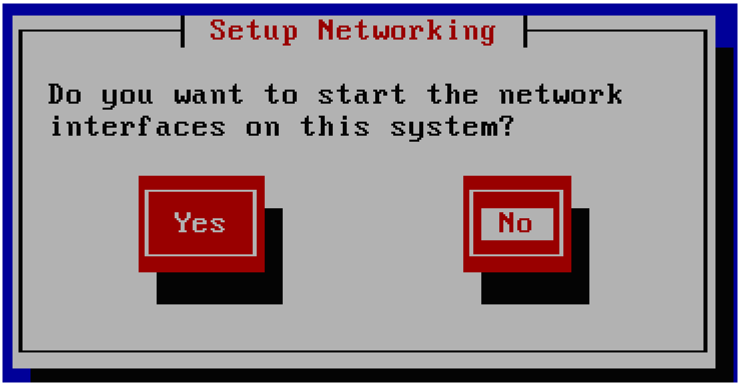
3. Select the appropriate **keyboard** type and press **Enter**.



```
Welcome to IWSVA-5.0.1326 - Rescue Mode

Keyboard Type

What type of keyboard do you have?

sg-latin1
sk-qwerty
slovene
sv-latin1
trq
ua-utf
uk
us
```

FIGURE 4-7. Select the appropriate keyboard type.

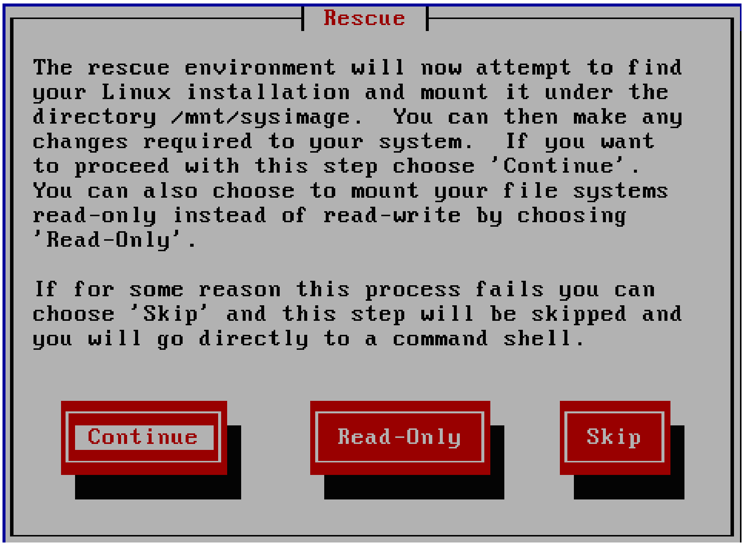
4. Select **No** in the Network Setup and press **Enter**.



Do you want to start the network interfaces on this system?

FIGURE 4-8. No network setup is needed.

5. Select **Continue** and press **Enter** to allow the system to locate your installation and mount it.



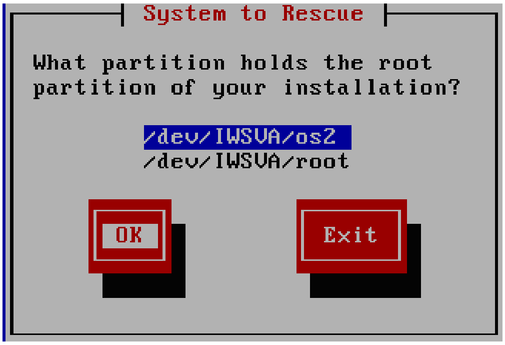
The rescue environment will now attempt to find your Linux installation and mount it under the directory /mnt/sysimage. You can then make any changes required to your system. If you want to proceed with this step choose 'Continue'. You can also choose to mount your file systems read-only instead of read-write by choosing 'Read-Only'.

If for some reason this process fails you can choose 'Skip' and this step will be skipped and you will go directly to a command shell.

FIGURE 4-9. Allow installation location and mount.

6. Select **OK** on the following System to Rescue page to continue.

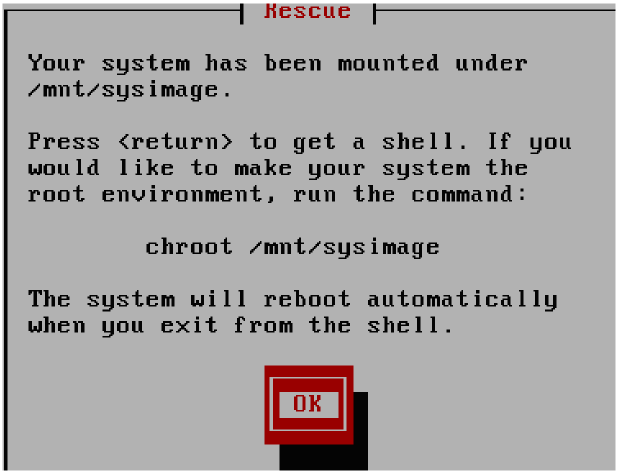
Note: Depending on your setup, this page may not appear.



```
System to Rescue

What partition holds the root
partition of your installation?

    /dev/IWSVA/os2
    /dev/IWSVA/root
```

FIGURE 4-10. System to rescue path displays

7. Press **Enter** to enter the OS shell.



```
Rescue

Your system has been mounted under
/mnt/sysimage.

Press <return> to get a shell. If you
would like to make your system the
root environment, run the command:

        chroot /mnt/sysimage

The system will reboot automatically
when you exit from the shell.
```

FIGURE 4-11. Acknowledge the mount and enter the shell.

8. Run the recovery tools located on the disk by executing the following commands:

   ```
   #chroot /mnt/sysimage
   #/var/upgrade_tool/rollback_tools.sh
   ```

9. Reboot the upgrade package by executing the following commands:

   ```
   #exit
   #exit
   ```

Chapter 5

Migrating to InterScan Web Security Virtual Appliance

This chapter describes the following:

About Migration

InterScan Web Security Virtual Appliance (IWSVA) 5.1 supports both full and partial migration. Use full migration to restore the 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.

WARNING! **IWSVA 5.1 does not support migration from another language version of IWSVA 5.1, IWSVA 5.0, IWSVA 3.1, or IWSS 3.1 Linux/Windows**

Before you perform a full migration, make sure the hardware configuration and deployment mode are the same on both the source and target IWSVA 5.1 machines.

Trend Micro recommends that you configure the target IWSVA 5.1 machine to use the same IP address as in the backup configuration file (exported from the source IWSVA 5.1 machine) to prevent unexpected behavior after a full migration.

Do NOT connect both IWSVA 5.1 machines to the network simultaneously. Only one IWSVA 5.1 machine should be connected at a time.

The configuration and policy information for the following IWSVA products can be migrated to IWSVA:

- IWSS 3.1 Linux
- IWSS 3.1 Windows
- IWSVA 3.1
- IWSVA 5.0
- IWSVA 5.1

If you are migrating from IWSVA 5.0, see Migrating to InterScan Web Security Virtual Appliance on page 5-1.

If you are migrating from a previous version other than IWSVA 5.0, you need to:

- **Step 1.** Back up your configuration file using the tool provided in the product's web console. In IWSVA 3.1 and above, the configuration backup function is located at **Administration > Config Backup/Restore**.

- **Step 2.** Do a fresh installation, as shown in Installing InterScan Web Security Virtual Appliance on page 3-1.
- **Step 3.** Reapply the configuration file you backed up in step one by restoring the configuration file to the IWSVA 5.1 server. Use **Administration > Backup/Restore**.

Important Notes

- You can export IWSVA configuration to a backup file. Export information includes both system level and application level configuration settings.
- Use the **Config Backup & Restore** page in the Web console to import the backup file containing the IWSVA 5.1 configuration. A screen displays to prompt you to select either full migration or partial migration.
- Password information in a configuration backup file will not be displayed in clear text.
- IWSVA records a configuration import or export action in the audit log.

Information Not Migrated

The following lists the items that are not migrated.

Full Migration

- Logs stored in databases, reports, messages, and quarantined files
- Pattern and engine files and related version information located in configuration files
- Database passwords
- Product activation code
- HTTPS and applet re-sign CA certificates
- OS and application patches

Partial Migration

- Logs stored in databases, reports, messages, and quarantined files
- Pattern and engine files and related version information located in configuration files

- Database passwords and configurations
- Product activation code
- HTTPS and applet re-sign CA certificates
- Deployment mode configurations
- All configuration settings under the Administration menu in the Web console
- The following settings from IWSS 3.1 Linux, IWSS 3.1 Windows, IWSVA 3.1 and IWSVA 5.0:
    - Schedule reports
    - Log and report paths
- (For partial IWSVA 5.1-to-IWSVA 5.1 migration) System level settings such as IP address, hostname, and so on
- OS and application patches

Overview of the Migration Process

This procedure lists the major steps for both full and partial migration.

Note: To migrate from IWSVA 5.0 to IWSVA 5.1, see On-box Upgrade from InterScan Web Security Virtual Appliance 5.0 to 5.1 on page 4-1.

Procedure:

1. Back up previous IWSx settings for configuration rollback in case the migration process is not successful.
2. Perform a fresh IWSVA 5.1 installation on a new machine.
3. Import the previously backed up configuration file to the new IWSVA machine. If you are migrating from a source IWSVA 5.1 to a target IWSVA 5.1 machine, you can choose to perform a full or partial migration.
4. You can access the Web console to configure new IWSVA 5.1 features that are not in IWSVA 3.1, IWSS 3.1 Linux/Windows, or IWSVA 5.0.

Note: After the migration process completes, the default settings apply for IWSVA 5.1 features that are not available in IWSVA 5.0, IWSVA 3.1, and IWSS 3.1 Linux/Windows.

For a list of settings that are not migrated, refer to *Information Not Migrated on page 5-3*.

Migrating from IWSS 3.1 Linux/Windows to IWSVA 5.1

Note: IWSVA 5.1 does not support migration from another language version of IWSS 3.1 Linux/Windows.

Procedure:

1. Open the Web console of the source machine; then, select **Administration > Support**; then, click **Generate System Information File**.
2. Click **Download to your computer** to save the file to a local drive on your computer.
3. Open the Web console of the target IWSVA 5.1 machine and then select **Administration > Configuration Backup/Restore** from the main menu.
4. Click **Browse** to select a backup file and then click **Import**.

Migrating from IWSVA 3.1 and IWSVA 5.0 to IWSVA 5.1

Note: IWSVA 5.1 only supports partial migration if you want to restore back to a previous backup IWSVA 3.1 or IWSVA 5.0 configuration.

IWSVA 5.1 does not support migration from another language version of IWSVA 3.1 or IWSVA 5.0.

Procedure:

1. Open the Web console of the source IWSVA 3.1 machine; then, select **Administration > Configuration Backup & Restore**, and then click **Export**.

   The screen displays a progress bar. When the export process is finished, a result page displays the status. If configuration export is successful, IWSVA opens a dialog box to prompt you to save the configuration file to a local disk. Save the file to a local drive on your computer.

2. Open the Web console of the target IWSVA 5.1 machine and then select **Administration > Configuration Backup & Restore** from the main menu.

3. Click **Browse** to select a backup file and then click **Import**.

Migrating from IWSVA 5.1 to Another IWSVA 5.1

Note: IWSVA 5.1 does not support migration from another language version of IWSVA 5.1.

To perform a full migration, make sure the hardware configuration and deployment mode are the same on both IWSVA machines. Trend Micro also recommends you configure both machines to use the same IP address to prevent unexpected behavior after a full migration.

If the IP address information in the backup file is different from the IP address of the IWSVA machine to which you want to import the file, the migration results screen will not display. In this case, you can view the migration results in the Audit Log screen.

After a full migration, if the separate management interface is enabled on the source IWSVA 5.1 machine, you must use the management IP address of the source IWSVA 5.1 machine to access the Web console on the target IWSVA 5.1 machine.

Procedure:

1. Open the Web console of the source IWSVA 5.1 machine and select **Administration > Configuration Backup& Restore**. Then, click **Export** to back up the configuration.

   The screen displays a progress bar. When the export process is finished, a result page displays the status. If the configuration export process is successful, IWSVA opens a dialog box to prompt you to save the configuration file to a local disk. Save the file to a local drive on your computer.

2. Open the Web console of the target IWSVA 5.1 machine and then click **Administration > Configuration Backup/Restore** from the main menu.
3. Click **Browse** to select a backup file and then click **Import**.

   A screen displays prompting you to select a full or partial migration.
4. Choose an option and click **OK** to continue.

After Migrating

Existing customers can check the "What's New" section in the first chapter of the *IWSVA Administrator's Guide* to see the new features are available in this release. New customers can see all of the other IWSVA features listed after the "What's New" section.

Appendix A

Deployment Integration

This appendix describes the following:

- *IWSVA in a Distributed Environment on page A-2*
- *Integration with LDAP on page A-4*
- *Damage Cleanup Services (DCS) Integration on page A-7*
- *Integration with a Cisco Router using WCCP on page A-10*
- *Configuring the Cisco Device and IWSVA for WCCP on page A-11*
- *Configuring IWSVA for a WCCP Service Group on page A-13*
- *Protecting an HTTP or FTP Server using Reverse Proxy on page A-18*
- *Integration with an ICAP Device on page A-19*

IWSVA in a Distributed Environment

InterScan Web Security Virtual Appliance (IWSVA) is designed to be part of a distributed system and can establish a number of network connections based on the configuration settings.

The administrator must ensure the following:

- None of the required channels are blocked
- All channels have enough throughput
- Servers use a supported version of the software
- Servers are able to handle heavy traffic load

Connection Requirements and Properties

Table A-1 provides the required connections and their properties.

TABLE A-1. Required Connections and Properties

CONNECTING COMPONENT	TRAFFIC: TYPE AND VOLUME	IF THE CONNECTION IS LOST
Clients	Should be measured on the real network.	No protection
Database server	**Type:** TCP **Volume:** • **Low**—if access logging is disabled. • **Medium**—if access logging is enabled.	Cached data is used for already started services. Services will not start.
LDAP server (if configured)	**Type:** LDAP **Volume:** Medium	Cached data is used for already started services. Services will not start.

TABLE A-1. Required Connections and Properties (Continued)

CONNECTING COMPONENT	TRAFFIC: TYPE AND VOLUME	IF THE CONNECTION IS LOST
Trend Micro Active Update Server	**Type:** HTTP and HTTPS **Volume:** 10-50 Mb/day	IWSVA components cannot be updated in time.
Web Reputation	**Type:** HTTP **Volume**: Depends on the specific access	Cached data is used for already started services. Service will not start and user is given access to requested URL.
Trend Micro DCS server (if configured)	**Type:** HTTP **Volume:** Depends on the number of infected machines	No cleaning is performed for infected machines.

Throughput and Availability Requirements

The administrator must determine the IWSVA availability requirements.

- Is IWSVA downtime acceptable?
- If so, what is the proper action (bypass or stop) to enforce when IWSVA is down?
- If a failover configuration with multiple IWSVA instances is used, do the LDAP and database servers have the same level of failover?

Integration with LDAP

Support Referral Chasing for Multiple LDAP Servers

IWSVA has an LDAP module that allows communication with multiple LDAP servers with the ability to establish multidomain trees- and forest-like environments.

If the configured main LDAP server from the IWSVA Web console **Administration > Network Configuration > Deployment Mode | User Identification** page cannot resolve client credentials, and the "referral chasing" is enabled (providing that the referral server(s) is configured), IWSVA attempts to query for the requested User/Group object with the configured Primary Referral Server. If the queried object is still not found, a configured Secondary Referral will be queried. In order to do that, it must keep the credentials of the administrative account for all LDAP servers in the `[LDAP-Setting]` section of the `intscan.ini` file.

The Windows Active Directory (AD) Global Catalog enables LDAP clients, such as IWSVA, to query objects native to the domain being queried, and those residing in remote domains, as long as the AD server being queried and the remote AD server has Global Catalog enabled. The Global Catalog server accepts the LDAP requests on port 3268 and allows querying the user credentials, full name and membership in the global and universal groups across all other domains in the forest. The use of the Global Catalog is handy when creating IWSVA LDAP policies for a parent group with user(s)/group(s) member(s) residing on remote domains that are part of many subdomain levels.

To use this feature, the IWSVA administrator should configure the main LDAP server that IWSVA uses from the Web console **Administration > Network Configuration > Deployment Mode | User Identification** page to communicate with a designated Global Catalog-enabled Active Directory server using port 3268, instead of using the default LDAP communication port 389.

Note: Global Catalog is only available in Microsoft Active Directory. The advantage of using the Global Catalog port includes better performance for LDAP object lookup, and allows object lookup that resides in many sublevels of the Active Directory tree (beyond three). However, in order for IWSVA to utilize the Global Catalog, the AD being requested for an object needs to have the Global Catalog enabled along with the AD where the queried user or group objects reside. IWSVA supports the use of the Global Catalog port only to be configured as the main LDAP server, and not part of the IWSVA referral chasing servers.

Tip: Trend Micro recommends allowing IWSVA to query the root Active Directory server with the Global Catalog enabled, and using Universal group types to do group nesting when applying policies. This can be seen by the Global Catalog and will be visible throughout the Active Directory. For more information, see Microsoft support (`http://support.microsoft.com/kb/231273`).

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.

- IWSVA must have a valid hostname assigned at **Administration > Deployment Wizard > Network Interface** page in the web console. Make sure the hostname is also entered in the corporate DNS server.
- Ensure that the user ID cache is enabled. By default, this is enabled. If it has been disabled for any reason, it must re-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 1.5 hours. If you need 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 nonbrowser applications trying to access the Internet. For example, the MSN application might try to access the Internet before the user has a chance to log in to 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. 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.

  b. Instruct users to open their Web browsers and get authenticated before starting up applications that need Internet access.

  c. Add the IP address of the client machine to “LDAP authentication White List.” IP address in this list will bypass LDAP authentication.

- When LDAP authentication is enabled and you have enabled the bridge mode on IWSVA and have selected **Enable transparence** on the Deployment Mode screen, a warning screen is displayed. This is because **Simple transparency** is selected by default and IWSVA does not support user or group name authentication in the simple transparency mode. In this case, click **OK** to close the warning screen and select WCCP to use LDAP authentication.

- When user or group authentication is enabled in either the forward proxy mode or the transparent mode with the 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 to the domain network can access the local intranet without having to enter the log on information (such as the username and password); that is, no password pop-up screen displays.

Note: You must configure your IE settings to enable automatic authentication on each client computer.

By default, automatic authentication is enabled in IE 7.0.

Refer to the Administrator's Guide for additional information.

Damage Cleanup Services (DCS) Integration

While IWSVA can detect and block worms and spyware at the HTTP and FTP gateway, it can also work in conjunction with Trend Micro Damage Cleanup Services to clean infected clients. Damage Cleanup Services is a comprehensive service that helps assess and clean system damage without installing software on client computers in a network. It performs the following activities:

- Removes registry entries created by worms and Trojans
- Removes memory resident worms, Trojans, and spyware/grayware
- Repairs system file configurations modified by malware

After IWSVA is registered with one or more DCS servers, IWSVA issues a cleanup request if it detects one of the following trigger conditions:

- Client PC attempts to access a URL classified as "Spyware," a "Disease Vector," or a "Virus Accomplice" by the Phish pattern file, or
- Client PC uploads a virus classified as a worm

Note: If malware attempts to contact a remote server using a protocol other than HTTP, IWSVA will not detect it, thus will not trigger a cleanup.

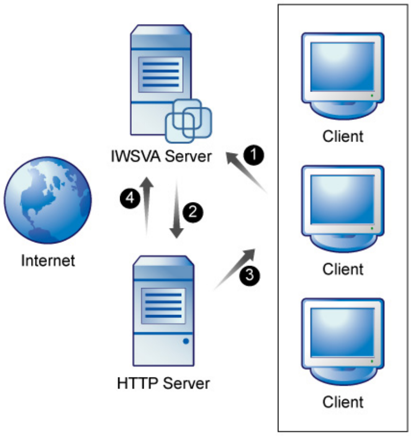


FIGURE A-1. How IWSVA requests DCS to perform a client cleanup

When IWSVA registers to a DCS server, infected client cleanups are handled in the following manner:

1. IWSVA detects the client attempting to access a URL listed in the PhishTrap pattern file or uploading a worm.
2. IWSVA requests the DCS server to clean up the infected client.
3. DCS attempts to connect to the infected client and clean it through remote procedures.
4. DCS reports the outcome of its cleaning attempt to IWSVA for logging.

When it receives a cleanup request from IWSVA, DCS attempts to connect to the infected client and repair the system damage. The outcome of the cleaning attempt, either successful or unsuccessful, is reported back to the IWSVA server for logging. If the cleanup attempt is not successful, then the client is redirected to a Web page hosted on the DCS server and an ActiveX control again attempts to clean the infected computer, with the permission of the computer’s user.

Note: If you are using DCS in conjunction with a HTTPS-enabled IWSVA Web management console, IWSVA must be configured to allow access to the secure port (typically 8443). If access to the secure port is blocked, IWSVA will be unable to redirect clients to DCS for clean-up requests.

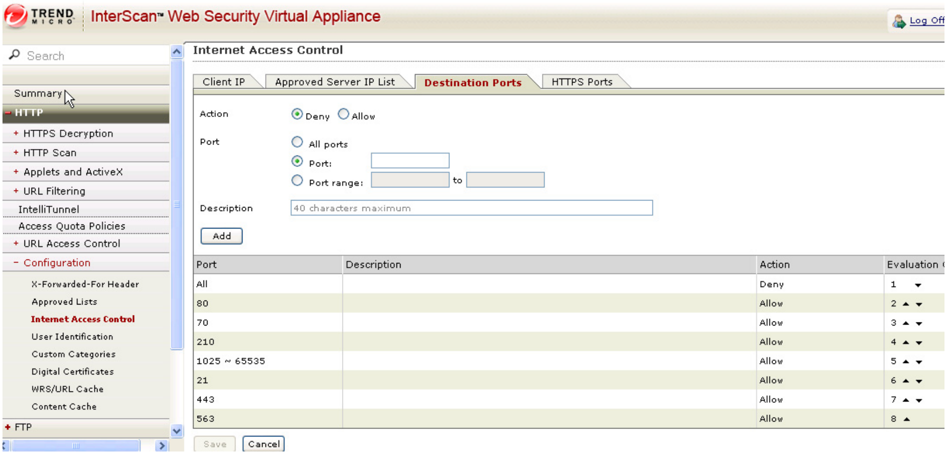
Using SSL with Damage Cleanup Services (DCS)

To redirect clients to DCS to clean up malicious code when you are using the HTTPS-enabled Web management console, access to the secure port that IWSVA uses (typically 8443) must be enabled. Otherwise, redirection to DCS will not be successful, because the redirection request will be blocked.

To allow access to secure port 8443:

1. Click **HTTP > Configuration > Internet Access Control**, and make the **Destination Ports** tab active.
2. Under the Action drop-down list, select **Allow.**
3. Select the **Port** radio button.
4. In the **Port** field, enter the port number used for HTTPS traffic (typically 8443).

5. Click **Add** and then **Save**.



Action ● Deny ○ Allow

Port ○ All ports
● Port:
○ Port range: to

Description 40 characters maximum

Port	Description	Action	Evaluation
All		Deny	1
80		Allow	2
70		Allow	3
210		Allow	4
1025 ~ 65535		Allow	5
21		Allow	6
443		Allow	7
563		Allow	8

FIGURE A-1 Allow access to the secure port (typically 8443) if using DCS and the HTTPS management console

Integration with a Cisco Router using WCCP

You can integrate IWSVA on a network that uses a Cisco router at the gateway without changing the browser settings of the client machines. This is achieved by utilizing Cisco's WCCP protocol.

Configuring the Cisco Device and IWSVA for WCCP

In order to prevent communication related issues, WCCP needs to be configured on the Cisco router or switch before being configured on IWSVA.

To configure a Cisco device and IWSVA for WCCP:

1. Configure WCCP on either the router or switch being used with IWSVA.

   Refer to your Cisco device manual for configuration details.
2. Log in to the IWSVA Web console.
3. Click **Administration > Deployment Wizard > Deployment Mode.**
4. Select **Web Cache Coordination Protocol (WCCP)** and click **Next**.
5. Enter the router IP address(es) on the Network Interface page.

   A maximum of eight routers can be entered. Enter only valid IP address(es).
6. Optionally, enter a password.

   If you specify no password for IWSVA, then you should specify no password for the router. If you specify a password for IWSVA, then ensure that the same password is also used for the Cisco device(s).

   While certain routers support Message-Digest algorithm 5 (MD5) encryption types 0-7, IWSVA only supports WCCP encryption types 0-6. Therefore, if you set the optional router password type for WCCP communication, choose a value from 0-6. Encryption type 7 is a Cisco proprietary type and is not supported.
7. Choose the WCCP forwarding method: GRE or Layer 2.

   Typically, Cisco routers only support GRE. Cisco switches only support the Layer 2 redirect assignment method. If in doubt, refer to the router or switch manual.
8. Select Assignment Method, Hash Tables or (default) Mask/value sets.
9. Click **Next** until you reach the Results page and receive a successful confirmation to save the WCCP settings.

After the WCCP configuration is saved, you can use the `show ip wccp 80 detail` command on the router or switch to verify that IWSVA has been added as one of the WCCP cache engines. If this addition is successful, various information displays, including the IWSVA IP address (Web Cache ID) and the state of the IWSVA unit, which will be usable. The following is a typical display indicating that IWSVA was added successfully:

```
Web Client ID:          10.204.170.97
Protocol Version:       2.0
State:                  Usable
Redirection:            L2
Packet Return:          GRE
Packet Redirection:     55
Connect Time:           00:09:08
Assignment:             MASK
```

If IWSVA was not added successfully as one of the WCCP cache engines, then no information will be displayed. In this case, you can use the `debug ip wccp packets` command to determine the problem.

For IWSVA, certain WCCP communication-related information is also available from the `http.log` file in the `/etc/iscan/log/` directory. To locate this information, search for log entries that begin with "WCCP."

Note: The CLI command, `show module log http,` can be used to search for log entries.

To view WCCP logs, turn on the log flag (`wccp_logging = 1`) within the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file.

Configuring WCCP Assignment Method

By default, the WCCP assignment method is set to mask. You can change this setting using the Deployment Wizard in the web console.

To configure WCCP assignment method:

1. Log into the web console and go to Administration > Deployment Wizard.
2. Select **Web Cache Coordination Protocol (WCCP)** and c lick **Next**.
3. Modify the value of WCCP Assignment Method by selecting one of the following options:

- Hash tables
- Mask/value sets (default)

4. Change other parameters, if necessary.
5. Click **Next** until you reach the Results page and receive a successful confirmation.

Configuring IWSVA for a WCCP Service Group

After installed, IWSVA uses service ID 80 (a WCCP component) to represent the WCCP service group. The associated router redirects HTTP/HTTPS and FTP traffic to this service group. In order to work with IWSVA, configure your routers using the same service ID. If a router does not have ID 80 available, then choose another service ID and then customize IWSVA as described in this section.

Load Balancing for WCCP Communication

Using the Well-Known Service Group for WCCP communication with more than one IWSVA device as part of the service group does not load balance as well as using the Dynamic Service Group (default service ID 80 for IWSVA). The load balancing offered by the Well-Known Service Group deviates more from the round robin concept than does the Dynamic Service Group. This might be because of the load balancing algorithm WCCP uses, and the way the WCCP router or firewall operates.

For best performance and resource usage distribution among IWSVA devices, Trend Micro recommends using the Dynamic Service Group (default service ID 80 for IWSVA) where applicable.

Note: In order to prevent communication related issues, WCCP needs to be configured on the Cisco router or switch before being configured on IWSVA (see Configuring the Cisco device and IWSVA for WCCP).

Configuring IWSVA to use the Dynamic Service Group

The WCCP's Dynamic Service ID is configurable by editing the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file.

You can modify the following default entries from 80 to the desired service ID.

```
wccp_service=dynamic 80 protocol=tcp

flags=src_ip_hash priority=120 ports=80,21,443
```

Note: The first and second lines of the previous code sample should be typed as a single line. Because of space limitations in this document, this code occupies two lines.

To configure the Dynamic Service ID:

1. Access IWSVA though SSH or direct console.
2. Log in as the root user.
3. From the shell, stop the WCCP daemon by issuing the following command:

   ```
   /usr/iwss/S99ISWCCPd stop
   ```

4. Modify the following parameters in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file by modifying the default service ID from 80 to the desired value.

   Example:

   ```
   wccp_service=dynamic 99 protocol=tcp

   flags=src_ip_hash priority=120 ports=80,21,443
   ```

5. Change the WCCP service ID on the WCCP-supported Cisco device to the configured service ID.

   In the previous example, the configured service ID is 99.

6. From the console manager, restart the WCCP daemon by issuing the following command:

   ```
   /usr/iwss/S99ISWCCPd restart
   ```

Note: In order to implement the new service ID on IWSVA, restart the `wccpd` daemon after the service ID is modified. This results in both IWSVA and the supported WCCP Cisco device being configured to use the same service ID that allows them to belong to the same service group. As members of the same service group, IWSVA and the WCCP Cisco device can communicate with each other.

The valid customizable WCCP Dynamic Service ID range is from 51-255, while 0-50 is reserved for Well-Known services. Certain WCCP routers only accept service ID range from 0-99.

Configuring IWSVA to use the Well-Know Service Group

For some older routers that do not support WCCP Dynamic Service group, IWSVA can be configured to use the Well-Known Service group.

Note: If IWSVA is configured to use the Well-Known Service ID to join a Well-Known Service group, then Trend Micro recommends configuring only one router on each IWSVA device.

To configure the Well-Known Service ID:

1. Access the IWSVA through an ssh or direct console.
2. Log in as the `root` user.
3. Modify the following parameters in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file by commenting out the first line and then by adding the second one below:

   ```
   # wccp_service=standard 0 protocol=tcp
   flags=src_ip_hash,dst_ip_hash,source_port_hash priority=120
   ports=80
   ```

   ```
   flags=src_ip_hash,dst_ip_hash,source_port_hash priority=120
   port=80
   ```

   ```
   wccp_std_service=standard 0
   ```
4. Change the WCCP service ID on the WCCP-supported Cisco device to the configured service ID.

In the previous step, the configured ID is 0. Typically, Cisco devices with WCCP support using the string, Web-cache, as part of the WCCP command for using service ID 0.

5. From the shell, restart the WCCP daemon by issuing the following command:

```
/usr/iwss/S99ISWCCPd restart
```

Note: Based on the WCCP specification, the Well-Known service group configuration does not support FTP traffic redirection to IWSVA for scanning. Configure the WCCP Cisco device to use the Well-Known service type prior to configuring IWSVA to avoid WCCP communication issues.

Configuration 1: Firewall only between WCCP Router and Internet

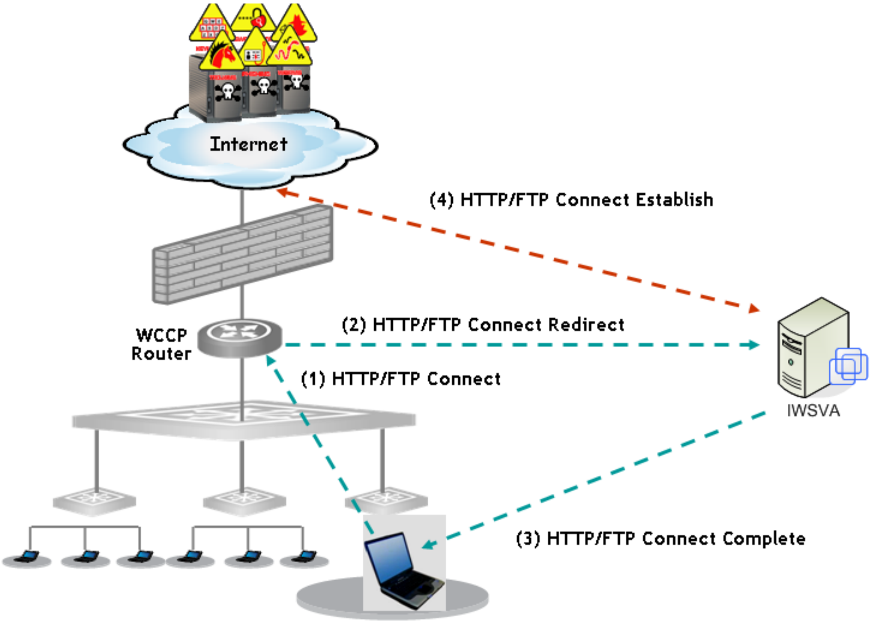

Internet
(4) HTTP/FTP Connect Establish
WCCP
Router
(2) HTTP/FTP Connect Redirect
(1) HTTP/FTP Connect
IWSVA
(3) HTTP/FTP Connect Complete

FIGURE A-2. WCCP and HTTP and FTP Traffic

Figure A-2 illustrates HTTP and FTP traffic.

Configuration 2: Firewall on Client Machine

If the client machine (laptop in the previous graphic) uses a personal firewall in addition to the firewall between the WCCP router and the Internet, then IWSVA cannot support FTP scanning.

Configuration 3: Stateful Firewall Between Client and IWSVA

If a stateful firewall exists between the client machine (laptop in the previous graphic) and IWSVA, then IWSVA cannot support FTP scanning.

Controlling WCCP Logging

HTTP and WCCP both write to the HTTP log. While HTTP uses the verbose attribute to enable or disable detailed logging, WCCP uses a different attribute to enable or disable logging.

By default, WCCP logging is enabled. You can disable WCCP logging by adding the line `wccp_logging=0` to the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file. Changing the line to `wccp_logging=1` turns WCCP logging back on again.

Configuration steps:

1. If the WCCP is already enabled, stop the WCCP daemon from the command line after accessing the IWSVA shell interface by `/usr/iwss/S99ISWCCPd stop`.
2. Add the line `wccp_logging=0 under the [http]` section in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file.
3. Start the WCCP daemon from command line `/usr/iwss/S99ISWCCPd` start.

Note: WCCP logging only records WCCP control messages and not user traffic activities. The WCCP daemon needs to be restarted to pick up the WCCP logging settings in the `IWSVAPIProtocolHttpProxy.pni` file.

Sample PIX Firewall Configuration

The following is an example of how WCCP could be configured on a PIX firewall using a Well-Known and Dynamic Service ID, along with an enabled password. The inside statement represents the name associated with an inside (most trusted) network interface on a PIX firewall.

The command lines containing Web-cache are used for a Well-Known Service ID. The command lines containing 80 are used for a Dynamic Service ID, with the default value for IWSVA specified. For more detailed PIX firewall configurations, refer to the relevant Cisco documentation.

```
wccp web-cache password <password>
wccp interface inside web-cache redirect in
wccp 80 password <password>
wccp interface inside 80 redirect in
```

The password is alphanumeric and can be up to eight characters in length. The password is MD5-based and the same password specified for the firewall must be specified for IWSVA.

Protecting an HTTP or FTP Server using Reverse Proxy

If you are protecting the HTTP server, install the HTTP scanning service in the HTTP proxy mode and use the reverse proxy configuration.

- Define the following configuration setting in the [http] section of the pni-file
  - `self_proxy=reverse`—specifies operation mode
  - `reverse_server`—specifies the IP address of the protected HTTP server
  - `reverse_server_port`—specifies the TCP port of the protected HTTP server

Note: To simplify the deployment of the reverse-proxy configuration in an HTTP/HTTPS environment, IWSVA can listen for the incoming (HTTPS) connection on a port specified by the `[main]/secondaryport` configuration parameter, and forward this traffic without scanning to port 443 of the protected server.

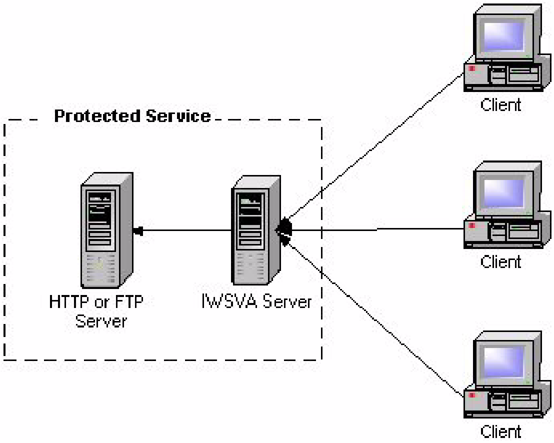


FIGURE A-3. Protecting a Dedicated Server

If you are protecting the FTP server, install the FTP scanning service and configure it to use an FTP proxy.

- Define the following configuration settings in the [ftp] section of the pni-file:

`proxy_mode=dedicated`	specifies operational mode
`ftp_server`	specifies the IP address of the protected FTP server
`ftp_server_port`	specifies the TCP port of the protected server

Integration with an ICAP Device

You can integrate IWSVA on a network that utilizes an ICAP 1.0 compliant cache server.

Setting up an ICAP 1.0-compliant Cache Server

Configure an ICAP client to communicate with the ICAP server.

- *To set up ICAP for NetCache Appliance: on page A-20*
- *To set up ICAP for the Blue Coat Port 80 Security Appliance: on page A-22*
- *To set up ICAP for Cisco CE ICAP servers: on page A-25*

Setting up ICAP for NetCache Appliances

To set up ICAP for NetCache Appliance:

1. Log on to the NetCache console by opening `http://{SERVER-IP}:3132` in a browser window.
2. Click **Setup**, and then click **ICAP** > **ICAP 1.0** in the left menu.
3. Click **General**, and then select **Enable ICAP Version 1.0**. Click **Commit Changes**.

> **Note:** An "`icap: This service is not licensed`" error message appears when you have not provided the required ICAP license key for NetCache.

4. Enter an ICAP license key:
   a. Click the **Setup** tab, and then click **System > Licenses** on the left menu. The **System Licenses** screen appears.
   b. Type **IWFLPWA** under the **ICAP license** section.
   c. Click **Commit Changes**.
5. Select the **Service Farms** tab on the **ICAP 1.0** screen, and then click **New Service Farm** to add ICAP servers. Then, assign the service farm name in the **Service Farm Name** field.
   - For response mode, select **RESPMOD_PRECACHE** in the **Vectoring Point** field
   - For request mode, select **REQMOD_PRECACHE** in the **Vectoring Point** field
6. Select **Service Farm Enable**.
7. In the **Load Balancing** field, choose the proper algorithm that you use for load balancing (if you have more than one ICAP server in the service farm). Clear **Bypass on Failure**.

Note: Disable **Bypass on Failure** if the priority is more on virus propagation within your network. Otherwise, enable **Bypass on Failure** to guarantee an unblocked connection to the Internet.

8. Under the **Consistency** field, choose **strong** from the drop-down menu and leave the **lbw Threshold** field empty.
9. Under the **Services** text box (for response mode), type:
`icap://{ICAP-SERVER-IP}:1344/resp on,`
where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP for response mode.

   Under the **Services** text box (for request mode), type
`icap://{ICAP-SERVER-IP}:1344/REQ-Service on,`
where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP for request mode.

   For multiple IWSVA ICAP server services, type the additional entries in step 9. For example:

   For response mode,

   - `icap://{ICAP-SERVER1-IP}:1344/resp on`
   - `icap://{ICAP-SERVER2-IP}:1344/resp on`

   Click **Commit Changes**.

   For request mode,

   - `icap://{ICAP-SERVER1-IP}:1344/REQ-Service on`
   - `icap://{ICAP-SERVER2-IP}:1344/REQ-Service on`

   Click **Commit Changes**.

Note: For multiple ICAP servers within a service farm with **strong** consistency selected, make sure that all ICAP servers have identical `intscan.ini` and other configuration files and the same virus pattern. The service farm will not work properly if the ICAP servers have different configurations.

10. Click the **Access Control Lists** tab, and then select **Enable Access Control Lists**.
11. Type `icap (Service Farm name of the ICAP Server) any` in the **HTTP ACL** field.
12. Click **Commit Changes**.

To configure scanning FTP over HTTP traffic, go to **FTP > Configuration > Access Control Lists**, and then add "`icap (service farm name)`" into the **FTP ACL** field.

Setting Up ICAP for the Blue Coat Port 80 Security Appliance

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

1. Log on to the management console by typing `http://{SERVER-IP}:8081` in the address bar of your Web browser (specifying port 8081 as the default management port).

   For example, if the IP address configured during the first-time installation is 123.123.123.12, enter the URL http://123.123.123.12:8081 in the Web browser.
2. Select **Management**. Type the log on username and password if prompted.
3. Click **ICAP** in the left menu, and then click **ICAP Services**.
4. Click **New**. The **Add ICAP Service** screen appears.
5. In the **ICAP service name** field, type an alphanumeric name and then click **OK**.
6. Highlight the new ICAP service name and click **Edit**.

   The **Edit ICAP Service name** screen appears.
7. Type or select the following information:

   a. 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 number. The default ICAP port number 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 timeout, 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 timeout 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** and then click **Apply**.

Note: You can edit the configured ICAP services. To edit a server configuration again, select the service and click **Edit**. The examples used for configuring ICAP for Blue Coat are based on version 2.1.07. The settings might vary depending on the version of Blue Coat used.

---

9. Add a 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 installed 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 have not installed JRE on your workstation, a security-warning window appears. Click **Yes** to continue. Follow the instructions to install the JRE.

To add the response mode policy:

a. Select **Management**. Type the log on username and password if prompted.

b. Click **Policy** in the left menu, and then click **Visual Policy Manager**.

c. Click **Start**.

If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.

d. On the menu bar, click **Edit > Add Web Content Policy**.

The **Add New Policy Table** screen appears.

e. Type the policy name under the **Select policy table name** field. Click **OK**.

f. Under the **Action** column, right-click **Bypass ICAP Response Service** and click **Set**.

The **Add Object** screen appears.

g. Click **New** and select **Use ICAP Response Service**.

The **Add ICAP Service Action** screen appears.

h. 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**, and then click **OK** again.

i. Click **Install Policies**.

To add the request mode policy:

a. Select **Management**. Type the log on username and password if prompted.

b. Select **Policy** in the left menu, and then click the **Visual Policy Manager** tab.

c. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.

d. On the menu bar, click **Edit > Add Web Access Policy**.

The **Add New Policy Table** screen appears.

e. Type the policy name under the **Select policy table name** field. Click **OK**.

f. Under the **Action** column, right-click **Deny** and click **Set**.

The **Add Object** screen appears.

g. Click **New** and select **Use ICAP Request Service**. The **Add ICAP Service Action** screen appears.

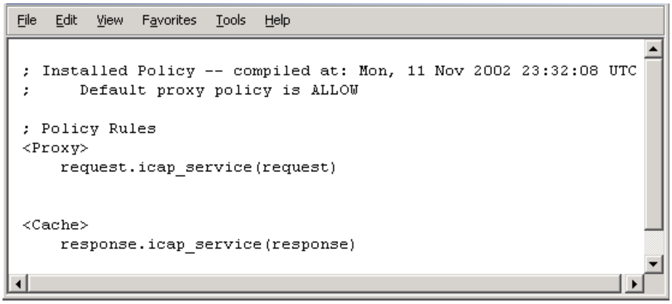
h. Choose the ICAP service name under the **ICAP Service/Cluster Names** field.

i. Enable **Deny the request** under the **On communication error with ICAP service** section.

j. Click **OK**, and then click **OK** again.

k. Click **Install Policies**.

10. 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 A-1 Current configured policy

Setting up ICAP for 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.

To set up ICAP for Cisco CE ICAP servers:

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 the following:

   ```
   icap service RESPMOD SERVICE NAME
   ```

   The ICAP service configuration menu opens. 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. 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, you must 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 management console:

1. Select **Management**.

   Type the log on username and password if prompted.

2. Click **ICAP** in the left menu, and then click the **ICAP Clusters** tab.

3. Click **New**.

   The **Add ICAP Cluster** screen appears.

4. In the **ICAP cluster name** field, type an alphanumeric name and then click **OK**.

5. Highlight the new ICAP cluster name and click **Edit**.

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

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

   The **Edit ICAP Cluster Entry name** screen appears.
9. In the **ICAP cluster entry weight** field, assign a weight from 0-255.
10. Click **OK** and then **OK** again, and finally **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 management console:

1. Select **Management**. Type the log on username and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Clusters** tab.
3. Click the cluster you want to delete.
4. Click **Delete**, and then click **OK** to confirm.

Enabling “X-Virus-ID” and “X-Infection-Found” Headers

IWSVA can return two optional headers from the ICAP server whenever a virus is found: the “X-Virus-ID” and the “X-Infection-Found” headers. Neither of these headers are returned by default for performance reasons, because many ICAP clients do not use these headers. They must be enabled in the IWSVA management 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/documents/specification/draft-stecher-icap-subid-00.txt`

To enable the X-Virus-ID header:

1. From the main menu, click **Administration > Network Configuration > Deployment Mode**.
2. On the **Deployment Mode** page, select **Enable 'X-Virus-ID' ICAP header** and/or **Enable 'X-Infection-Found' ICAP header**.

Appendix B

Tuning and Troubleshooting

This appendix explains the following:

- *IWSVA Performance Tuning on page B-2*
- *Troubleshooting on page B-6*

IWSVA Performance Tuning

If you are experiencing issues with slow browsing performance, consider the following modifications and the InterScan Web Security Virtual Appliance (IWSVA) remote rating service.

URL Filtering

IWSVA utilizes the Trend Micro URL Filtering Engine to perform URL categorization and reputation rating based on the data supplied by the Trend Micro Web Reputation feature. Trend Micro recommends using the default setting of a weekly update check to ensure that your installation has the most current URL Filtering Engine.

IWSVA can control URL 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, has hacking potential, or has a reputation score that deems it untrustworthy. Both the optional URL Filtering module and Web Reputation are controlled by the specifications you make in policies.

For additional details, see Chapter 8 in the Administrator's Guide.

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 and 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 group membership information. By default, entries in this cache will be valid for 48 hours, or until the cache fills (at which point the entries are replaced, starting with the oldest).

  The time to live (TTL) for entries in this cache can be configured through the setting `user_groups_central_cache_interval` in the [user-identification] section of `intscan.ini` configuration file.
- 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 will be attributed to that user, provided the new request is issued within a configurable window of time (15 minutes by default for HTTP, 90 minutes for ICAP) 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.

  To enable or disable this cache, change the `enable_ip_user_cache` setting in the [user-identification] section of the `intscan.ini` file. To change the TTL of this cache, change the `ip_user_central_cache_interval` (unit is hours). For example, to create a TTL of 30 minutes, enter `0.5`.
- 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 username) in the user authentication cache so the subsequent requests over a keep-alive connection will not authenticate again. The client IP address and client's username serve as two forward references, or links, to the "client IP to user ID cache" and "user group membership cache," respectively. IWSVA will thus still be able to retrieve the user's connection information from both the IP-user and user-group caches.

When deploying IWSVA with LDAP integration, it is important to consider the additional load that authenticating HTTP requests will place on the LDAP directory server. In an environment that cannot effectively use the client IP to user ID cache, the directory server will need to be able to handle queries at the same rate as IWSVA receives HTTP requests.

Disable Verbose Logging When LDAP is Enabled

Trend Micro recommends turning off verbose logging in the `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 will log 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 with 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.

LDAP Authentication in Transparent Mode

Before configuring LDAP authentication on IWSVA deployed in transparent mode, review the following criteria to ensure each item is fully met.

- IWSVA must have a valid hostname assigned (click **Administration > Deployment Wizard**, then update host name on Network Interface page). Make sure the hostname is also entered in the corporate DNS server.
- Ensure that the user ID cache is enabled. By default, this is enabled. If it has been disabled for any reason, it must re-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 1.5 hours. If you need to lower the cache time-out 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 nonbrowser applications trying to access the Internet. For example, the MSN application might try to access the Internet before the user has had 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. 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.

b. Instruct users to open their Web browsers and get authenticated before starting up applications that need Internet access.

c. Add the IP address of the client machine to “LDAP authentication White List.” IP address in this list will bypass LDAP authentication.

Note: When User/group authentication is enabled in either forward proxy mode or transparent mode with an 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 to the domain network can access the local intranet without having to enter the log on information (such as the username and password); that is, no password pop-up screen displays.

Refer to the IWSVA Administrator’s Guide for detailed configuration steps.

Troubleshooting

Troubleshooting Tips

- **Issue:** IWSVA could not connect to the database specified in the Database Connection Settings page. The IWSVA management console displays the following error message:

  ```
  JDBC-ODBC BRIDGE: [UNIXODBC] Could not connect to the
  server; Could not connect to remote socket.
  ```

  Solution:

  - Check the ODBC connection or the database server and try again.

- **Issue:** The IWSVA management console displays an authentication error message.

  ```
  JDBC-ODBC BRIDGE: [UNIXODBC]FATAL: Password authentication
  failed for user.
  ```

  Solution:

  - Verify the user credential for the PostgreSQL Server and also ensure that the database settings are correct (**Administration > IWSVA Configuration > Database Connections**). If the problem persists, ensure that the permissions in the `etc/iscan/odbc.ini` file are correct.

Before Contacting Technical Support

When contacting Technical Support with your issues, having specific information can streamline the process:

Installation Problems

Collect the following information about your installation problem before contacting Trend Micro technical support to expedite the process.

1. IWSVA version and build number
2. Screenshot of the exact error that appears during installation
3. The stage of the installation

General Feature Problems

If you have problems with IWSVA, collect the following information to provide to Trend Micro support:

- The system file(s) that describes the current state of IWSVA.

  To compile these files, access the Web console and choose **Administration > Support** and then click **Generate System Information File**. This button is an extension of the Case Diagnostic Tool (CDT), allowing you to package the current machine “state” at a click of a button.

  The system file(s) that IWSVA generates from clicking the **Generate System Information File** button are packaged into a single file with the following format: `info_YYYYMMDD_999999.tar.tz`

  Where `YYYY` is the current year, `MM` is the current month, and `DD` is the current day that the package file was generated. `999999` is the UNIX time code.

  The system file(s) contains the following information:

  - **IWSVA information**—Includes IWSVA product version, engine version and build number, current pattern file (if available), and IWSVA hot fixes and service pack information. Product and integration settings are also part of this information
  - **IWSVA system logs**—Includes IWSVA logs and debug logs, logs generated by the syslogd daemon (if system logs are enabled), and the core dump file
  - **System/network information**—Includes the hardware configuration, operating system, build, system resource status, other application installed, and network information
  - **CDT-compliant configuration/plug-ins information**—Includes information about changes made to CDT as a result of IWSVA adding a new component, such as a TMCM or MCP agent.
- Core files are first created in the first directory listed below, and then moved to the second directory listed:
  - `/etc/iscan/CoreDump`
  - `/etc/iscan/UserDumps`

Use these files when working with Trend Micro technical support to help diagnose the cause of your problem. To view the files yourself, use a program like GDB, the GNU Project debugger.

- Log file for the day the issue occurred
  - All log files the day the issue occurred (logs are stored in `/etc/iscan/log` by default)
  - Make sure `verbose=1` is set in the [ftp], [http], and [notification] sections of the `intscan.ini` file
  - Make sure `log_trans=yes` is set under the [ftp] and [http] sections of the `intscan.ini` file
- From the Web console, take a screen shot of the **Summary > Scanning** tab page.
- Record the IWSVA version number
- URL samples (if applicable)
- Get a packet capture of the failing transaction by using the CLI capture command (for example, enter `start task capture interface eth0` in enable mode).

Appendix C

Best Practices for IWSVA Installation and Deployment

This appendix describes the following:

- *IWSVA Installation Overview on page C-2*
- *Properly Sizing Your Environment on page C-4*
- *Selecting Deployment Method and Redundancy on page C-5*

IWSVA Installation Overview

This installation overview provides a quick reference on the order and key steps to install and configure InterScan Web Security Virtual Appliance (IWSVA) to function with the core scanning, logging, and reporting features. The detailed sections in the Best Practices appendix of the *IWSVA Administrator's Guide* will provide the URLs for downloading the necessary material. For complete instructions on installing IWSVA, please refer to the following chapters:

- *Installing InterScan Web Security Virtual Appliance on page 3-1*
- *On-box Upgrade from InterScan Web Security Virtual Appliance 5.0 to 5.1 on page 4-1*
- *Migrating to InterScan Web Security Virtual Appliance on page 5-1*

For complete feature and command instructions, refer to the *IWSVA Administrator Guide*.

To install and configure IWSVA:

1. Obtain the latest IWSVA software and documentation set from the Trend Micro Update Center or by purchasing the IWSVA installation disks. You can download IWSVA products and updates from: http://www.trendmicro.com/download/product.asp?productid=86
2. Register the product to obtain the Activation Codes. These will be required to activate IWSVA and its core modules. Products can be registered at: https://olr.trendmicro.com/registration/us/en-us/product_login.aspx
3. Review the *IWSVA Customer Sizing Guide* and *IWSVA Installation Guide* to determine the deployment topology and the number of IWSVA units required to support your environment.
4. Install the IWSVA application and license the components with the Activation Keys obtained from Step 2. Use the **Administration > Product License** function to perform this task.
5. Download any service packs and critical patches that are applicable to the IWSVA product you installed. Service packs and critical patches are version specific and are cumulative with the latest service pack containing the previous hot fixes and critical patches from the previous service packs. Best practice is to download and install the latest service pack for your IWSVA version and any newer critical patches to bring the IWSVA unit up to date.

IWSVA provides operating system updates separately from application service packs. Make sure the latest operating system patch is also downloaded and applied along with the application service pack. Always read the patch's ReadMe file to familiarize yourself with the installation procedure before upgrading your system.

Use the **Administration > System Patch** and **Administration > Update OS** functions to perform these tasks.

6. Configure the system settings. This includes setting the system date and time, configuring optional network configurations (such as enabling SSH for remote access, PING, optional static routes, etc), defining optional upstream proxy servers, enabling SNMP, and so forth. Use the Administration function to perform these tasks.
7. Configure IWSVA to a corporate LDAP server if you need to enforce policies, log events, and report Internet activity based on LDAP users and/or groups. Use the **HTTP > Configuration > User identification > User Identification tab t**o perform this function.
8. Review the default settings for the automatic pattern file and scan engine update intervals. Change to meet your needs if necessary. You can also perform a manual update for a newly installed IWSVA system to update the signature files and scan engines. Use the Updates function to perform these tasks.
9. Configure log settings and external syslog servers to set the logging granularity and setup any 3rd party logging support. Review the default system log retention option and change to meet your needs if necessary. Use the Logs function to perform these tasks.
10. Create policies to monitor and govern Internet traffic. Policies can be defined for the following protocols and traffic types: HTTPS, HTTP, Applet & ActiveX, URL Filtering, IntelliTunnel, Access Quota, and FTP. Use the HTTP and FTP functions to perform these tasks.
11. Define report templates and scheduled reports. Review the default number of scheduled reports to save for your daily, weekly, and monthly reports. If necessary, change to meet your needs. Use the Reports function to complete these tasks.
12. Create additional administrator, auditor, or reporter accounts to backup your administrator account and to grant other users access to administrative and reporting functions. Use the **Administration > Management Console > Account Administration** function to complete this task.

13. Backup the IWSVA configuration to keep a copy of the newly created configuration. Use the **Administration > Config Backup/Restore** function to complete this task.
14. Optional installation steps may include the following:
    - Customizing the notification messages
    - Setting up server farms
    - Registering IWSVA to the Advanced Reporting & Management (ARM) module
    - Registering IWSVA to Trend Micro's Control Manager (TMCM) central management system
    - Registering IWSVA to Damage Cleanup Services (DCS) server

Properly Sizing Your Environment

Before installing IWSVA into your network, you must first determine how many IWSVA servers are required to support your company's user population and Internet activity. Please refer to the *IWSVA Customer Sizing Guide* for detailed information on how to calculate the number of IWSVA units needed for your environment.

Things to consider for properly sizing your environment include:

- Number of total users in your company that will access the Internet
- Number of users accessing the Internet simultaneously
- Average number of concurrent sessions used by each active user
- Growth in user population and Internet use
- The type of server hardware being used
- The amount of bandwidth IWSVA needs to scan
- Redundancy and failover

Best Practice Suggestions

- Always size your environment for growth. Trend Micro doesn't recommend sizing your deployment based on current maximum peak loads as internet usage will always grow.
- Architect redundancy into the IWSVA architecture to prevent against single points of failure and to provide roll over during a device failure.

- Redundant architectures must be designed to support your maximum number of users when it fails over to the backup unit or secondary. Otherwise, performance and response time expectations will drop when a unit fails.

Selecting Deployment Method and Redundancy

IWSVA is one of the most flexible Web gateway security products for deployment options. IWSVA can be deployed in the following topologies:

- Forward Proxy
- Transparent Bridge
- WCCP
- ICAP
- Reverse Proxy
- Simple Transparency

Each deployment mode has its benefits and services a specific need. You should be aware of the advantages and disadvantages of each deployment mode before deciding on how to install the IWSVA product into your network. Please see *Deployment Primer on page 2-1* for detailed information on each deployment method and what key benefits are offered by each one.

If you are considering redundant architectures, you must review and consider the following points:

WCCP - IWSVA supports the Cisco WCCP protocol to allow you to build load sharing, redundancy, and scalability into your IWSVA architecture. If your routers and/or switches support Cisco WCCP, this is one of the most economical ways to add high availability features. One drawback of WCCP is that it can only redirect popular Internet protocols to the scanning devices efficiently. See the IWSVA ReadMe document for the WCCP versions supported.

ICAP - IWSVA supports ICAP v1.0 devices to allow you to scan content from popular caching servers. ICAP can also be used to create a scalable architecture through a one-to-many configuration with several IWSVA servers connected to a single cache server. This is a popular option for customers who need to cache web content to reduce bandwidth consumption and to lower Internet latency.

SQUID - IWSVA bundles the popular open source caching program, called Squid, to offer customers an economical way to cache web content without paying additional licensing fees. With IWSVA 3.1 and 5.0, Squid can be enabled through IWSVA's CLI interface and is deployable as a downstream proxy or an upstream proxy in relation to IWSVA. Starting with IWSVA 5.1, basic Squid configuration, reporting and enablement is integrated with the IWSVA 5.1 Web console. Squid is supported in upstream proxy mode with IWSVA 5.1. Squid support is offered through the open source community and is provided by Trend Micro on its Web Gateway products for convenience.

Proxy Pac File - Simple load sharing can be created through a proxy pac file if you are deploying in Forward Proxy mode. Many customers have experienced good results by creating a proxy pac file that routes traffic to a specific IWSVA device based on source IP address or source network. This allows you to manually scale your network and to load share users across many IWSVA servers without any added costs or network complexity.

You can also configure the proxy pac file to return multiple proxy servers to build a simple redundancy solution. Be aware that not all browsers may be able to interpret the multiple proxy server response. If they can't interpret the multiple proxy servers, redundancy will not be possible.

Layer 4 Load Balancing Switches - IWSVA can support external load balancing switches in Forward Proxy Mode using the “simple transparency” feature. Having an external load balancing switch adds additional cost and configuration complexity, but delivers the highest performance and flexibility in terms of redundancy and load sharing. Commercial load balancers that Trend Micro customers have used successfully include Foundry Networks/Brocade, F5, and Citrix NetScaler. If cost is a consideration, alternative open source software-based load balancers such as Red Hat Enterprise can also provide good scalability and redundancy options.

- If installing under VMware, consider using VMware's redundancy and fault tolerant functions to create a robust and scalable solution. These include:
  - VMotion
  - vSphere Fault Tolerance Services

Be aware that at the time of this writing, vSphere's Fault Tolerance service only permits one virtual CPU. This allows a full redundant solution to be developed, but offers less performance due to the single CPU limitation. For more information on setting up a vSphere FT configuration, refer to the *Best Practices Guide for Utilizing VMware Fault Tolerance for High Availability* document on the VMware web site.

Best Practice Suggestions

- IWSVA uses a hybrid malware scanning architecture that is comprised of cloud-based scanning and on-box scan engines. This solution provides one of the industry's highest detection and prevention rates. Cloud-based scan engines provide proactive detection and blocking services based on reputation services. To ensure fast performance with low latency, you need to provide IWSVA access to a fast and robust DNS architecture. ISP provided DNS servers should not be used as frequent DNS requests made by the IWSVA device may not be adequately supported and may possibly overwhelm the ISP's DNS server.
- IWSVA's internal clock settings should be synchronized with other servers and devices in your security architecture. These include LDAP servers, syslog servers, upstream SIEM devices, and Trend Micro's Advanced Reporting and Management server. If the date and time are mismatched, you may experience improper logging and reporting of critical events. For best results, use the same set of NTP servers to sync the date and time on all devices.
- For high volume installations of more than 3000 users, you should consider dedicating a server to house the Squid caching function (if enabled). During high workloads, IWSVA and Squid will contend for the same disk services. This will affect the cache hit performance as well as IWSVA's reporting performance. One alternative is to use two physical hard disk adapter cards in the same server with two separate disk volumes - one for IWSVA and one for Squid.
- For redundancy and scalability, consider installing more than one instance of IWSVA and using one of the scaling options mentioned in this section to eliminate single points of failure and improve system up time.
- For installations with an upstream proxy, you must properly configure IWSVA’s upstream proxy settings in the Forward Proxy settings and the Update Connection Settings to ensure proper Internet access.
- If you are planning to use IWSVA to protect external facing web servers that customers can access, consider installing a separate instance of IWSVA in reverse proxy mode to protect these web servers. Do not place the external facing web servers behind your corporate IWSVA server that your normal users would go through as this may affect your ability to enforce both customer facing policies and your normal corporate user policies.

- After installing IWSVA, always check the Trend Micro download site for additional critical patches and/or service packs to ensure that the latest patches are installed. Patches listed on the IWSVA Download site are listed in chronological order. Always apply the latest application and OS patches to your specific version. IWSVA service packs are backwardly compatible. That is, the latest service pack will always contain any hot fixes and patches issued prior to the service pack's release date. You do not need to install previous patches before the latest applicable service pack for your product. IWSVA may have the following patch types:
    - **Application Service Pack** - a service pack or patch that is used to update the IWSVA application. The latest service pack will contain all previously released patches.
    - **OS Service Pack** - a service pack or patch that is used to update the operating system and driver files. The latest service pack will contain all previously released patches.
    - **Critical Patch** - a patch that is used to fix an urgent application or OS problem and will not contain previous patches. It is only issued to fix a specific problem.

Appendix D

Maintenance and Technical Support

This appendix describes 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 for InterScan Web Security Virtual Appliance (IWSVA), visit the following URL:

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

The Update Center screen displays. Select your product from the links on this screen:

Clicking the link for Trend Micro™ InterScan™ Web Security Virtual Appliance (IWSVA) takes you to the Update Center page for IWSVA. Scroll down to review the patches that are available.

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 installation instructions in the readme.

Maintenance Agreement

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 for that 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. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Note: If the Maintenance Agreement expires, your License Agreement will not.

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will be alerted of the pending discontinuance. 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/
```

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 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 on to the account at the Trend Micro online registration Web site:

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

You are prompted to enter a log on ID and password.

To view your Registration Profile, type the log on ID and password created when you first registered your product with Trend Micro (as a new customer), and then click **Log on**.

Contacting Technical Support

To contact Trend Micro Technical Support, visit the following URL:

`http://kb.trendmicro.com`

Then, click the link for one of the following regions:

- Asia/Pacific
- Australia and New Zealand
- Europe
- Latin America
- United States and Canada

Follow the instructions for contacting support in your region.

In the United States, Trend Micro representatives can be reached through phone, fax, or email. Our Web site and email addresses follow:

`http://www.trendmicro.com`

`support@trendmicro.com`

For regional contact information and the specific technical support numbers for all the regional and worldwide offices, open the IWSVA management console and choosing **Support** from the menu in the management console's banner.

General US phone and fax numbers follow:

`Voice: +1 (408) 257-1500 (main)`

`Fax: +1 (408) 257-2003`

Our US headquarters is located in the heart of Silicon Valley:

```
Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
```

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The “virus doctors” at TrendLabs monitors 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, to mitigate virus outbreaks and provide urgent support.

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.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

`http://kb.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.

Known Issues

Known issues are features in your IWSVA software that might temporarily require a workaround. Known issues are typically documented in section 7 of the Readme document you received with your product. Readme files for Trend Micro products, along with the latest copies of the product manuals, can also be found in the Trend Micro Update Center:

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

Known issues can be found in the technical support Knowledge Base:

`http://kb.trendmicro.com`

Trend Micro recommends that you always check the Readme file for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

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://subwiz.trendmicro.com/SubWiz`

Click the "Submit a suspicious file/undetected virus" link. The following screen displays.

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**: Include a brief description of the symptoms you are experiencing. Our team of virus engineers will "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 or 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 displays. This screen also displays a case number for the problem you submitted. Make note of the case number for tracking purposes.

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`

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 Virus Map of the top 10 risks around the globe
- Consult the Virus 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 papers

- 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
- Read about TrendLabs, Trend Micro's global antivirus research and support center

To open Security Information:

1. Open the IWSVA management console.
2. Click **Security Info** from the drop-down menu at the top-right panel of the screen.

   The **Security Information** screen displays.

Appendix E

Creating a New Virtual Machine Under VMware ESX for IWSVA

This appendix describes how to create a new virtual machine for InterScan Web Security Virtual Appliance (IWSVA).

- *Introduction on page E-2*
- *Creating a New Virtual Machine on page E-2*

Introduction

The actual installation of ESX is not covered in this document. Refer to VMware's product documentation to install this product.

The steps outlined in the following section detail the process to create a new virtual machine under VMware ESX to install IWSVA.

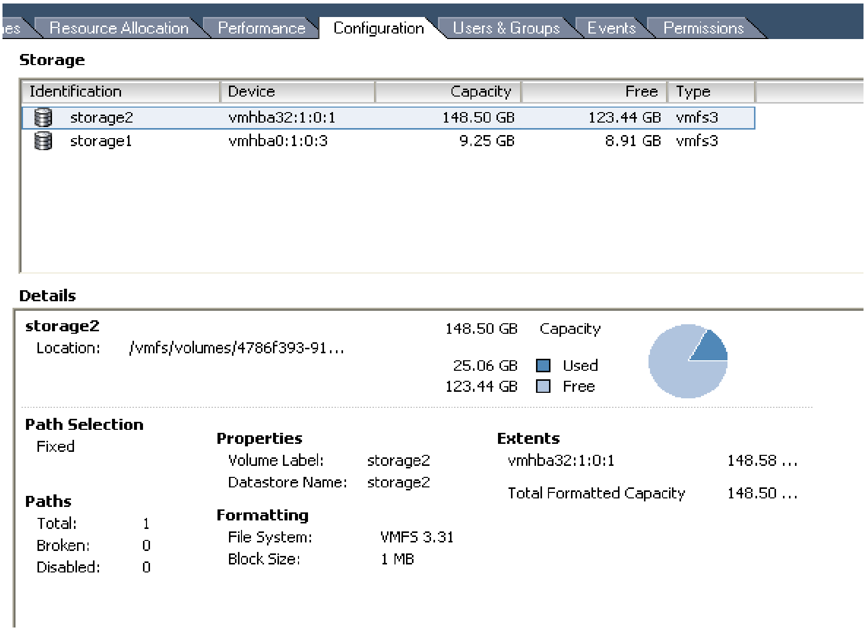
Creating a New Virtual Machine

Use the following steps as a guideline for creating the virtual machine for your environment. The number of CPUs, NIC cards, memory, and hard disk space selected should reflect the requirements for your deployment. The values entered here are for instructional purposes.

To create a new virtual machine:

1. Open the VMware Virtual Infrastructure client and click the **Configuration** tab.
2. From the **Hardware** area, click **Storage**.

3. In the **Storage** area, double click a storage area that contains enough space to upload the IWSVA ISO.



Storage

Identification	Device	Capacity	Free	Type
storage2	vmhba32:1:0:1	148.50 GB	123.44 GB	vmfs3
storage1	vmhba0:1:0:3	9.25 GB	8.91 GB	vmfs3

Details

storage2
Location: /vmfs/volumes/4786f393-91...

148.50 GB	Capacity
25.06 GB	■ Used
123.44 GB	□ Free

Path Selection
Fixed

Paths

Total:	1
Broken:	0
Disabled:	0

Properties

Volume Label:	storage2
Datastore Name:	storage2

Formatting

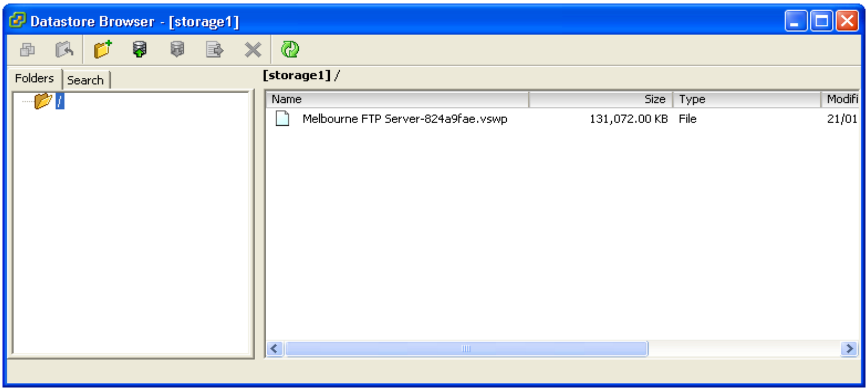
File System:	VMFS 3.31
Block Size:	1 MB

Extents

vmhba32:1:0:1	148.58 ...
Total Formatted Capacity	148.50 ...

FIGURE E-4. Configuration Tab

The Datastore Browser window opens.



Name	Size	Type	Modifi
Melbourne FTP Server-824a9fae.vswp	131,072.00 KB	File	21/01

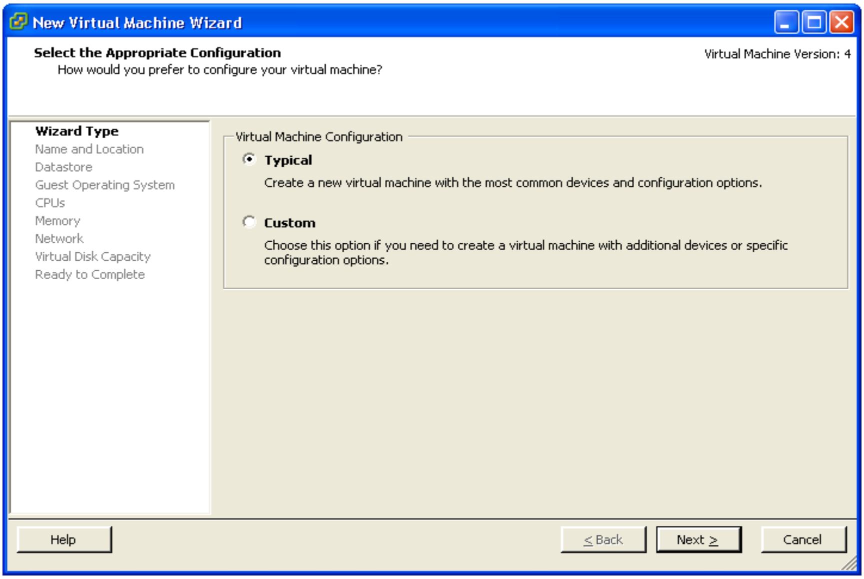
FIGURE E-5. Storage Area

4. From the button bar, click the upload button (database icon with upward-pointing arrow) and upload the IWSVA ISO to this datastore.
5. Close the datastore after the upload has completed.

To create the virtual machine

6. From the menu bar, select **File** > **New** > **Virtual Machine**.

The New Virtual Machine Wizard appears.



New Virtual Machine Wizard

Select the Appropriate Configuration
How would you prefer to configure your virtual machine?

Virtual Machine Version: 4

Virtual Machine Configuration

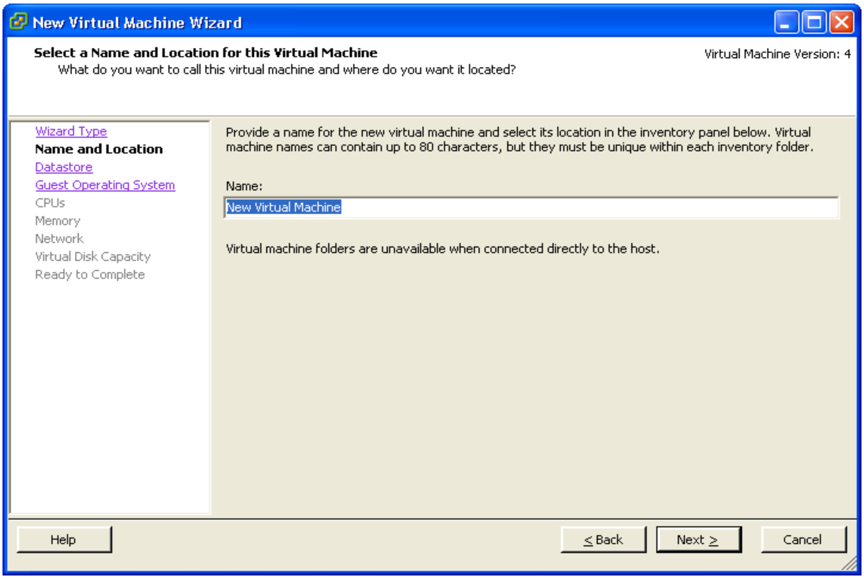
● **Typical**
Create a new virtual machine with the most common devices and configuration options.

○ **Custom**
Choose this option if you need to create a virtual machine with additional devices or specific configuration options.

FIGURE E-6. Virtual Machine Configuration

7. Under **Virtual Machine Configuration**, leave **Typical** selected.
8. Click **Next**.

The Name and Location Selection page appears.



New Virtual Machine Wizard

Select a Name and Location for this Virtual Machine
What do you want to call this virtual machine and where do you want it located?

Virtual Machine Version: 4

Provide a name for the new virtual machine and select its location in the inventory panel below. Virtual machine names can contain up to 80 characters, but they must be unique within each inventory folder.

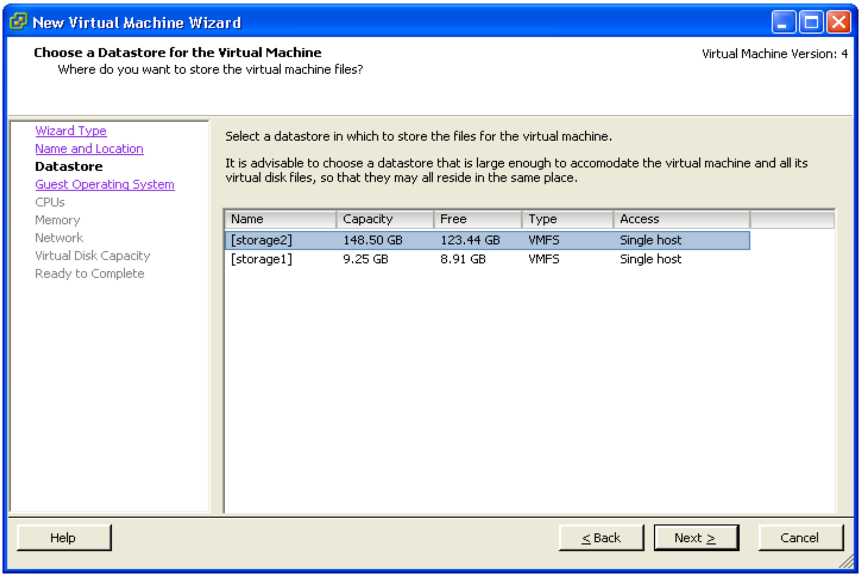
Name: New Virtual Machine

Virtual machine folders are unavailable when connected directly to the host.

FIGURE E-7. Name and Location of Virtual Machine

9. Type in the **Name** field, an appropriate machine name and then click **Next.**

The Virtual Machine Datastore Selection page appears.



Choose a Datastore for the Virtual Machine

Where do you want to store the virtual machine files?

Select a datastore in which to store the files for the virtual machine.

It is advisable to choose a datastore that is large enough to accomodate the virtual machine and all its virtual disk files, so that they may all reside in the same place.

Name	Capacity	Free	Type	Access
[storage2]	148.50 GB	123.44 GB	VMFS	Single host
[storage1]	9.25 GB	8.91 GB	VMFS	Single host

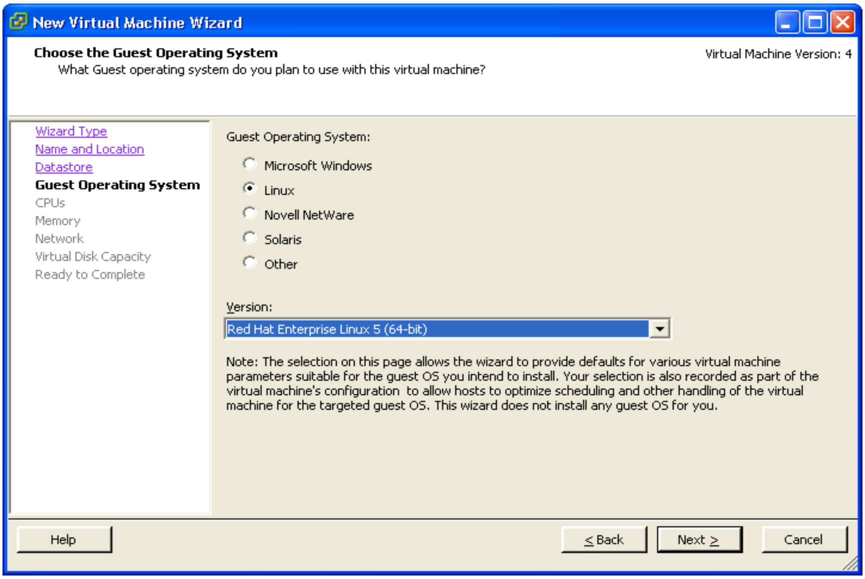
FIGURE E-8. Virtual Machine Datastore

10. Select the datastore where the virtual machine will reside.

    This does not have to be the same datastore used to upload the IWSVA ISO.

11. Click **Next**.

The Virtual Machine Guest Operating System screen appears.



Choose the Guest Operating System

What Guest operating system do you plan to use with this virtual machine?

Virtual Machine Version: 4

Guest Operating System:

○ Microsoft Windows
● Linux
○ Novell NetWare
○ Solaris
○ Other

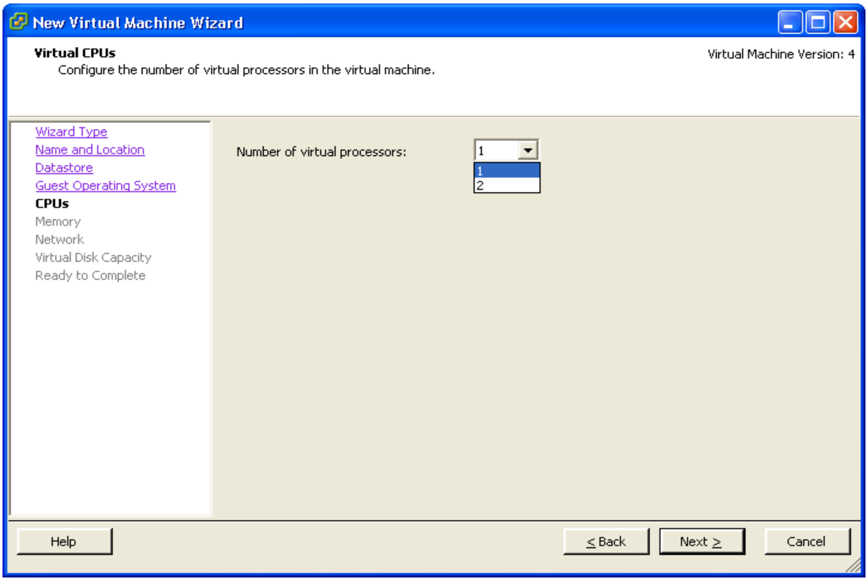
Version: Red Hat Enterprise Linux 5 (64-bit)

Note: The selection on this page allows the wizard to provide defaults for various virtual machine parameters suitable for the guest OS you intend to install. Your selection is also recorded as part of the virtual machine's configuration to allow hosts to optimize scheduling and other handling of the virtual machine for the targeted guest OS. This wizard does not install any guest OS for you.

FIGURE E-9. Virtual Machine Guest Operating System

12. For the guest operating system, select Linux and Red Hat Enterprise 5 64Bit.
13. Click **Next**.

The New Virtual Machine Wizard (Virtual CPUs) screen appears.



New Virtual Machine Wizard

Virtual CPUs

Configure the number of virtual processors in the virtual machine.

Virtual Machine Version: 4

Number of virtual processors: 1

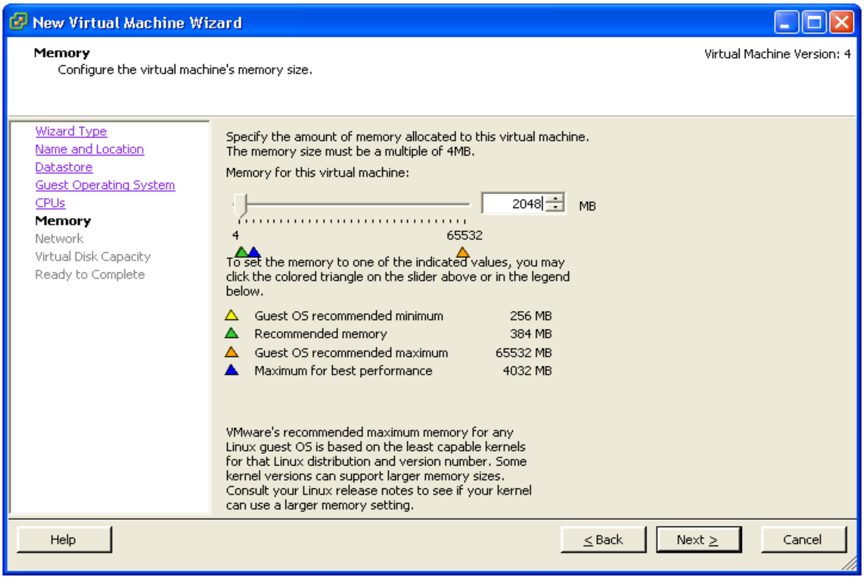
FIGURE E-10. Virtual Machine CPU

14. Select the number of processors for the virtual machine.

    IWSVA takes advantage of the Virtual SMP, so select the maximum number of virtual processors available.

15. Click **Next**.

The New Virtual Machine Wizard (Memory) screen appears.



Memory

Configure the virtual machine's memory size.

Virtual Machine Version: 4

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4MB.

Memory for this virtual machine: 2048 MB

To set the memory to one of the indicated values, you may click the colored triangle on the slider above or in the legend below.

▲	Guest OS recommended minimum	256 MB
▲	Recommended memory	384 MB
▲	Guest OS recommended maximum	65532 MB
▲	Maximum for best performance	4032 MB

VMware's recommended maximum memory for any Linux guest OS is based on the least capable kernels for that Linux distribution and version number. Some kernel versions can support larger memory sizes. Consult your Linux release notes to see if your kernel can use a larger memory setting.

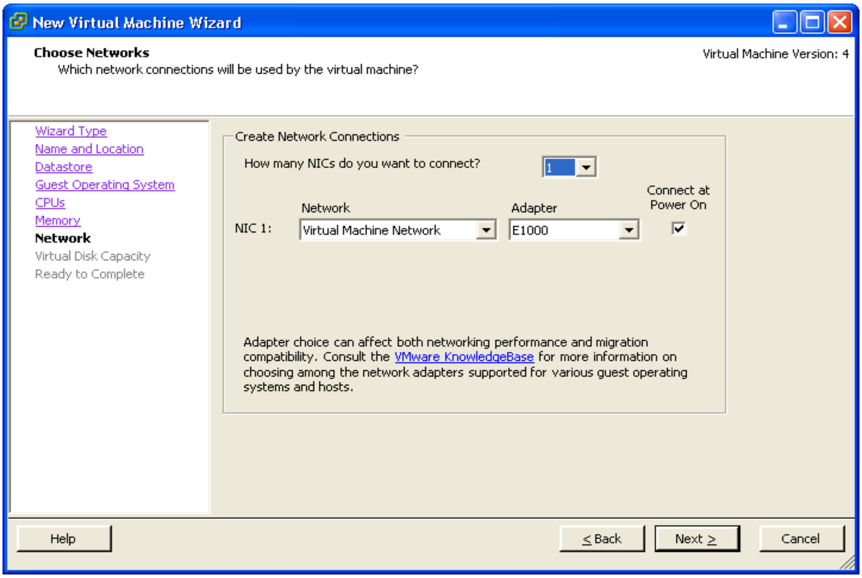
FIGURE E-11. Virtual Machine Memory

16. Allocate 2048MB of memory as a minimum for IWSVA.

    For production networks, Trend Micro recommends at least 4096 MB of RAM.

17. Click **Next**.

The New Virtual Machine Wizard (Memory) screen appears.



New Virtual Machine Wizard

Choose Networks

Which network connections will be used by the virtual machine?

Virtual Machine Version: 4

Create Network Connections

How many NICs do you want to connect? 1

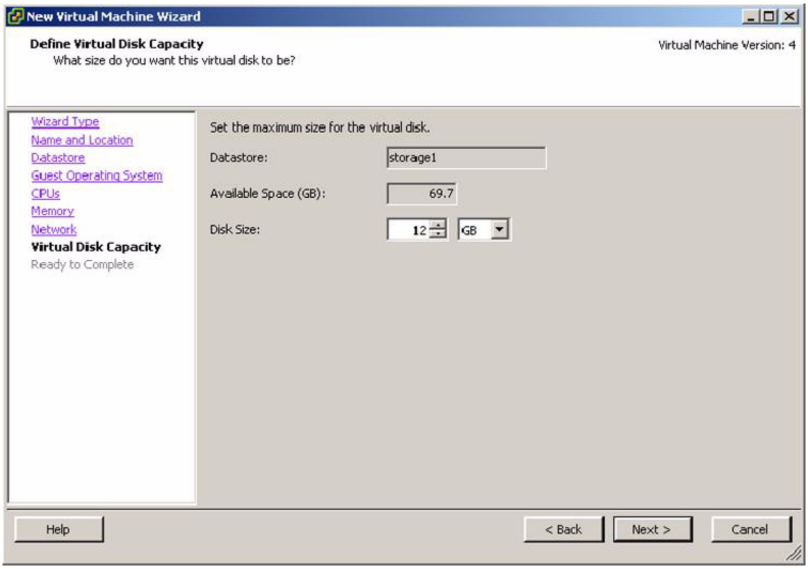
	Network	Adapter	Connect at Power On
NIC 1:	Virtual Machine Network	E1000	☑

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

FIGURE E-12. Virtual Machine Network

18. Accept the default network settings and then click **Next**.

The Virtual Disk Capacity screen appears.



New Virtual Machine Wizard

Define Virtual Disk Capacity

What size do you want this virtual disk to be?

Virtual Machine Version: 4

Set the maximum size for the virtual disk.

Datastore: storage1

Available Space (GB): 69.7

Disk Size: 12 GB

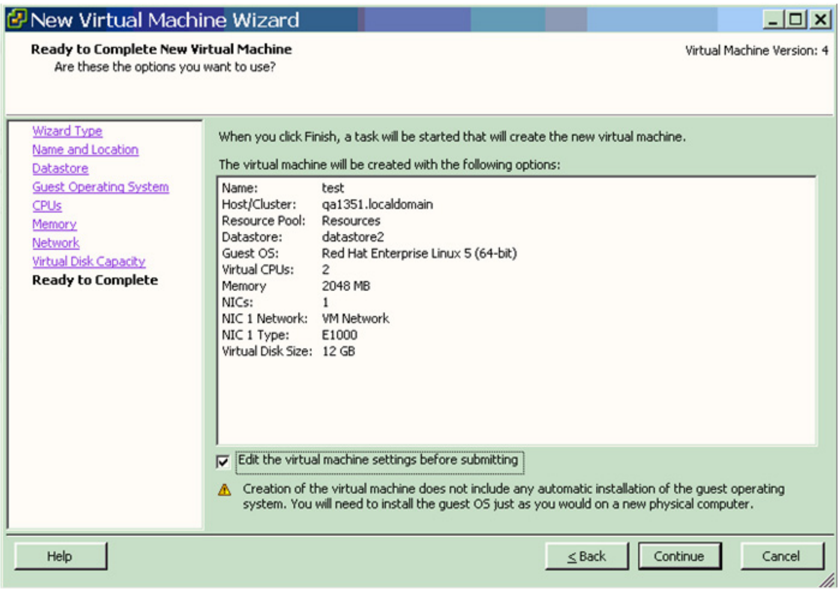
FIGURE E-13. Virtual Disk Capacity

19. For testing purposes, it is adequate to leave the 12GB disk allocation at its default.

    For production environments, provide at least 300GB for logging and reporting purposes. See *Hardware Requirements on page 1-2* for more information on disk space allocation.

20. Click **Next**.

The New Virtual Machine Wizard (Ready to Complete New Virtual Machine) screen appears.



Ready to Complete New Virtual Machine
Are these the options you want to use?

Virtual Machine Version: 4

When you click Finish, a task will be started that will create the new virtual machine.

The virtual machine will be created with the following options:

Name:	test
Host/Cluster:	qa1351.localdomain
Resource Pool:	Resources
Datastore:	datastore2
Guest OS:	Red Hat Enterprise Linux 5 (64-bit)
Virtual CPUs:	2
Memory	2048 MB
NICs:	1
NIC 1 Network:	VM Network
NIC 1 Type:	E1000
Virtual Disk Size:	12 GB

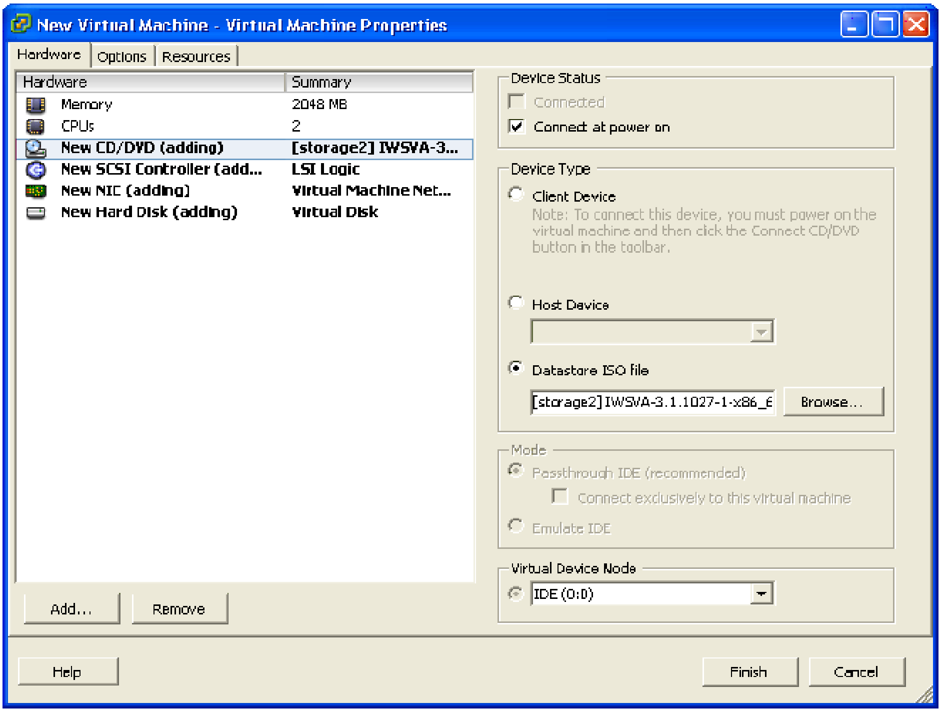
☑ Edit the virtual machine settings before submitting

⚠ Creation of the virtual machine does not include any automatic installation of the guest operating system. You will need to install the guest OS just as you would on a new physical computer.

FIGURE E-14. Ready to Complete

21. Check the **Edit the virtual machine settings before submitting** check box and then click **Continue**.

The Virtual Machine Properties screen appears.



New Virtual Machine - Virtual Machine Properties

Hardware	Summary
Memory	2048 MB
CPUs	2
New CD/DVD (adding)	**[storage2] IWSVA-3...**
New SCSI Controller (add...	**LSI Logic**
New NIC (adding)	**Virtual Machine Net...**
New Hard Disk (adding)	**Virtual Disk**

Device Status

□ Connected

☑ Connect at power on

Device Type

○ Client Device

Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar.

○ Host Device

● Datastore ISO file

[storage2] IWSVA-3.1.1027-1-x86_6

Mode

● Passthrough IDE (recommended)

□ Connect exclusively to this virtual machine

○ Emulate IDE

Virtual Device Node

IDE (0:0)

FIGURE E-15. Virtual Machine Properties screen

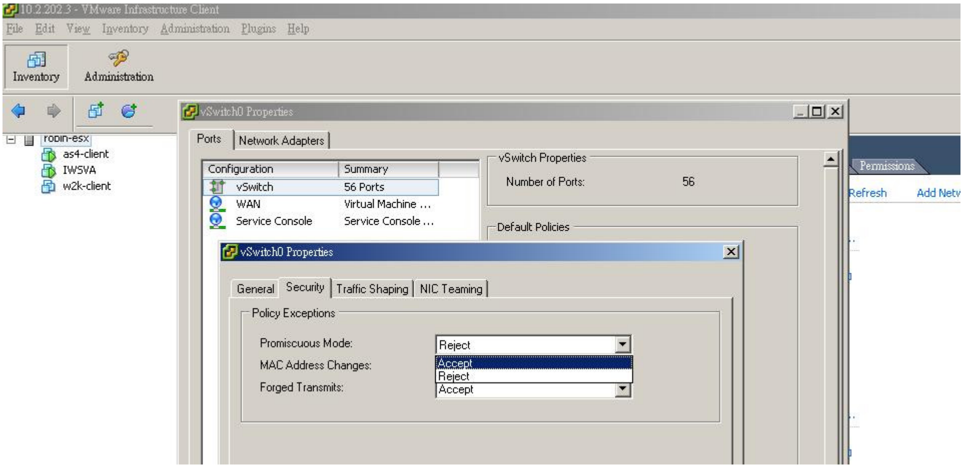
22. Click on the floppy drive and then click **Remove**.
23. Select the **New CD/DVD** option and then select the **Datastore ISO file** radio button on the right hand side.
24. Click **Browse** and then select the IWSVA ISO that was uploaded in Step 4.

    If you did not copy the Installation ISO onto the VMware server's hard disk, then you can select **Host Device** or **Client Device** from which to load the installer. **Client Device** uses the remote workstation's CD/DVD ROM drive to perform the installation and **Host Device** uses the VMware Server's CD/DVD ROM drive to perform the installation. Using one of these two methods saves about 500 MB or more of disk space on the VMware server.

25. Ensure that the **Connect at power on** check box for the **New CD/DVD** is checked.

Note: When IWSVA is installed on a VMware ESX server and configured in Transparent Bridge mode, you must enable the virtual switch to accept the Promiscuous mode in the ESX server.

When deploying IWSVA in bridge mode, do not connect the two data network interfaces to the same switch; otherwise, a loop will be created in your network.



Configuration	Summary
vSwitch	56 Ports
WAN	Virtual Machine ...
Service Console	Service Console ...

Number of Ports: 56

Promiscuous Mode: Reject (Accept / Reject)

MAC Address Changes:

Forged Transmits: Accept

FIGURE E-16. Promiscuous mode in the ESX 3.5 server

26. Click **Finish**.

    The new IWSVA 5.1 Virtual Machine is now ready and configured to be powered on and begin the installation process.

Index