TREND MICRO

Intrusion Defense Firewall 1.5

Advanced threat protection for Endpoints

for OfficeScan Client/Server Edition

Administrator's Guide

Endpoint Security

Document Part No.: OSEM15025/110817

Release Date: September 2011

The user documentation for Trend Micro Intrusion Defense Firewall introduces the main features of the software and installation instructions for your production environment. Read through it before 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 always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:
http://www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Chapter 1: Introducing Intrusion Defense Firewall

Chapter 2: Getting Started with Intrusion Defense Firewall

Chapter 3: Dashboard

Chapter 4: Alerts

Chapter 5: Reports

Chapter 6: Managing Computers

Chapter 7: Security Profiles

Chapter 8: Using the IDF Firewall

Chapter 9: Using Deep Packet Inspection

Chapter 10: Components

Chapter 11: Managing the IDF Server Plug-in

Chapter 12: System

Chapter 13: Logging

Chapter 14: Getting Help

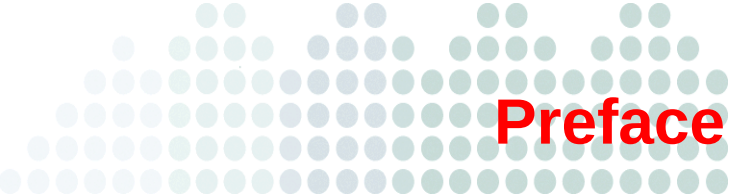
Appendix A: Ports Used by IDF

Appendix B: Computer and Client Plug-in Status

Appendix C: Events

Index

List of Tables



Preface

Welcome to the Trend Micro™ Intrusion Defense Firewall™ *Administrator's Guide*. This guide discusses getting started information, client installation procedures, and Intrusion Defense Firewall (IDF) server and client management.

Topics in this chapter:

Intrusion Defense Firewall Documentation

Intrusion Defense Firewall documentation includes the following:

TABLE P-1. OfficeScan documentation

DOCUMENTATION	DESCRIPTION
Deployment Guide	A PDF document that discusses requirements and procedures for installing the IDF Server Plug-in, upgrading the Server Plug-in, and installing the IDF Client Plug-in
Administrator's Guide	A PDF document that discusses getting started information, IDF Client Plug-in installation procedures, and IDF Server Plug-in and Client Plug-in management
Help	HTML files that provide "how to's", usage advice, and field-specific information. The Help is accessible from the IDF Server Plug-in user interface.
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation.
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: http://esupport.trendmicro.com/support

Download the latest version of the PDF documents and readme at:

http://www.trendmicro.com/download

Audience

The Intrusion Defense Firewall documentation is intended for OfficeScan Administrators who are responsible for OfficeScan management. These users are expected to have in-depth knowledge of networking, server management, and OfficeScan.

Document Conventions

To help you locate and interpret information easily, the OfficeScan documentation uses the following conventions:

TABLE P-2. 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 tasks
Italics	References to other documentation or new technology components
TOOLS > CLIENT TOOLS	A "breadcrumb" found at the start of procedures that helps users navigate to the relevant Web console screen. Multiple breadcrumbs means that there are several ways to get to the same screen.
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, C:\Program Files\<file_name> can be C:\Program Files\sample.jpg.
Note: text	Provides configuration notes or recommendations

TABLE P-2. Document conventions (Continued)

CONVENTION	DESCRIPTION
Tip: text	Provides best practice information and Trend Micro recommendations
WARNING! text	Provides warnings about activities that may harm computers on your network

Chapter 1

Introducing Intrusion Defense Firewall

This chapter introduces Trend Micro™ Intrusion Defense Firewall™ and describes what's new in this release.

Topics in this chapter:

About Instrusion Defense Firewall

Trend Micro™ Intrusion Defense Firewall™ 1.5 for OfficeScan™ is an advanced intrusion defense system. It provides the best and last line of defense against attacks that exploit vulnerabilities in commercial and custom software, including web applications. IDF enables you to create and enforce comprehensive security policies that proactively protect sensitive data, applications, computers or network segments. The system consists of an IDF Server Plug-in™ and multiple IDF Client Plug-ins™.

New in this Release

Trend Micro™ Intrusion Defense Firewall™ includes the following new features and enhancements:

Performance and Scalability

Intrusion Defense Firewall 1.5 brings increased overall performance and scalability by significantly improving the speed and efficiency of security update deployments, heartbeats, recommendation scans, memory usage, and the IDF Server Plug-in user interface.

Automatic Activation and/or Protection of Newly Added Computers

Tasks now let you automatically and conditionally activate and/or assign Security Profiles to computers that are:

- Added via Client Plug-in-initiated activation
- Added when OfficeScan client inventory is synchronized

Expanded OfficeScan Corporate Edition (OSCE) Support

Intrusion Defense Firewall 1.5 supports the following OSCE features:

- OSCE 10.6 and PLM 2.0
- OSCE dashboard widgets
- OSCE mash-up widgets

Event Tagging

Event Tagging allows you to manually tag events with predefined or custom labels, which enables specialized views of events, dashboards, and reports that can be applied to a single event, similar events, or even to all future similar events.

Expanded Platform and File System Support

Intrusion Defense Firewall 1.5 supports the following client and server platforms:

- 32- and 64-bit clients and servers
- Separate 32- and 64-bit client deployment
- FAT32 file systems
- Microsoft SQL Server 2008

Multi-Language Support

Intrusion Defense Firewall 1.5 is available in multiple language versions. Please contact Trend Micro to find out what languages are available.

Chapter 2

Getting Started with Intrusion Defense Firewall

This chapter introduces the Trend Micro™ Intrusion Defense Firewall™ Server Plug-in, describes the basics of the Server Plug-in interface, and provides an overview of the Server Plug-in screens. For a description of how to install and configure IDF, see the *Intrusion Defense Firewall Deployment Guide*.

Topics in this chapter:

The IDF Server Plug-in

The IDF Server Plug-in is the application for managing all client computers. The server performs two important functions:

- Installs, monitors, and manages IDF clients
- Downloads most of the components needed by clients. The server downloads components from the Trend Micro ActiveUpdate server and then distributes them to clients.

The IDF Server Plug-in is capable of providing real-time, bidirectional communication between the server and clients. The IDF Server Plug-in operates as a plug-in to OfficeScan and allows you to manage the clients from the browser-based OfficeScan Web console, which you can access from virtually anywhere on the network. The server communicates with the client (and the client with the server) through Hypertext Transfer Protocol (HTTP).

The IDF Client Plug-in

Protect computers from security risks by installing the IDF Client Plug-in on each computer. The client provides Port Scanning and Recommendation Scanning.

Opening the IDF Server Plug-in Interface

The IDF Plug-in Interface is the central point for monitoring Internet Defense Firewall. The IDF Plug-in Interface opens as a plug-in to the OfficeScan Web console. Once logged into OfficeScan Web console, you can access the IDF Server Plug-in.

To open the IDF Server Plug-in:

1. Open the OfficeScan Web console.
2. In the navigation panel, click **Plug-in Manager**.
3. In the Intrusion Defense Firewall section, click **Manage Program**.

   The Intrusion Defense Firewall - Getting Started screen appears.
4. To open IDF next time without the Getting Started screen displayed, select **Do not display this message the next time I access the Intrusion Defense Firewall**.
5. In the Intrusion Defense Firewall - Getting Started screen, click **Continue**.

   IDF Interface opens with the Dashboard displayed.

FIGURE 2-1. IDF Dashboard

IDF Server Plug-in Interface

IDF Server Plug-in's web-based user interface was designed to provide you with easy access to all elements of the IDF system. The following are its main features.

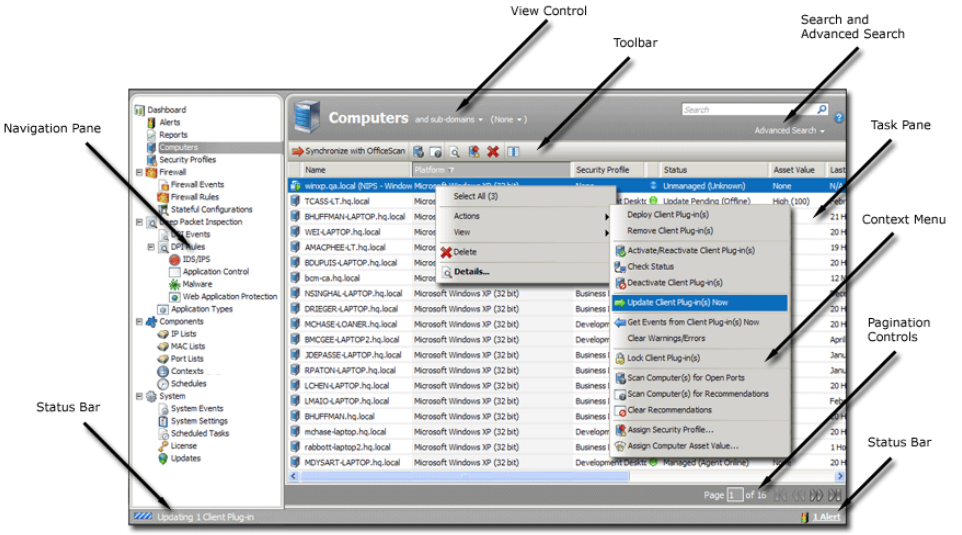


FIGURE 2-2. IDF User Interface

Navigation Pane

The navigation pane contains the tree-based navigation system. Elements of the IDF system are organized as follows:

- **Dashboard**: an at-a-glance overview of the status of the IDF system
- **Alerts**: a summary of current critical and warning alerts concerning system or security events
- **Reports**: a report generator to produce summaries of system status and summaries of activities
- **Computers**: a list of computers on your network with status information for each
- **Security Profiles**: a list of defined Security Profiles
- **Firewall**

    - **Firewall Events**: logs of security-related Firewall activity
    - **Firewall Rules**: where you define and manage Firewall Rules
    - **Stateful Configurations**: where you define and manage Stateful Configurations
- **Deep Packet Inspection**
    - **DPI Events**: logs of security-related DPI activity
    - **DPI Rules**: where you define and manage DPI Rules
    - **Application Types**: Application Types are defined by connection direction, protocol, and ports. They define the traffic DPI Rules operate on.
- **Components**: a list of common components used by various elements of the IDF system
- **System**: where you can find administrative tools to manage the operation of the IDF system, and view records and reports of system events

Task Pane

Clicking an element in the navigation pane will display that element's screen in the task pane. Almost all of your work will be done on a screen in the task pane. Where the task pane displays lists of items, columns can be added or removed by clicking the **Add/Remove Columns** button in the toolbar (). The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Pagination Controls

Some lists displayed in the task pane will contain more elements than can be shown on a single screen. When this is the case, the pagination information shows the subset of items you are viewing. Use the pagination tool to move from page to page of your list or enter an item number in the text box to start the list there. The number of items to display per page can be configured in the System section.

View Control

Where appropriate, the view control gives you options for displaying listed items. For example, when you click a computer domain in the navigation pane, computers belonging to that domain will be listed in the task pane. The view control will let you choose between displaying only computers from that domain, and displaying computers in that domain and all sub-domains. Where appropriate, the view control lets you organize your listed items into categories. For example, you may want to domain your listed computers by the Security Profile that has been assigned to them.

Toolbar

The toolbar holds buttons which carry out various actions specific to the screen you are working in. Most commonly, these will include buttons for the deletion, modification, and creation of list items. Many of the toolbar options are also available from the context menu. The IDF Server Plug-in allows you to save your searches for reuse. This effectively lets you create reusable filters to apply to listed items.

Search and Advanced Search

The simplest way to search is to use the "simple" search bar.

FIGURE 2-3. The Simple Search Bar

This will search the database for matches among the listed items (Firewall Events in the Firewall screen, System Events on the System Events screen, etc.)

Note: All items will be searched, not just the ones currently displayed. For instance, if you are viewing Firewall Events for all computers over the last 7 days, the Firewall Events screen may display a message like "Only the most recent 1,000 out of 55,056 items have been included. Consider using a narrower date range or additional search criteria." Even though only 1000 items are made available for display, all 55,056 items will be searched. The search engine will search through each field in the database except the date.

For more sophisticated searches, click “Advanced Search” and then “Open Advanced Search”.

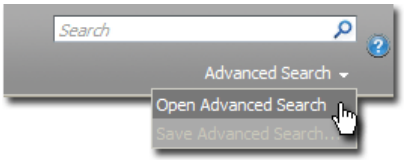


FIGURE 2-4. Advanced Search

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by domain or computer Security Profiles.

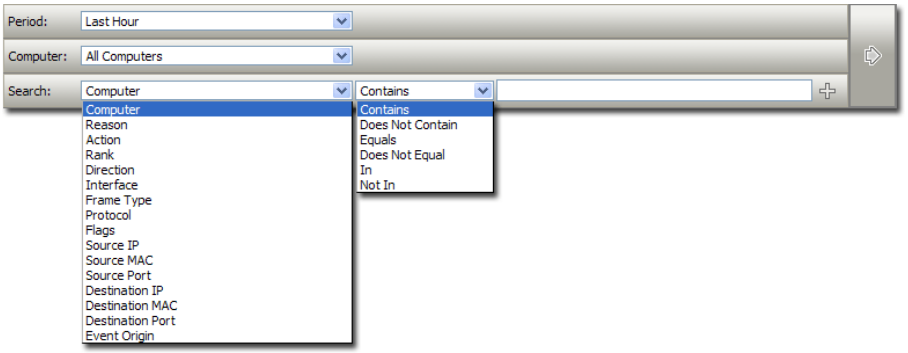


FIGURE 2-5. Computers Toolbar

Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string

- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Status Bar

The status bar displays information relating to the current state of your IDF system. The number of active alerts (if any) is displayed at the right edge of the status bar. The left side of the status bar dynamically displays what actions are currently in progress such as computer-discovery, port-scanning operations, Client Plug-in activations, Client Plug-in updates, or Client Plug-in upgrades.

Context Menus

Many of the IDF Server Plug-in's screens have context-sensitive menus. Right-clicking a security Profile, for example, gives you a context menu with quick access to most of the options in the toolbar for that screen. Right-clicking a computer domain displays a context menu with options to manage the current domain or create a new one.

Note: Many elements of the UI display informative tool tips when the mouse pointer is held over them.

Program Overview

The Server Plug-in provides the following screens for managing Intrusion Defense Firewall:

- Dashboard
- Alerts
- Reports
- Computers

- Security Profiles
- Firewall
- Deep Packet Inspection
- Components
- System

Dashboard

The Dashboard provides a quick at-a-glance view of the state of the IDF system. The following figure shows an example of the Dashboard display.

FIGURE 2-6. Dashboard screen

The Dashboard displays information panels, called “widgets”, that can be customized on the screen and filtered by date/time range. For detailed information about the Dashboard, see *Dashboard* starting on page 3-1.

Alerts

The Alerts screen allows you to view and configure IDF Alerts. IDF Alerts notify you when important events occur that may require action. The following figure shows the Alerts screen.

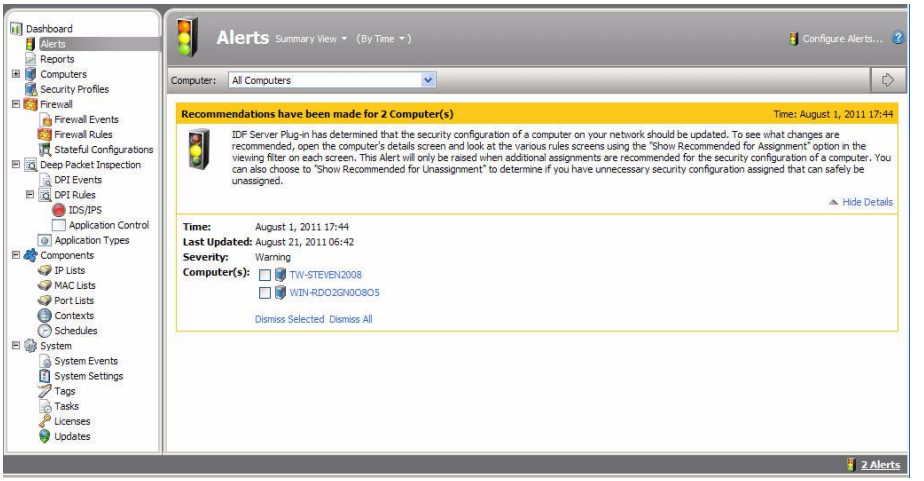


FIGURE 2-7. Alerts screen

For detailed information about the Alerts screen, see *Alerts* starting on page 4-1.

Reports

The Reports screen allows you to generate reports. The following figure shows the Reports screen.

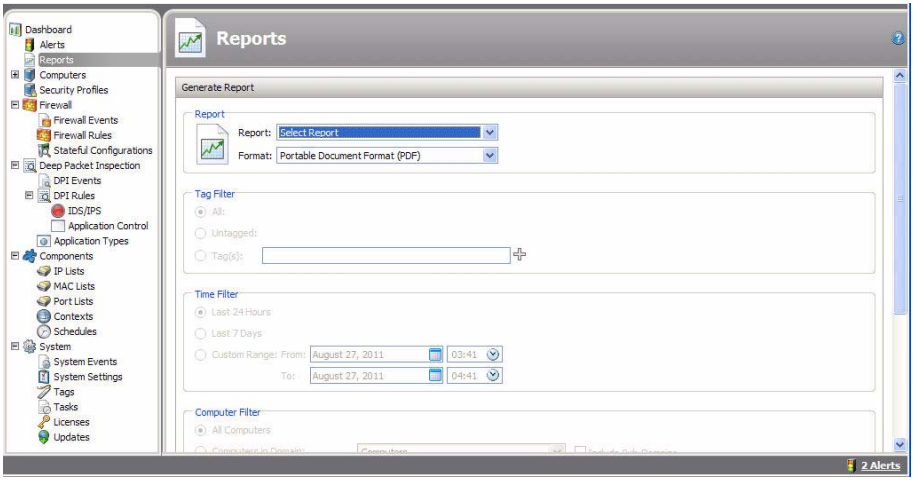


FIGURE 2-8. Reports screen

For detailed information about generating reports, see *Reports* starting on page 5-1.

Computers

The Computers screen allows you to manage the computers in your network. The following figure shows the Computers screen.

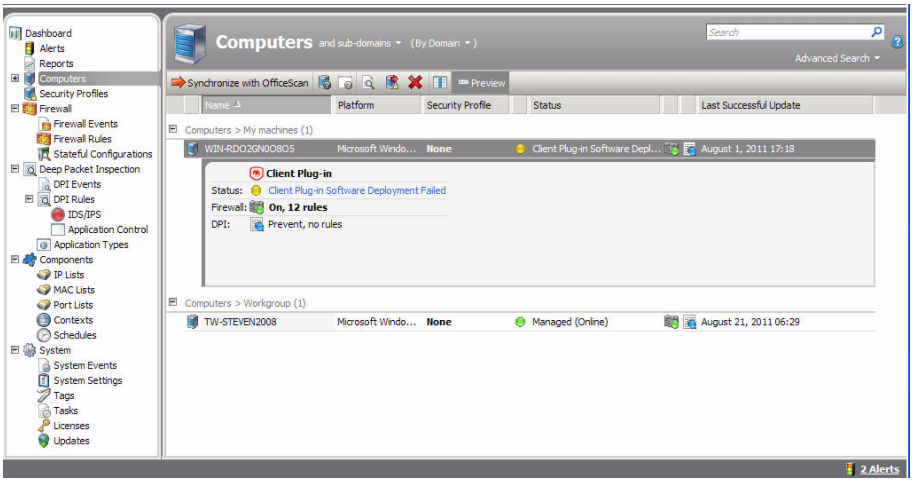


FIGURE 2-9. Computers screen

For detailed information about how to manage computers, see *Managing Computers* starting on page 6-1.

Security Profiles

Security Profiles allow common configurations of Firewall Rules, Stateful Configurations, and DPI Rules to be saved for easy assignment to multiple computers. The following figure shows the Security Profiles screen.

FIGURE 2-10. Security Profiles screen

For detailed information about Security Profiles, see *Security Profiles* starting on page 7-1.

Firewall

The Firewall screen allows you to manage the Firewall, including monitor Firewall Events and configure Firewall Rules. The following figure shows the Firewall Rules screen.

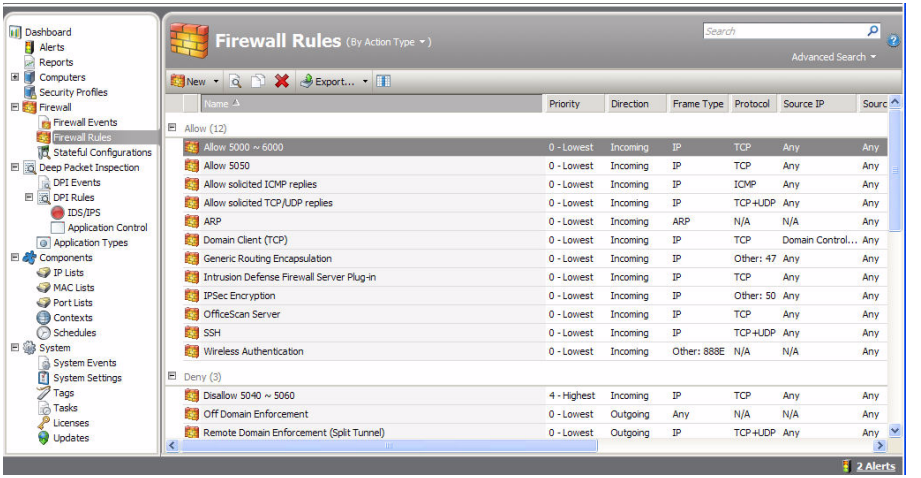


FIGURE 2-11. Firewall screen

For more information on managing the Firewall, see *Using the IDF Firewall* starting on page 8-1.

Deep Packet Inspection

The Deep Packet Inspection screen enables you to monitor DPI events and configure DPI Rules. The following figure shows the DPI Rules screen.

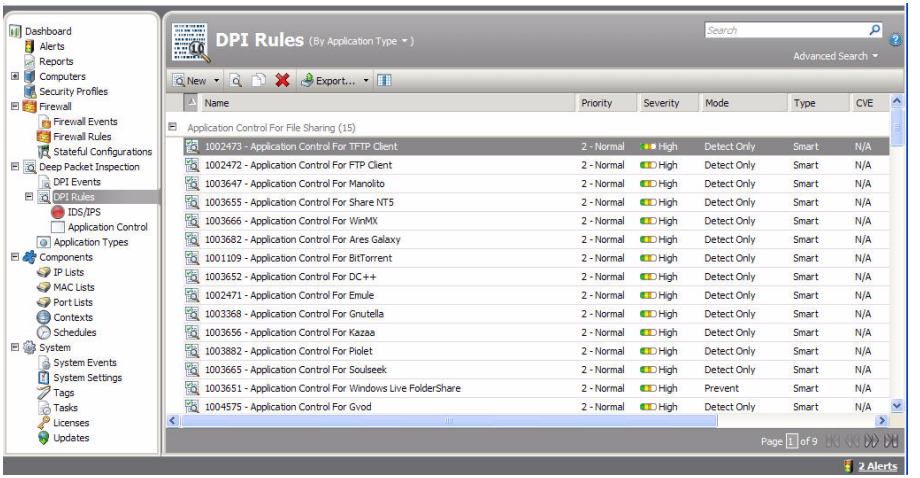


FIGURE 2-12. Deep Packet Inspection DPI Rules screen

For more information on managing Deep Packet Inspection, see *Using Deep Packet Inspection* starting on page 9-1.

Components

The Components screens allow you to manage IP lists, MAC lists, Port lists, Contexts, and Schedules. The following figure shows the Components Port Lists screen.

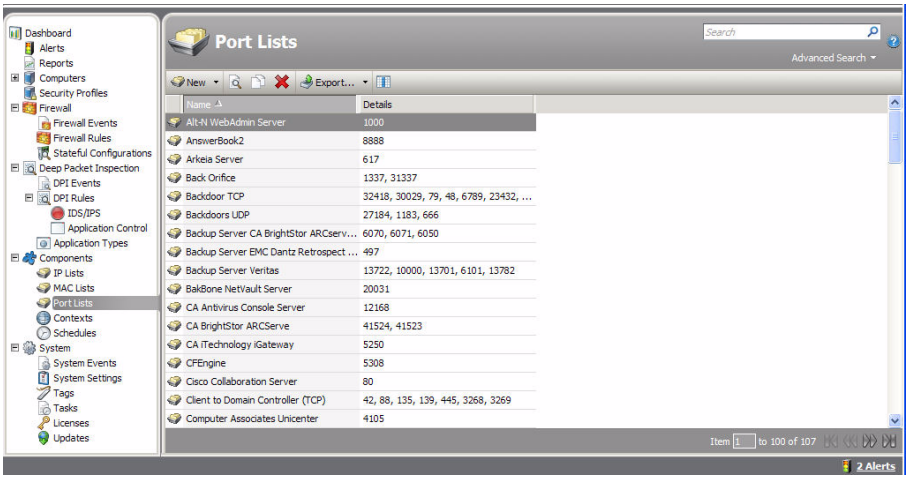


FIGURE 2-13. Components Port Lists screen

For more information on managing components, see *Components* starting on page 10-1.

System

The System screens allow you to manage system tasks, including monitor system events, configure system settings, define event tags, define tasks, and manage licenses and updates. The following figure shows the System Events screen.

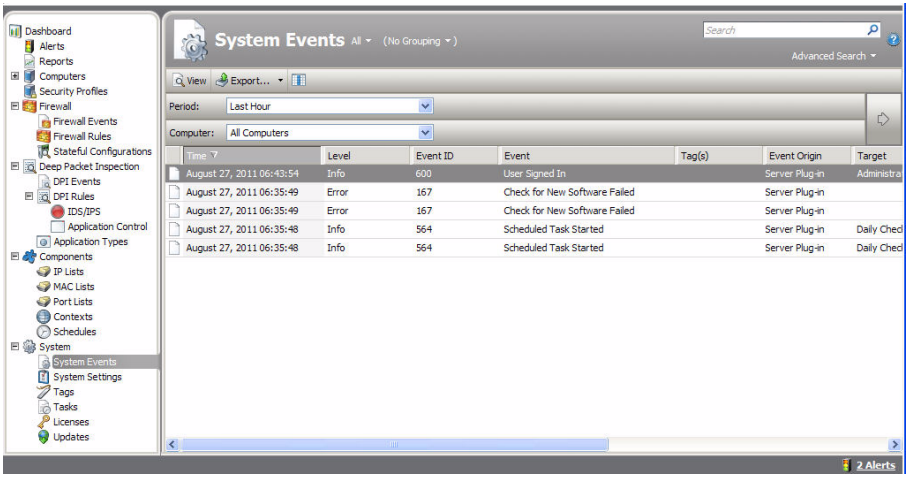


FIGURE 2-14. System Events screen

For more information, see *System* starting on page 12-1.

Chapter 3

Dashboard

This chapter describes how to use Trend Micro™ Intrusion Defense Firewall™ Dashboard.

Topics in this chapter:

About the Dashboard

The Dashboard is the first screen that comes up after you log in to the IDF Server Plug-in. The Dashboard provides a quick at-a-glance view of the state of the IDF system by displaying a configurable number of information panels, called "widgets," that provide information such as Alert history and status, computer status, firewall activity, DPI activity, Reconnaissance Scan history, and System Event history. When logging in to the IDF Server Plug-in, the layout of the Dashboard is preserved from your last session.

FIGURE 3-1. Dashboard

To open the Dashboard, select **Dashboard** from the IDF Main Menu.

About Widgets

Many widgets contain links to let you "drill down" to the data. For example, clicking a column in the DPI History chart takes you to the DPI Events screen listing all the DPI Events that occurred on that day.

Note: The trend indicators next to the numeric values in the 1x1 widgets. An upward or downward pointing triangle indicates an increase or decrease compared to the previous time period, and a flat line indicates no significant change.

Customizing the Dashboard

Several aspects of the Dashboard can be configured and customized, and layouts can be saved and displayed when you log in. (The Dashboard will be displayed as you left it when you logged out.

Configurable elements of the Dashboard display are by tag, the time period the data is taken from, which computers' or computer domains' data is displayed, which widgets are displayed, and the layout of those widgets on the screen.

Configuring Widget Layout

Widgets can be rearranged on the screen by selecting them by the title bar, and dragging and dropping them to their new locations. Move the widget over an existing one and they will exchange places. (The widget that is about to be displaced will temporarily gray out.) Widgets can also be added to or removed from the Dashboard display.

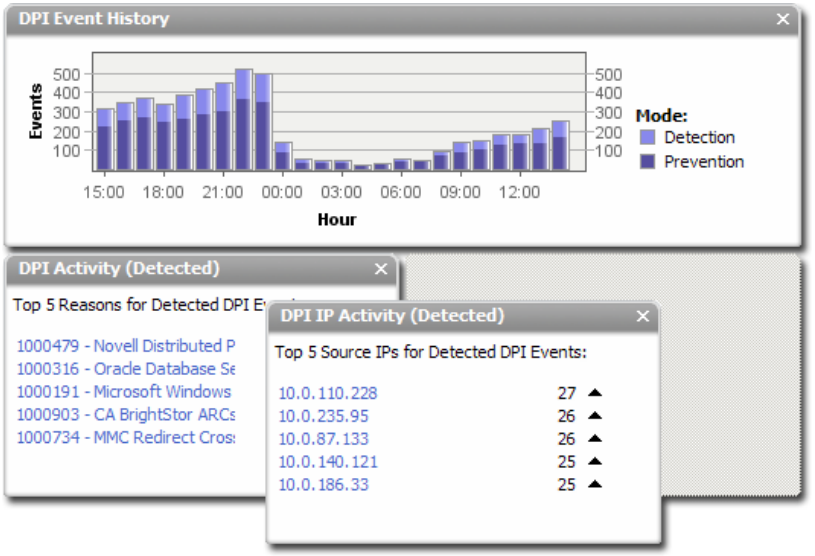


FIGURE 3-2. Changing Widget Layout

Adding and Removing Dashboard Widgets

Click **Add/Remove Widgets...** at the top right of the Dashboard to open the Add/Remove Widgets window to view the list of available widgets and choose which widgets to display.

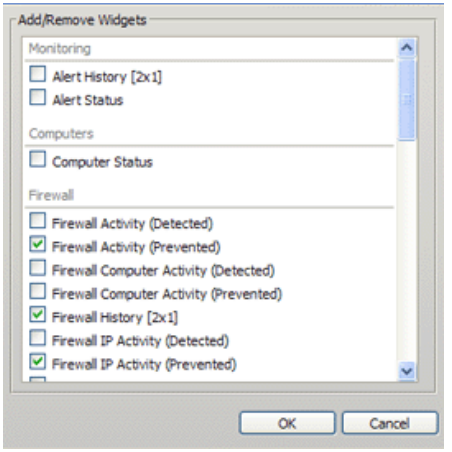


FIGURE 3-3. Adding and removing Dashboard Widgets

To remove a widget from the Dashboard, click the "X" in the top-right corner of the widget.

Filtering Information by Tags

The Dashboard allows you to filter information by one or more tags, or to view all or untagged information. To switch between these views, use the drop-down menu at the top of the screen.

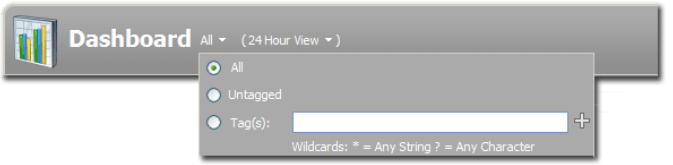


FIGURE 3-4. View by Tag

To filter by tags, enter the tag names into the **Tag(s)** box. Use * to indicate any string and ? to indicate any character. To remove the filter, select **All** or **Untagged**.

Filtering Information by Date/Time Range

The Dashboard displays data from either the last 24 hours, or the last seven days. To switch between these two views, use the drop-down menu at the top of the screen.

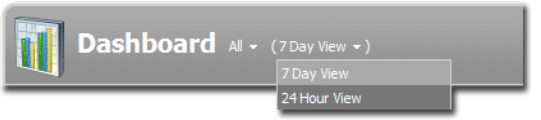


FIGURE 3-5. Date/Time Range

Filtering by Computer and Computer Domain

Use the Computer: drop-down menu to filter the displayed data to display only data from specific computers.

FIGURE 3-6. Computers and Computer Domains

Managing Dashboard Configurations

Individual Dashboard configurations can be saved, loaded, and deleted using the **Configuration** menu at the top right of the Dashboard.

To save a Dashboard configuration:

PATH: IDF MAIN MENU | DASHBOARD

1. Add, remove, and rearrange widgets and set any filters as desired.
2. Click the **Configuration** menu in the top right of the Dashboard and select **Save Configuration...**
3. Enter a name in the **Name** box and click **OK**.

To delete a Dashboard configuration:

PATH: IDF MAIN MENU | DASHBOARD

- Click the **Configuration** menu in the top right of the Dashboard and click the X next to the Configuration name.

Opening a Saved Dashboard Configuration

To open a saved configuration, click **Configuration** and select the configuration from the drop-down menu

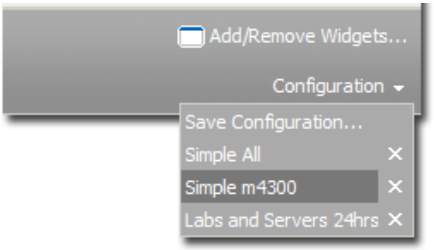


FIGURE 3-7. Opening a Saved Dashboard Configuration

Chapter 4

Alerts

This chapter describes how to use Trend Micro™ Intrusion Defense Firewall™ Alerts to monitor events.

Topics in this chapter:

About Alerts

There are just over 60 conditions that trigger Alerts in the IDF system. Generally Alerts exists to warn of system status anomalies such as computers going offline or DPI Rules being out of date, although there are some alerts for the detection of fingerprinting scans and other security-related events. (For notifications of individual DPI and Firewall Events, consider setting up a Syslog server.)

Viewing Alerts

The Alerts screen displays all active alerts. Alerts can be displayed in a Summary View which will domain similar alerts together, or in List View which lists all alerts individually. To switch between the two views, use the drop-down menu next to "Alerts" in the screen's title.

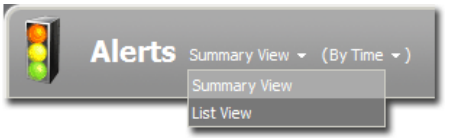


FIGURE 4-1. Alerts

In Summary View, expanding an alert panel (by clicking **Show Details**) displays all the computers that have generated that particular alert. (Clicking the computer will display the computer's Details window.)

In Summary View if the list of computers is longer than five, an ellipsis ("...") appears after the fifth computer. Clicking the ellipsis displays the full list. Once you have taken the appropriate action to deal with the alert, you can dismiss the alert by selecting the checkbox next to the target of the alert and clicking the **Dismiss** link. (In List View, right-click the alert to see the list of options in the context menu.)

Alerts can be of two types: system and security. System alerts are triggered by System Events (Client Plug-in Offline, Clock Change on Computer, etc.) Security alerts are triggered by DPI and Firewall Rules. Alerts can be configured by clicking **Configure Alerts....**

Note: Use the computers filtering bar to view only alerts for computers in a particular computer domain, with a particular Security Profile, etc.

Configuring Alerts

Alerts can be turned on or off, the severity set to Warning or Critical, and which of the following actions to take when an Alert occurs.

- Send email to notify when this alert is raised.
- Send email to notify when conditions for this alert change, such as the number of items.
- Send email to notify when this alert no longer exists.

To configure Alerts:

PATH: IDF MAIN MENU | ALERTS

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS > SYSTEM

1. Click **Configure Alerts...** at the top-right of the Alert screen, or in the System screen, click **View Alert Configuration...**

   The Alert Configuration window opens, showing a list of the alerts, along with Severity and On/Off information.
2. To filter the list, choose **By Severity** or **No Grouping** from the drop-down list at the top of the screen.
3. To view alert information and edit the actions precipitated by each alert, right-click on the alert and select **Properties...** to open the Properties window.

   Alerts can be turned on or off; their severity can be switched between Warning and Critical.

   Note: Alerts cannot be configured differently for individual Security Profiles or computers. All configuration changes to an Alert's properties are global.

You can specify a default email address to which all email alerts will be sent. To set up Alert emails, see the next section, *Setting Up Alert Emails*.

Setting Up Alert Emails

The IDF Server Plug-in can send an email when selected alerts are triggered. To enable the email system, you must give IDF Server Plug-in access to an SMTP mail server. You must configure your SMTP settings and select which alerts will trigger emails. There are over 30 conditions that trigger alerts and you may not want all of them to trigger the sending of an email.

To configure your SMTP Settings:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS > SYSTEM

1. In the "SMPTP" area, type the address of your SMTP mail (with the port if required).
2. Enter a "From" email address from which the emails should be sent. Optionally type a "bounce" address to which delivery failure notifications should be sent if the alert emails can't be delivered.
3. If your SMTP mail server requires outgoing authentication, type the username and password credentials. Once you've entered the necessary information, use **Test SMTP Settings** to test the settings.

To configure which alerts trigger the sending of an email:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

4. Click the **System** tab, then click **View Alert Configuration...** to display the list of all alerts.

   A checkmark in the "On" column indicates whether the alert is on or not. If it is on, it means the alert will be triggered if the corresponding situation arises, but it does not mean an email will sent out.
5. Double-click an alert to view its **Alert Configuration** screen, or right-click on the alert and select **Properties...** from the popup menu.
6. To have an alert trigger an email, choose **On** and select at least one of the **Send Email** checkboxes.

Chapter 5

Reports

This chapter describes how to configure and generate Trend Micro™ Intrusion Defense Firewall™ reports.

Topics in this chapter:

About Reports

Most of the reports generated by the Reports screen have configurable parameters such as date range or reporting by computer domain. Parameter options will be disabled for reports to which they don't apply. The available report types are:

- Alert Report
- Attack Report
- Firewall Report
- Forensic Computer Audit Report
- Computer Report
- DPI Report
- Recommendation Report
- Summary Report
- Suspicious Application Activity Report
- System Event Report

Generating Reports

Reports allow you to generate reports in PDF or RTF formats. You can select the type of report and filter the information to include by tags, time period, security profile, and domain or computer. You can choose to password protect the reports.

To generate a report:

PATH: IDF MAIN MENU | REPORTS

1. In the "Reports" area, select the type of report to generate and a format. The reports can be output to PDF or RTF format.
2. In the "Tag Filter" area, define any tags for the report.

   When you select a report which contains event data, you have the option to filter the report data using Event Tags. Select **All** for only tagged events, **Untagged** for only untagged events, or select **Tag(s)** and specify one or more tags to include only those events with your selected tag(s).
3. In the "Time Filter" area, you can set the time filter for any period for which records exist. This is useful for security audits.

Note: Reports use data stored in counters. Counters are data aggregated periodically from Events. Counter data is aggregated on an hourly basis for the most recent three days. Data older than three days is stored in counters that are aggregated on a daily basis. For this reason, the time period covered by reports for the last three days can be specified at an hourly level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.

4. In the "Computer Filter" area, set the computers whose data will be included in the report.
5. In the "Encryption" area, you can set password protection.

Note: If your reporting requirements are not met by the original reports included with IDF Server Plug-in, it may be possible to have custom reports designed for you. Please contact your support provider for more information.

Chapter 6

Managing Computers

This chapter describes how to manage Trend Micro™ Intrusion Defense Firewall™ Computers and the IDF Client Plug-in.

Topics in this chapter:

About Computers

Intrusion Defense Firewall enables you to monitor the computers in your network, manage the Client Plug-in on each computer, perform port scans and Recommendation Scans, assign Security Profiles, and view Events for a computer.

Viewing Computer Information

The Computers screen allows you to manage and monitor the computers on your network, displaying the managed computers along with information about each computer such as the platform, security profile, status, and last successful update.

To open the Computers screen, click **Computers** in the IDF main menu.

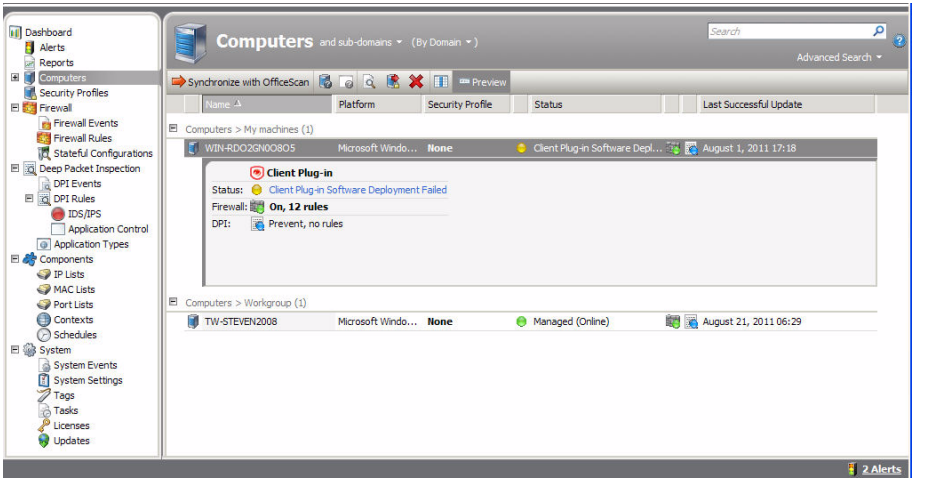


FIGURE 6-1. Computers Screen

This screen updates itself periodically. To add or remove information columns, click the **Add/Remove Columns** button in the toolbar, and select the columns to include from the **Add/Remove Columns** popup window.

Viewing a Computer Preview

Preview expands a display area beneath a listed computer. The preview pane displays the presence of a Client Plug-in, its status, and details about the Firewall and DPI modules.

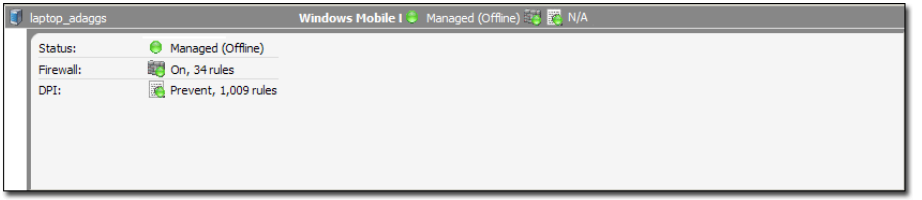


FIGURE 6-2. Computer Preview Pane

To view a computer preview:

PATH: IDF MAIN MENU | COMPUTERS

1. Click **Preview** in the toolbar.
2. Select the computer to preview. The Preview option remains enabled until you click the **Preview** button again.

Checking the Status of a Computer

This command simply checks the status of a Computer without performing a scan or activation attempt. For detailed information on computer status, see *Computer and Client Plug-in Status* on page B-1.

To check the status:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers for which to check the status.
2. Right-click to display the popup menu and select **Actions > Check Status**.

Searching for a Computer

Use the Search textbox to search for a particular Computer among listed Computers. For more sophisticated search options, use the "Advanced Search" option below it.

Advanced Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string
- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

Synchronizing the Computer List with OfficeScan

The IDF computer list is synchronized automatically with OfficeScan every time you start the Server Plug-in, but it will not be updated if Computers are added to OfficeScan while the Server Plug-in is running. Use **Synchronize with OfficeScan** button on the toolbar to force a synchronization with OfficeScan while the Server Plug-in is running.

Note: When the OfficeScan Client is installed on a Computer, the OfficeScan Server assigns it a unique identification number. It is this unique identification number that OfficeScan and Intrusion Defense Firewall use to keep track of individual Computers. If the OfficeScan Client is uninstalled from a Computer and then reinstalled (with the Intrusion Defense Firewall Client Plug-in), OfficeScan will assign the Computer a new Unique ID. The next time you synchronize with OfficeScan to update the list of Computers, Intrusion Defense Firewall will see the new unique identification number and treat the Computer as a new entry. Because the Computer's hostname will not have changed, the new listing for the Computer will append "_1" (or "_2", or "_3", and so on) to the end of the hostname. You will now have the same Computer listed twice: once as "hostname" and again as "hostname_1". You should delete the first listing ("hostname") and keep the second ("hostname_1"). (You can rename "hostname_1" back to "hostname" after deleting the original listing.)

Scanning Computers for Open Ports

A port scan performs a scan on all selected computers and checks the Client Plug-in installed on the computer to determine whether its state is either "Client Plug-in Deactivate Required", "Client Plug-in Activate Required", "Client Plug-in Reactivate Required", or "Online". (The scan operation, by default, scans ports 1-1024. This range can be changed in the **System > System Settings** section under the **Scan** tab.)

For information on how configure the ports to scan, see *Configuring Port Scan Settings* on page 10-5.

Note: Port 4118 is always scanned regardless of port range settings. It is the port on the computer to which Server Plug-in initiated communications are sent. If communication direction is set to "Client Plug-in Initiated" for a computer (**Computer Details > System > Settings > Computer > Communication Direction**), port 4118 is closed.

To scan for open ports from the computer list:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers to scan.
2. Click **Scan for Open Ports** in the toolbar, or right-click and select **Actions > Scan for Open Ports** from the popup menu.

To scan for open ports from the computer Firewall screen:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computer.
2. Right-click and select **Details...** from the popup menu.
3. In the navigation pane, click **Firewall**.
4. Click the **Scan for Open Ports** button.

Another way to initiate port scans is to create a Scheduled Task to regularly carry out port scans on a list of computers.

Canceling Any Currently Executing Port Scans

If you have initiated a set of port scans to a large number of Computers and/or over a large range of ports and the scan is taking too long, use this option to cancel the scans.

To cancel a scan:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers for which to cancel a scan.
2. Right-click to display the popup menu and select **Actions > Cancel Scan(s) for Open Ports** or **Cancel Scan(s) for Recommendations**.

Scanning Computers for Recommendations

Scan for Recommendations causes the IDF Server Plug-in to scan the Computer and then make recommendations for Security Rules based on what is detected. The results of a recommendation scan can be seen in the Computer's Details window on the various Rules screens. See *Viewing and Editing Computer Details* on page 6-21 for more information.

When you instruct IDF to run a Recommendation Scan on a computer, the IDF Client Plug-in scans the computer's registry, running processes, open ports, file system, and services for known vulnerabilities. The Client Plug-in scans not only the operating system but also installed applications. Based on what is detected, IDF will recommend DPI Rules.

Note: For large deployments, Trend Micro recommends managing Recommendations at the Security Profile level. That is, all computers that are to be scanned should already have a Security Profile assigned to them. This way, you can make all your rule assignments from a single source (The Security Profile) rather than having to manage individual rules on individual computers.

Recommendation Scans can be initiated manually or you can create a Scheduled Task to periodically run scans on certain computers.

To scan for recommendations manually:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers to scan.
2. Click **Scan for Recommendations** in the toolbar, or right-click and select **Actions > Scan for Recommendations** from the popup menu.

To create a Recommendation Scan Scheduled Task:

PATH: IDF MAIN MENU | SYSTEM > TASKS

1. Click **New** on the toolbar and select **New Scheduled Task** to display the **New Scheduled Task** wizard.
2. Select **Scan Computers for Recommendations** from the **Type** menu and select how often you want the scan to occur. Click **Next**.
3. The next screen will let you be more specific about the scan frequency, depending on your choice. Make your selection and click **Next**.
4. Now select which computer(s) will be scanned and click **Next**.

> **Note:** As usual, for large deployments it's best to perform all actions through Security Profiles.

5. Finally, give a name to your new Scheduled Task, select whether or not to "Run Task on Finish", click **Finish**.

Managing Recommendation Scan Results

Once a Recommendation Scan is complete, open the Security Profile that is assigned to the computers you have just scanned. Navigate to **Deep Packet Inspection > DPI Rules**. Sort the rules **"**By Application Type**"**, and select **"**Show Recommended for Assignment" from the display filter menu:

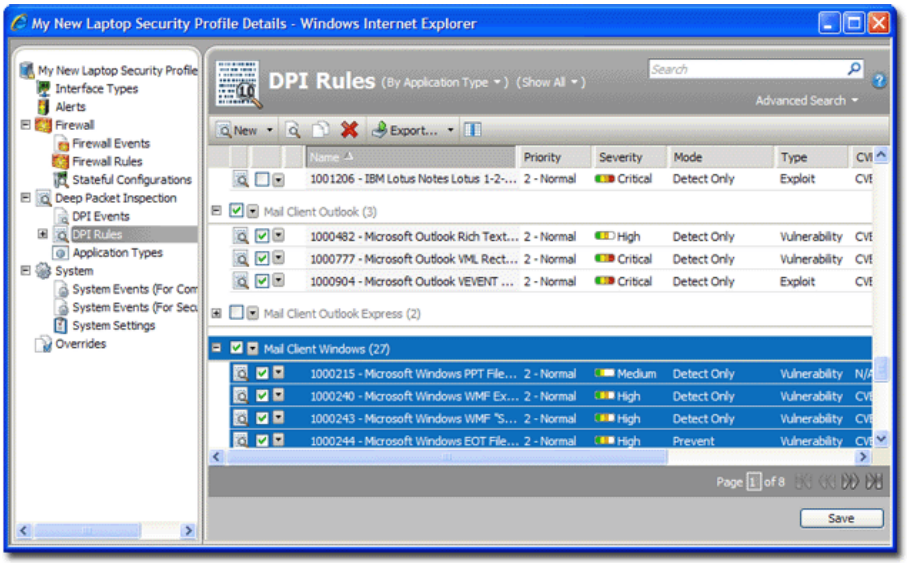


FIGURE 6-3. Recommendation Scan Results

All the recommendations made for all the computers included in the Security Profile will be listed.

Note: There are two kinds of green flags. Full flags ( ) and partial flags( ). Recommended Rules always have a full flag. Application Types may have a full or partial flag. If the flag is full, it signifies that all the Rules that are part of this Application Type have been recommended for assignment. If the flag is partial, it signifies that only some of the Rules that are part of this Application Type have been recommended.

Also notice the tool tip in the screen shot above. It reads: "This DPI Rule is recommended on 3 of 21 computer(s) to which the security profile is assigned." Trend Micro recommends assigning all the recommended Rules to all the computers covered by the Security Profile. This may mean that some Rules are assigned to computers on which they are not required. However, the minimal effect on performance is outweighed by the ease of management that results from working through Security Profiles.

Remember that a Recommendation Scan will make recommendations for DPI Rules.

Once a Recommendation Scan has run, Alerts will be raised on the all computers for which recommendations have been made.

Note: The results of a recommendation scan can also include recommendation to unassign rules. This can occur if applications are uninstalled, if security patches from a manufacturer are applied, or if unnecessary rules have been applied manually. To view rules that are recommended for unassignment, select "Show Recommended for Unassignment" from the display filter menu.

Configuring Recommended Rules

Some Rules require configuration before they can be applied. For example, one DPI Rule requires that you set minimum and maximum thresholds for the number of emails expected to arrive in a day. If this is the case, an Alert will be raised on the computer on which the recommendation has been made. The text of the Alert will contain the information required to configure the rule.

Clearing Recommendations

Clear Rule recommendations resulting from a Recommendation Scan on this Computer. This will also remove the Computer from those listed in an Alert produced as a result of a Recommendation Scan.

Note: This action will not un-assign any rules that were assigned because of past recommendations.

To clear recommendations:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers for which to clear recommendations.
2. Right-click to display the popup menu and select **Actions > Clear Recommendations**.

Assigning Security Profiles

You can assign security profiles to one or more computers, or assign a profile to the current domain. For more on Security Profiles, see *Security Profiles* starting on page 7-1.

Assigning a Security Profile to a Computer

You can assign a Security Profile to one or more computers. The name of the Security Profile assigned to the computer will appear in the Security Profile column in the Computers List.

Note: If you apply other settings to a computer (for example, adding additional Firewall Rules, or modifying stateful configuration settings), the name of the Security Profile will be in bold indicating that the default settings have been changed.

To assign a Security Profile to one or more computers:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers to be assigned a profile.
2. Click **Assign Security Profile...** in the toolbar, or right-click and select **Actions > Assign Security Profile...** from the popup menu.
3. In the **Assign Security Profile** window, select the Security Profile to assign, and click **OK**.

Assigning a Security Profile to the Current Domain

Assigning a Security Profile to a Domain has the effect of assigning that profile to every computer in that Domain. Keep in mind that Security Profiles are tied to computers at the Computer level, and not at the Domain level. Assigning a Security Profile to a Domain will assign that Security Profile to all computers in that Domain, but any computers added subsequently to the Domain will not automatically have that Security Profile assigned to them.

Managing Client Plug-ins

The Client Plug-in is installed on all client computers in the network, allowing the Server Plug-in to communicate and manage security on the client computer.

Configuring Plug-in Communications

At the default setting (Bi-directional), the Client Plug-in will initiate the heartbeat but will still listen on the Client Plug-in port for Server Plug-in connections and the Server Plug-in is free to contact the Client Plug-in in order to perform operations as required. Server Plug-in Initiated means that the Server Plug-in will initiate all communications. Communication will occur when the Server Plug-in performs scheduled updates, performs heartbeat operations (below), and when you choose the Activate/Reactivate or Update Now options from the Server Plug-in interface. If you are isolating the computer from communications initiated by remote sources, you can choose to have the Client Plug-in itself periodically check for updates and control heartbeat operations. If this is the case, select Client Plug-in Initiated.

Note: The following information is collected by the Server Plug-in during a heartbeat: the status of the drivers (on- or off-line), the status of the Client Plug-in (including clock time), Client Plug-in logs since the last heartbeat, data to update counters, and a fingerprint of the Client Plug-in security configuration (used to determine if it is up to date). You can change how often heartbeats occur (whether Client Plug-in or Server Plug-in initiated), and how many missed heartbeats can elapse before an alert is triggered.

This setting (like many other settings) can be configured at three levels: on all computers by setting a system-wide default, only on computers to which a particular Security Profile has been assigned, and on individual computers.

On the system as a whole:

1. Go to the Server Plug-in's **System > System Settings** screen and click the **Computers** tab.
2. Select "Server Plug-in Initiated", "Client Plug-in Initiated", or "Bi-Directional" from the drop-down list in the Communication Direction panel.

Only on computers to which a particular Security Profile has been assigned:

1. Open the **Security Profiles Properties** screen of the Security Profile whose communications settings you want to configure.
2. Go to **System > System Settings** and go to the **Computer** tab.
3. In the "Direction of IDF Server Plug-in to Client Plug-in communication:" drop-down menu, select one of the three options ("Server Plug-in Initiated", "Client Plug-in Initiated", or "Bi-directional"), or choose "Inherited". If you select "Inherited", the Security Profile will inherit the setting that was specified in the Server Plug-in's **System > System Settings** screen. Selecting one of the other options will override the global selection.
4. Click **Save** to apply the changes.

Only on a specific computer:

1. Open the **Details** screen of the computer whose communications settings you want to configure.
2. Go to **System > System Settings** and go to the **Computer** tab.
3. In the "Direction of IDF Server Plug-in to Client Plug-in communication:" drop-down menu, select one of the three options ("Server Plug-in Initiated", "Client Plug-in Initiated", or "Bi-directional"), or choose "Inherited". If you select "Inherited", the computer will inherit the setting that was specified on its Security Profile's Details window or in the Server Plug-in's System > System Settings screen. Selecting one of the other options will override the Security Profile and/or the global selection.
4. Click **Save** to apply the changes.

Note: Client Plug-ins look for the IDF Server Plug-in on the network by the Server Plug-in's hostname. Therefore the Server Plug-in's hostname must be in your local DNS for Client Plug-in initiated or bi-directional communication to work.

Deploying the Client Plug-in

The Client Plug-in can generally be installed and managed using the Server Plug-in interface. However, in some cases, actions must be performed on the client computer itself.

Deploying the Client Plug-in from the Server

When you install a Client Plug-in on an OfficeScan client, the Client Plug-in will activate automatically.

Note: The Client Plug-in will install to `<PROGRAM FILES>Trend Micro\IDF Client` (This is the default location and cannot be changed.)

To deploy the Client Plug-in:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers on which to deploy the Client Plug-in.
2. Right-click to display the popup menu and select **Actions > Deploy Client Plug-in(s)**.

Using the Standalone Client Plug-in Installer

The IDF Stand-alone Client Plug-in Installer package is a self-extracting .msi file which is run on the client computer and is available from Trend Micro Support upon request. The client computer must already have the OSCE client installed on it. The Client Plug-in will perform automatic agent-initiated activation after installation but Client Plug-in Initiated Activation must be enabled from the IDF Server Plug-in console for automatic activation to work. (**System > System Settings > Computers**)

The standalone installer uses the OSCE Client to perform the installation of the IDF Client Plug-in, and assumes that the OSCE Client is already installed in the default location:

`C:\Program Files\Trend Micro\OfficeScan Client.`

To use the Standalone Client Plug-in Installer:

1. If you do not need logging: For the 32-bit platform, double-click `IdfClient-1.5.0.xxxx-en.i386.msi`. For the 64-bit platform, double-click `IdfClient-1.5.0.xxxx-en.x86_64.msi`. (`xxxx` is the internal build number.)
2. If you need logging, do the following instead of step 1 above:
   a. Open a command window.
   b. Navigate to the folder containing the standalone msi.
   c. Run the following command:

      ```
      msiexec /i IdfClient-1.5.0.xxxx-en.i386.msi /l*v
      idf_standalone.log
      ```

      The log file is named idf_standalone.log.
3. Verify the client is listed on the **Computers** screen and that its status is "Managed".

Note: Because the standalone installer will briefly interrupt the client's network connection, the installer must be run locally on the host computer.

Activating/Reactivating the Client Plug-in

When a Computer is unmanaged the Client Plug-in must be activated to move the Computer into a managed state. Prior to activation the Client Plug-in will be one of the following states:

- **No Client Plug-in**: Indicates there is no Client Plug-in running or listening on the default port. The "No Client Plug-in" status can also mean that a Client Plug-in is installed and running but is working with another Server Plug-in and communications are configured as "Client Plug-in Initiated", and so the Client Plug-in is not listening for this Server Plug-in. (If you wish to correct the latter situation, you will have to deactivate the Client Plug-in from the Computer).

- **Client Plug-in Installed**: The Client Plug-in is installed and listening, and is ready to be activated by the Server Plug-in.
- **Client Plug-in Activate Required**: The Client Plug-in is installed and listening and is waiting to be activated by the Server Plug-in.
- **Client Plug-in Reactivate Required**: The Client Plug-in is installed and listening and is waiting to be activated by the Server Plug-in.
- **Client Plug-in Deactivate Required**: The Client Plug-in is installed and listening, but has already been activated by another Server Plug-in. To be activated by this Server Plug-in, the Client Plug-in must be deactivated locally on the Computer.

After a successful activation the Client Plug-in state will change to "Managed". If the activation failed the Computer status will display "Client Plug-in Activation Failed" with the reason for the failure in brackets. Click this link to display the system event for more details on the reason for the activation failure.

To activate the Client Plug-in:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers on which to activate the Client Plug-in.
2. Right-click to display the popup menu and select **Actions > Activate/Reactivate**.

Stopping and Starting the Client Plug-in

Stopping or starting the Client Plug-in can only be done locally on the computer.

To start or stop the Client Plug-in:

- Stop: from the command line, run the following: sc stop ds_agent
- Start: from the command line, run the following: sc start ds_agent

Updating the Client Plug-in on a Computer

Updating the Client Plug-in on a Computer deploys any configuration changes you have made for that computer from the Server Plug-in to the Client Plug-in. Updates occur automatically at every heartbeat, but if you wish to apply your changes immediately, you can use this option. The **Update Now** button can be used to override the Computer access schedule or to force the Server Plug-in to retry an update if the previous attempt failed.

Note: The automatic updates actually occur immediately if the communications are not Client Plug-in initiated, and they occur on the next heartbeat if Client Plug-in initiated.

To update the Client Plug-in:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers on which to deactivate the Client Plug-in.
2. Right-click to display the popup menu and select **Actions > Update Now**.

Manually Upgrading the Client Plug-in

The occasion may arise where you are not able to upgrade the Client Plug-in software on a computer from the Server Plug-in interface because of connectivity restrictions between the Server Plug-in computer and the Client Plug-in computer. In such cases, upgrading the Client Plug-in software on a computer has to be performed manually.

The new Client Plug-in software has to be downloaded manually from the Trend Micro Download Center.

To manually upgrade the Client Plug-in, copy the Client Plug-in installer to the computer and run it. It will detect the previous Client Plug-in and perform the upgrade.

Deactivating the Client Plug-in on a Computer

Deactivating a Client Plug-in is not the same as uninstalling the Client Plug-in. Deactivation simply removes all rules, filters, etc. from the Client Plug-in and unbinds it from the exclusive control of the Server Plug-in. (Once a Server Plug-in activates a Client Plug-in, no other installation of an Intrusion Defense Firewall system can communicate with the Client Plug-in. Once deactivated, the Client Plug-in can then be re-activated by any Intrusion Defense Firewall Server, which will then have exclusive control over it.) Manual deactivation is required if the Server Plug-in can no longer communicate with the Client Plug-in.

You may want to transfer control of a Computer/Client Plug-in from one IDF Server Plug-in installation to another. If so, the Client Plug-in has to be deactivated and then activated again by the new Server Plug-in. Deactivating the Client Plug-in can be done

locally on the Computer through the Client Plug-in UI or from the Server Plug-in currently managing the Client Plug-in. (A computer does not have to be reachable in order to be deactivated. If an unreachable deactivated Computer becomes reachable again, it will simply appear as a "New (Unknown)" Computer in the Computers List.)

To deactivate the Client Plug-in from the Server Plug-in:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers on which to deactivate the Client Plug-in.
2. Right-click to display the popup menu and select **Actions > Deactivate**.

To manually deactivate the Client Plug-in:

1. On the client machine, open a command prompt window (**Start > Run > cmd.exe**).
2. Go to the Client Plug-in install directory:
   ```
   cd c:\Program Files\Trend Micro\IDF Client
   ```
3. Instruct the Client Plug-in to deactivate:
   ```
   dsa_control /r /c ds_agent.crt
   ```

The Client Plug-in is now ready to be activated by another (or the same) Intrusion Defense Firewall Server.

Note: The Computer is now no longer being protected by the Intrusion Defense Firewall filters and rules.

Uninstalling the Client Plug-in

The Client Plug-in can generally be uninstalled from the Server Plug-in interface; however, in some cases, the Client Plug-in may have to be uninstalled manually from the the client computer.

Note: The IDF Client Plug-in cannot be uninstalled using the Control Panel Add or Remove Programs applet.

To remove the Client Plug-in from the Server:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers from which to remove the Client Plug-in.
2. Right-click to display the popup menu and select **Actions > Remove Client Plug-in(s)**.

To manually uninstall a Client Plug-in:

1. On the client machine, open a command prompt window (**Start > Run > cmd.exe**).
2. For 32-bit Windows, type the following and press **Enter**:
   ```
   rundll32 "C:\Program Files\Trend Micro\IDF
   Client\IdfClientAgent.dll",Uninstall
   ```
3. For 64-bit Windows, type the following and press **Enter**:
   ```
   rundll32 "C:\Program Files (x86)\Trend Micro\IDF
   Client\IdfClientAgent.dll",Uninstall
   ```

Viewing Events for a Computer

You can examine system and administrative events (that is, non security-related events) associated with a particular computer, or examine the latest Firewall Events uploaded from the Client Plug-in on this computer. You can override the normal event retrieval schedule (usually every heartbeat) and retrieve the Event logs from the computers now. For detailed information on computer events, see *Client Plug-in Events* on page C-24.

To view system events for a computer:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computer for which to view system events.
2. Right-click to display the popup menu and select **View > View System Events...**.
3. A new window opens, displaying the system events for the selected computer. For information about system events, see *System Events* on page C-8.

To view firewall events for a computer:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computer for which to view firewall events.
2. Right-click to display the popup menu and select **View > View Firewall Events...**
3. A new window opens, displaying the firewall events for the selected computer. For information about system events, see *Firewall Events* on page C-2.

To get events from the Client Plug-in now:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers from which to get events.
2. Right-click to display the popup menu and select **Actions > Get Events Now**.

Clearing Warnings/Errors

If a Client Plug-in has been reset locally, or has simply been removed from the network before being deactivated or before the computer has been deleted from the Computers List, you can clear any warnings or errors generated for the computer.

To clear warnings and errors:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers for which to clear warnings and errors.
2. Right-click to display the popup menu and select **Actions > Clear Warnings/Errors**.

Locking and Unlocking a Computer

You can lock a computer if you are going to perform some maintenance on it and don't want to trigger a series of alerts on the Server Plug-in.

Note: The computer's status will be displayed as "locked" while in this state and the Server Plug-in will not communicate with the Client Plug-in or trigger any Computer/Client Plug-in related alerts. Existing Computer alerts are not affected. If a Computer update is in progress it will be allowed to complete normally. Note that the Client Plug-in is not told that the Computer is in a locked state. If communication between the Client Plug-in and the Server Plug-in has been set to "Client Plug-in Initiated" or "Bi-directional", it may generate an event which it will report when it finally contacts the Server Plug-in again.

To lock a computer:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers to lock.
2. Right-click to display the popup menu and select **Actions > Lock**.

To unlock a computer:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers to unlock.
2. Right-click to display the popup menu and select **Actions > Unlock**.

Assigning Computer Asset Value

A Computer Asset Value is a (customizable) rating system used to assign value to Computers. Each grade in the rating system has a value between 1 and 100. This value gets multiplied by the severity value of a rule to allow you to rank Firewall and DPI Rule Events. To configure Ranking, go to **System > System Settings > Ranking**.

To assign computer asset value:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computers to assign an asset value.
2. Right-click to display the popup menu and select **Actions > Assign Asset Value...**
3. In the **Assign Asset Value** window, select an asset value and click **OK**.

Viewing and Editing Computer Details

The computer's Details window mirrors the main interface of the IDF Server Plug-in. It includes all the settings and configurations that can be changed to override any higher level settings and configurations.

To open the Computer Details window:

PATH: IDF MAIN MENU | COMPUTERS

1. Select the computer for which to view or edit details and click Details in the toolbar, or right-click to display the popup menu and select **View > Details...**
2. A new window opens, displaying the a navigation bar to access details for the selected computer.

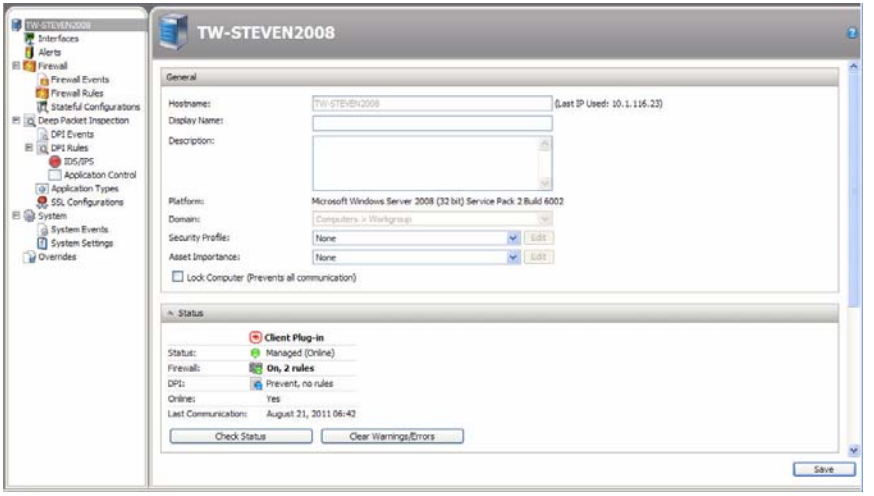


FIGURE 6-4. Computer Details Window

Computer Information

The Computer Information screen of the Computer Details window allows you to edit information about the selected computer, such as the host name and domain, and view information, such as Client Plug-in status.

To view or edit computer information:

PATH: IDF MAIN MENU | COMPUTERS > DETAILS

1. Select a computer and click **Details** in the toolbar, or right-click to display the popup menu and select **Details...**
2. In the "General" area, edit any of the following options:
   - **Hostname**: Appears in the Name column on the Computers screen. The name must be either the IP address of the computer or the hostname of the computer. (Either a fully qualified hostname or a relative hostname may be used if a hostname is used instead of an IP address.)
   - **Description**: a description of the computer.
   - **Platform**: Details of the computer's OS will appear here.
   - **Domain**: The computer domain to which the computer belongs appears in the drop-down list. You can reassign the computer to any other existing computer domain.
   - **Security Profile**: The Security Profile (if any) that has been assigned to this computer.

     Note: Keep in mind that if you unassign a Security Profile from a computer, Rules may still be in effect on the computer if they were assigned independently of the Security Profile.

   - **Asset Importance**: IDF Server Plug-in uses a ranking system to quantify the importance of Security Events. Rules are assigned a Severity Level (high, medium, low, etc.), and Assets (computers) are assigned an "Asset Importance" level. These levels have numerical values. When a Rule is triggered on a computer the Asset Importance value and the Severity Level value are multiplied together. This produces a score which is used to sort Events by importance. (Event ranking can be seen in the Events screens.) Use this Asset Importance drop-down list to assign an Asset Importance level to this computer. (To edit the numerical values associated with severity and importance levels, go to **System > System Settings > Ranking**.)

- **Lock Computer (Prevents all communication)**: Setting this option blocks all communications between the Client Plug-in and the Server Plug-in. The computer's Security Profile is still active (all rules are still applied to all traffic), but should any alerts be generated, they will not be sent to the Server Plug-in.

Note: You may wish to lock out a computer if you are going to perform some maintenance on it and don't want a series of alerts to appear in the Server Plug-in.

---

3. In the "Status" area, the following Status information and options are available:
   - **Status**: Shows the current computer status as follows:
     - When the computer is unmanaged the status will display "Unmanaged" followed by the Client Plug-in state in brackets ("No Client Plug-in", "Unknown", "Reactivation Required", "Activation Required", or "Deactivation Required").
     - When the computer is managed and no computer errors are present, the status will display "Managed" followed by the state of the Client Plug-in in brackets ("Online" or "Offline").
     - When the computer is managed and the Client Plug-in is in the process of performing an action (e.g., "Upgrading Client Plug-in (Install Program Sent)", etc.) the task status will be displayed.
     - When there are errors on the computer (e.g., "Offline", "Update Failed", etc.) the status will display the error. When more than one error is present, the status will display "Multiple Errors" and each error will be listed beneath.
   - **Firewall**: Whether the Firewall is on or off and how many rules are in effect.
   - **DPI**: Whether DPI is on or off and how many rules are in effect.
   - **Online**: Indicates whether the Server Plug-in can currently communicate with the Client Plug-in.
   - **Last Communication**: The last time the Server Plug-in successfully communicated with the Client Plug-in on this computer.

- **Check Status**: This button allows you to force the Server Plug-in to perform an immediate heartbeat operation to check the status of the Client Plug-in. Check Status will not perform an update of the Client Plug-in. (If an update is required click the Update Now button on the Actions tab.) When Server Plug-in to Client Plug-in Communications is set to "Client Plug-in Initiated" the Check Status button is disabled. (Checking status will not update the logs for this computer. To update the logs for this computer, go to the Actions tab.)
- **Clear Warnings/Errors**: Dismisses any alerts or errors on this computer.

4. In the "Activation" area, the following information and options are available:

   A newly installed IDF Client Plug-in needs to be "activated" by the IDF Server Plug-in before Security Profiles, Rules, requests for Event logs, etc. can be sent to it. The activation procedure includes the exchange of SSL keys which uniquely identify a Server Plug-in (or one of its nodes) and a Client Plug-in to each other. Once activated by an IDF Server Plug-in, a Client Plug-in will only accept instructions or communicate with the IDF Server Plug-in which activated it (or one of its nodes).

   An unactivated Client Plug-in can be activated by any IDF Server Plug-in.

   Client Plug-ins can only be deactivated locally on the computer or from the IDF Server Plug-in which activated it. If a Client Plug-in is already activated, the button in this area will read "Reactivate" rather than "Activate". Reactivation has the same effect as Activation. A reactivation will reset the Client Plug-in to the state it was in after first being installed and initiate the exchange of a new set of SSL keys.

5. In the "Update" area, the following information and options are available:

   When you change the configuration of a Client Plug-in on a computer using the IDF Server Plug-in (Apply a new DPI Rule, change logging settings, etc.) the IDF Server Plug-in has to send the new information to the Client Plug-in. This is an update. Updates usually happen immediately but you can force an update by clicking the Update Now button.

6. In the "Software" area, the following information and options are available:

   This displays the version of the Client Plug-in currently running on the computer. If a newer version of the Client Plug-in is available for the computer's platform you can click the Upgrade Client Plug-in... button to remotely upgrade the Client Plug-in from the IDF Server Plug-in. You can configure the IDF Server Plug-in to trigger an alert if new Client Plug-in versions for any of your computers by going to System > Updates in the main IDF Server Plug-in window.

7. In the "Support" area, you can create a Diagnostics Package:

The **Create Diagnostic Package...** button creates a snapshot of the state of the Client Plug-in on the computer. Your support provider may request this for troubleshooting purposes.

If you have lost communication with the computer, a diagnostics package can be created locally.

To create a diagnostics package locally on a Windows computer:

a. From a command line, type:

```
C:\Program Files\Trend Micro\IDF Client Plug-in>
dsa_control.exe /d
```

and press **Enter**.

b. A numbered zip file (for example, "341234567.zip") containing the diagnostics information will be created in the same directory.

8. To view or make any changes to interfaces, click **Interfaces** in the navigation pane.

The Interfaces screen displays the interfaces detected on the computer. If a Security Profile with multiple interface assignments has been assigned to this computer, interfaces that match the patterns defined in the Security Profile will be identified.

9. To view or make any changes to alerts, click **Alerts** in the navigation pane.

Alerts are displayed the same way as they are in the main IDF Server Plug-in window except that only alerts relating to this computer are displayed. When an Alert is dismissed here, it is also dismissed in the main IDF Server Plug-in window. For more information on Alerts, see *Alerts* starting on page 4-1.

10. To view or make any changes to the Firewall Settings, click **Firewall** in the navigation pane.

The Firewall for this computer inherits its on or off state either from its Security Profile or the global setting in the IDF Server Plug-in unless you choose to override it.

Note: If a Security Profile with Firewall turned off is applied to a computer and that computer is set to inherit firewall settings, all Firewall elements (Firewall Rules and Stateful Configurations) will be turned off on that computer, even elements that were assigned directly to the computer before the Security Profile was applied.

- **Events**: Firewall Events are displayed the same way as they are in the main IDF Server Plug-in window except that only events relating this computer are displayed.
- **Rules**: The Firewall Rules defined in the IDF Server Plug-in are displayed here. Select which ones will be active on this computer. If the computer has multiple interfaces, click the down-arrow and use the drop-down menu to select whether the Firewall Rule will apply to all interfaces or to specific interfaces only.

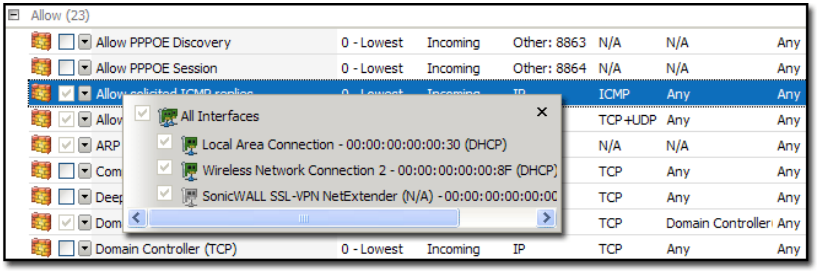


FIGURE 6-5. Rules

Note the checkmarks next to the active firewall rules. Grayed-out checkmarks indicate that the Firewall Rule is active on this computer because it has been applied by a Security Profile. (The same applies to any other type of rule.)

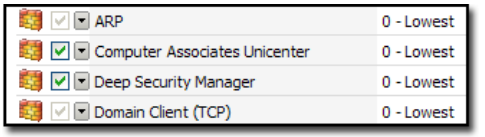


FIGURE 6-6. Rule Checkmarks

- **Stateful Configurations**: Select which Stateful Configuration to apply to this computer (if any). If the computer has multiple interfaces you can specify independent configurations for each interface.

11. Click **Deep Packet Inspection** in the navigation pane to view or make any changes.

    The DPI engine for this computer inherits its on or off state, its Inline behavior, and it Recommendation Scan behavior from the global setting in the IDF Server Plug-in or the Security Profile assigned to it unless you choose to override it.

- **Events**: DPI Events are displayed the same way as they are in the main IDF Server Plug-in window except that only events relating to this computer are displayed.
- **Rules**: The DPI Rules defined in the IDF Server Plug-in are displayed here. Select which ones will be active in this computer.
- **Application Types**: The Application Types defined in the IDF Server Plug-in are displayed here. Their properties can be edited globally or for this Security Profile only.
- **SSL Configurations**: IDF Server Plug-in supports DPI analysis of SSL traffic. The SSL Configurations screen allows you to create SSL Configurations for a given certificate-port pair on one or more interfaces. Certificates can be imported in P12 or PEM format and Windows computers have the option of using Windows CryptoAPI directly.

  To create a new SSL Configuration, click **New** and follow the steps in the **SSL Configuration** wizard.

  If the computer you are configuring is being installed on the computer hosting the IDF Server Plug-in, the wizard will provide let you use credentials already stored in the IDF Server Plug-in.

  Double-click an existing configuration to display its Properties window.

  Assignment:

  - **General Information**: The name and description of the SSL configuration, and whether it is enabled on this computer.
  - **Interface Assignments**: Which interfaces this configuration is being applied to.
  - **IP Assignment**: Which IP(s) this configuration applies to.
  - **Port Selection**: Which port(s) this configuration applies to.

  Credentials:

  The **Credentials** tab lists the current credentials, and has an **Assign New Credentials...** button which lets you change them.

Note: Filtering of SSL traffic is supported by the IDF Client Plug-in. The Client Plug-in does not support filtering SSL connections on which SSL compression is implemented.

---

12. To view or edit the System information, click **System**, **System Settings**, or **System Events** to open the System screens.
    - **System Events**: System Events are displayed the same way as they are in the main IDF Server Plug-in window except that only events relating to this computer are displayed.
    - **System Settings**: All System Settings from the IDF Server Plug-in that can be overridden on specific computers are displayed here.
13. Click **Overrides** to view or edit the elements have been overridden for the computer.

Inheritance and Overrides

Global settings can be overridden by settings at the Security Profile or computer level. For example, the Firewall can be turned off globally by going to the Firewall screen in the main IDF Server Plug-in window and setting "Firewall" to off.

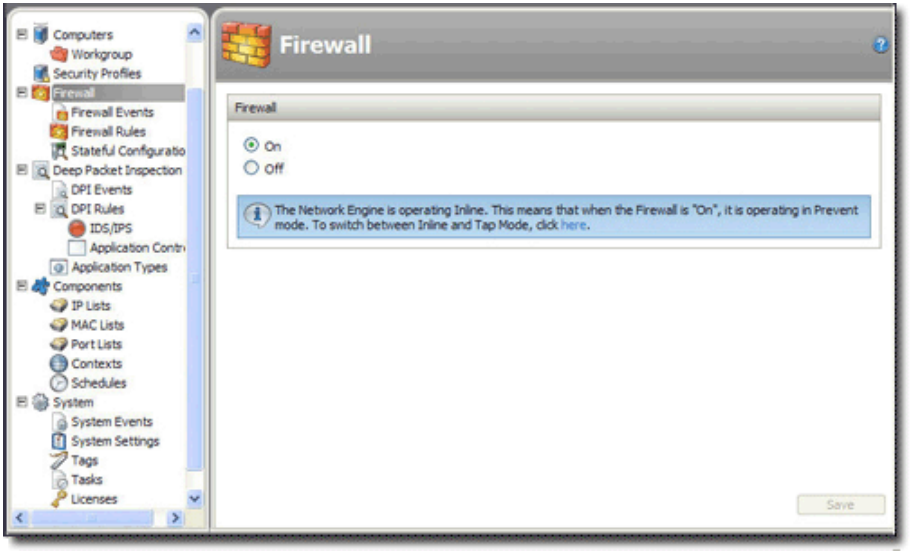


FIGURE 6-7. Firewall Settings

By default, lower levels in the hierarchy inherit their settings from the level above them. Therefore, if you turn off the Firewall at the Global level, it will be turned off in all Security Profiles and computers that are set to "Inherit".

FIGURE 6-8. Inheritance

Other Properties

Elements like Firewall Rules and DPI Rules can have some of their properties changed for specific computers. For example, let's say you have a Firewall Rule called FirewallRuleAlpha and among its properties is the fact that it operates on incoming port 12345 because the application you have designed the Firewall Rule for usually operates on that port.

But let's say you have one particular computer where that application operates on port 44444. Instead of writing a new Firewall Rule for this computer, we can simply open the computer's Details window, go to Firewall Rules, find the Firewall Rule in the list, right-click it and select "Properties (For This Computer)".

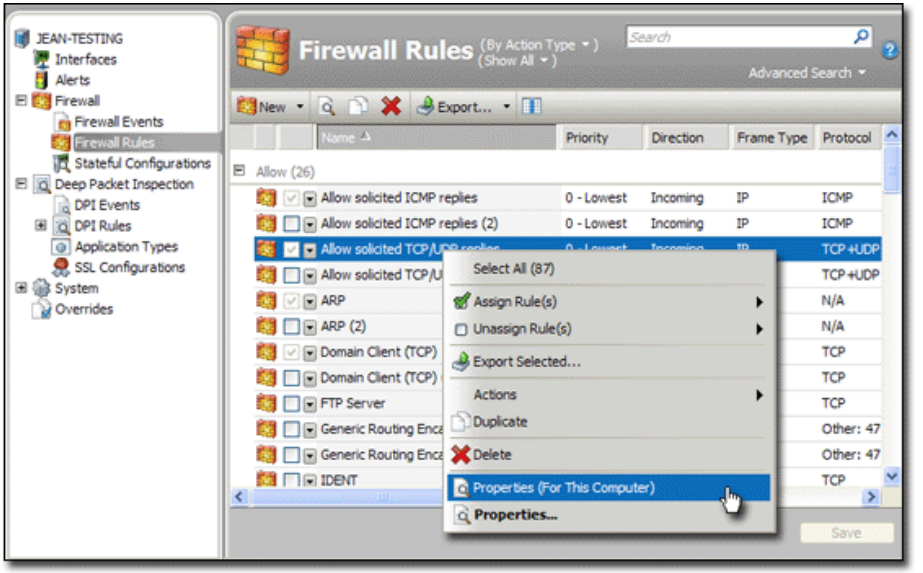


FIGURE 6-9. Properties (For This Computer)

In the Properties window for this Firewall Rule you will now see that many of the properties have a checkbox called "Inherit" next to them. This means that the setting is inherited from the level above it in the inheritance hierarchy (either from a Security Profile or the Global list). Clearing "Inherited" next to "Port:" and changing it to 44444 means that this Firewall Rule on this computer only will now operate on port 44444.

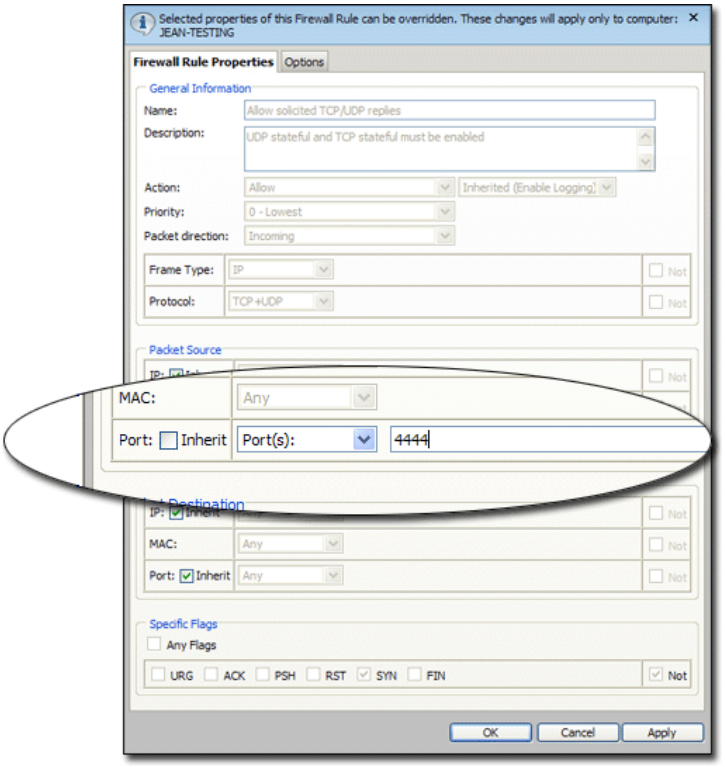


FIGURE 6-10. Inheriting Properties

This operation can also be performed at the Security Profile level if the Firewall Rule is part of a Security Profile. You would open the Security Profile's Details window and make the same changes. (You could then override those again on a particular computer.)

Viewing Computer or Security Profile Overrides

You can see what elements have been overridden on a Security Profile or a computer by opening the Details window and going to the Overrides screen.

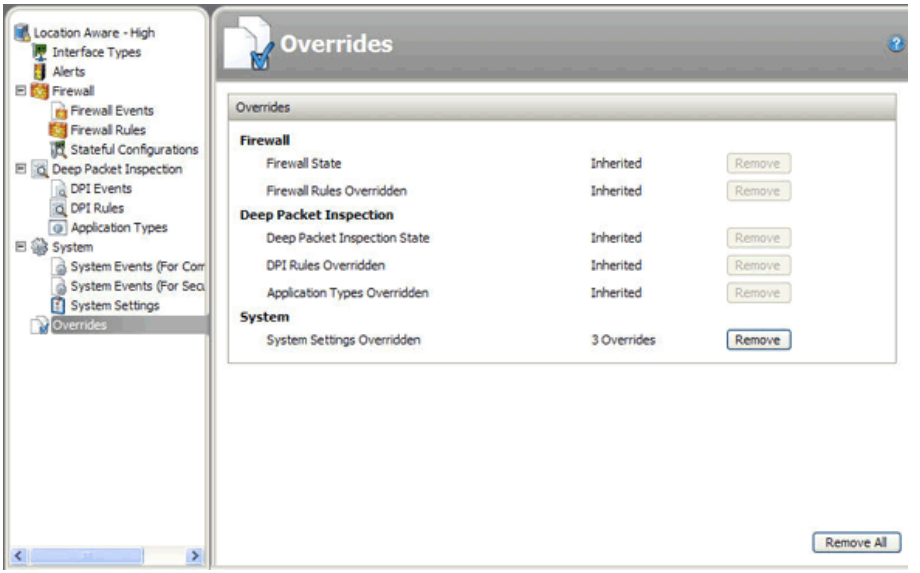


FIGURE 6-11. View Overrides

Chapter 7

Security Profiles

This chapter describes Trend Micro™ Intrusion Defense Firewall™ Security Profiles.

Topics in this chapter:

About Security Profiles

Security Profiles allow common configurations of Firewall Rules, Stateful Configurations, and DPI Rules (with interface assignments for each) to be saved for easy assignment to multiple computers.

Managing Security Profiles

To open the Security Profile screen, click Security Profiles in the IDF Main Menu. In the main Security Profiles screen, you will see a list of existing profiles. From here you can:

- Create New Security Profiles from scratch (New)
- Import Security Profiles from an XML file ()

Note: Do not import Security Profiles from a newer Security Update into a system running an older Security Update. The new Security Profile may reference rules that do not exist in the older version. Always make sure your Security Updates are current.

- Examine or modify the Properties of an existing Security Profile ()
- Duplicate (and then modify and rename) an existing Security Profile ()
- Delete a Security Profile ()
- Export a Security Profile to an XML file ()

Creating a Security Profile

Clicking New (New) opens the Security Profiles wizard which will prompt you for the name of the new profile and then give you the option of opening the Security Profile Details window. Clicking Details () displays the Security Profile Details window.

Note: You can create a new Security Profile based on a Recommendation Scan of a computer. To do so, select a computer and run a Recommendation Scan. (Right-click the computer on the Computers screen and select **Actions > Scan for Recommendations**). When the scan is complete, return to the Security Profiles screen and click **New** to display the New Security Profile wizard. When prompted, choose to base the new Security Profile on "an existing computer's current configuration". Then select "Recommended Application Types and DPI Rules" from among the computer's properties.

Note: The Security Profile will consist only of recommended elements on the computer, regardless of what Rules are currently assigned to that computer.

Viewing and Editing Security Profile Details

Whereas the main IDF Server Plug-in window serves to manage and organize the elements of the whole IDF system, the Security Profile Details window is used to select available elements from the IDF Server Plug-in and apply them to the particular Security Profile.

The Security Profile Details window is very similar to the main IDF Server Plug-in window except that all elements in the Security Profile Details screen apply specifically to the Security Profile. By default, all settings are inherited from the global settings of the main IDF Server Plug-in window. Changes can be made in the Security Profile window that will apply only to this Security Profile. When modifying the properties of an element in the main IDF Server Plug-in window (Firewall Rule, DPI Rule, etc.), the

only option is to modify the "Properties". When modifying the properties of an element in the Security Profile Details window, an additional option is available: "Properties (For This Security Profile)"

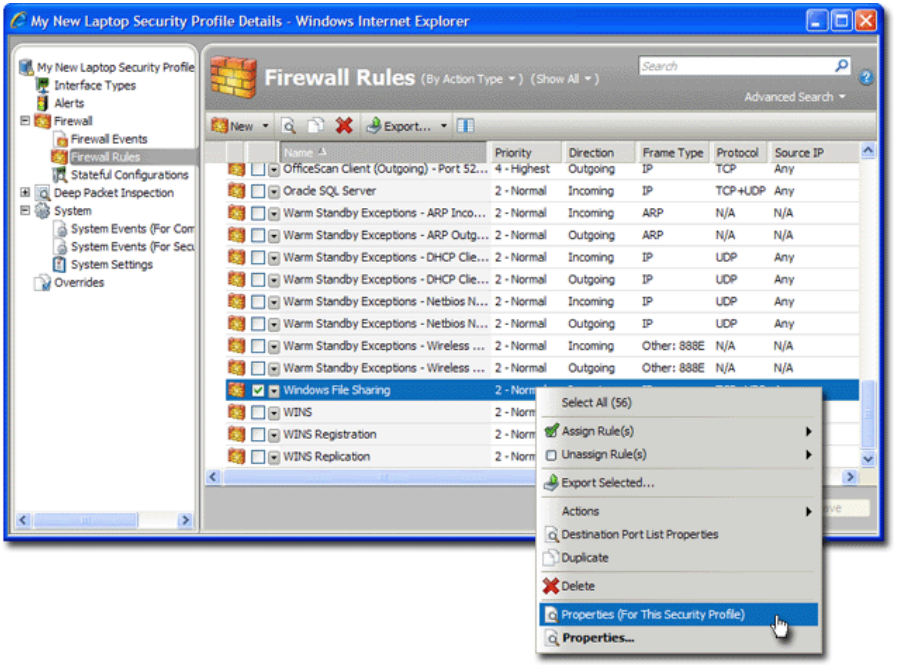


FIGURE 7-1. Security Profile Details

If you edit the "Properties (For this Security Profile)", the changes will only affect that element when it is applied to a computer by this Security Profile.

If you edit the "Properties", the changes will affect the element globally (except where it has been overridden elsewhere).

An element whose properties have been edited "For This Security Profile" will appear in bold letters in the Task Pane to indicate that it has special properties when applied to a computer as a part of this Security Profile.

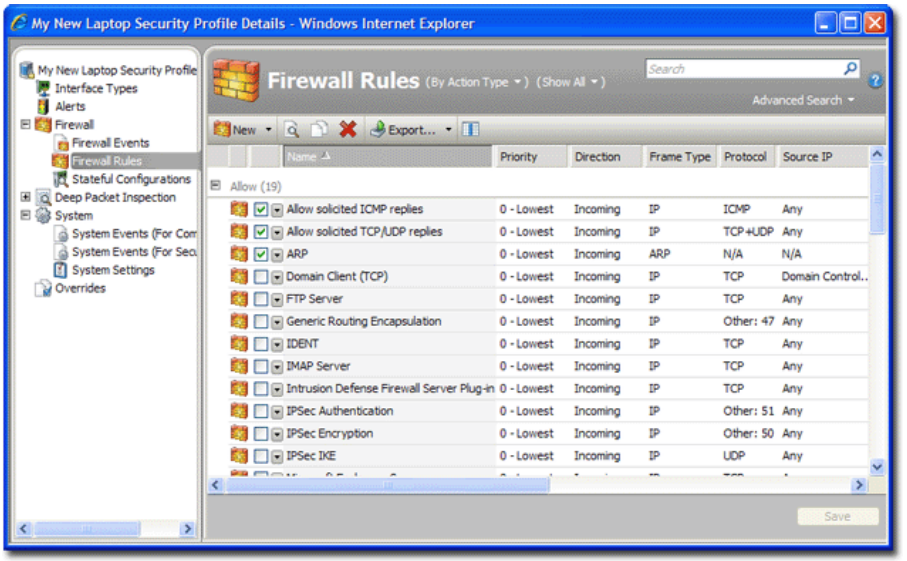


FIGURE 7-2. Properties (For This Security Profile)

To view or edit a Security Profile:

PATH: IDF MAIN MENU | SECURITY PROFILES

1. Select the profile to view or edit and click , or right-click on the profile and select **Details...**
2. In the Details window, navigate through the screens using the navigation pane and make any desired changes to the following:
   - **Interface Types**: If you have computers with more than one interface, you can assign various elements of a Security Profile (Firewall Rules, etc.) to each interface.

     To configure a Security Profile for multiple interfaces, select Multiple Interface Assignments and type names and pattern matching strings in the fields below.

The interface type name is used only for reference. Common names include "LAN", "WAN", "DMZ", and "Wi-Fi" though any name may be used to map to your network's topology.

The Matches defines a wildcard based interface name match to auto map the interfaces to the appropriate interface type. Examples would be "Local Area Connection *", "eth*", and "Wireless *". When an interface cannot be mapped automatically, an alert is triggered. You can manually map it from the Interfaces screen in the computer's Details window.

Note: If interfaces are detected on the computer which don't match any of these entries, the Server Plug-in will trigger an alert.

- **Alerts**: Alerts are displayed the same way as they are in the main IDF Server Plug-in window except that only alerts relating to computers using this Security Profile are displayed. When an Alert is dismissed here, it is also dismissed in the main IDF Server Plug-in window.
- **Firewall (Events, Rules, and Stateful Configurations)**: The Firewall for this Security Profile inherits its on or off state from the global setting in the IDF Server Plug-in unless you choose to override it.

Note: If a Security Profile with Firewall turned off is applied to a computer and that computer is set to inherit firewall settings, all Firewall elements (Firewall Rules and Stateful Configurations) will be turned off on that computer, even elements that were assigned directly to the computer before the Security Profile was applied.

- **Events**: Firewall Events are displayed the same way as they are in the main IDF Server Plug-in window except that only events relating to computers using this Security Profile are displayed.

- **Rules**: The Firewall Rules defined in the IDF Server Plug-in are displayed here. Select which ones will be active in this Security Profile. If you have defined multiple Interfaces for this Profile (above), use the gray drop-down menu to select whether the Firewall Rule will apply to all interfaces or to specific ones only.

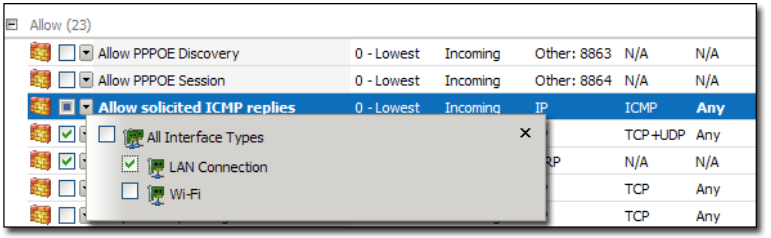


FIGURE 7-3. Properties (For This Security Profile)

- **Stateful Configurations**: Select which Stateful Configuration to apply to this Security Profile. If you have defined multiple Interfaces for this Profile (above), you can specify independent configurations for each interface.

- **Deep Packet Inspection (Events, Rules and Application Types)**: The DPI engine for this Security Profile inherits its on or off state, its Inline behavior, and it Recommendation Scan behavior from the Global or Security Profile setting unless you choose to override them.
  - **Events**: DPI Events are displayed the same way as they are in the main IDF Server Plug-in window except that only events relating to computers using this Security Profile are displayed.
  - **Rules**: The DPI Rules defined in the IDF Server Plug-in are displayed here. Select which ones will be active in this Security Profile. If you have defined multiple Interfaces for this Profile (above), use the gray drop-down menu to select whether the DPI Rule will apply to all interfaces or to specific ones only.
  - **Application Types**: The Application Types defined in the IDF Server Plug-in are displayed here. As with other elements at the Security Profile level, their properties can be edited globally or for this Security Profile only.

- **System**:
  - **Events (For Computers)**: System Events are displayed the same way as they are in the main IDF Server Plug-in window except that only events relating to computers using this Security Profile are displayed.
  - **Events (For Security Profile)**: System Events for this Security Profile (if it was created, modified, etc.) are displayed here.
  - **System Settings**: All System Settings from the IDF Server Plug-in that can be overridden on specific Security Profiles are displayed here.
- **Overrides**: Overrides shows the elements that have been overridden for the Security Profile.

3. Click **Save**.

Chapter 8

Using the IDF Firewall

This chapter describes Trend Micro™ Intrusion Defense Firewall™ Firewall.

Topics in this chapter:

About the IDF Firewall

The IDF Firewall protects clients and servers on the network. The IDF Server Plug-in interface provides screens for managing Firewall Events, Firewall Rules, and Stateful Configurations. By default, the IDF Server Plug-in collects Firewall and DPI Event logs from the IDF Client Plug-ins at every heartbeat. Firewall Rules examine the control information in packets, allowing you to either block or allow those packets based on rules. Stateful Configuration mechanism analyzes packets in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions.

Turning the Firewall On or Off

To turn the Firewall on or off:

PATH: PATH: IDF MAIN MENU | FIREWALL

1. In the "Firewall" area, choose **On** or **Off**.

   The information area will tell you whether the network engine is operating Inline or in Tap mode. When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that DPI Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.

2. To switch between Inline and Tap mode, go to **System > System Settings > Firewall and DPI**.

Firewall Events

By default, the IDF Server Plug-in collects Firewall and DPI Event logs from the IDF Client Plug-ins at every heartbeat. (This can be turned off from the **Firewall and DPI** tab in the **System > System Settings** screen.) The data from the logs is used to populate the various reports, graphs, and charts in the IDF Server Plug-in.

Once collected by the IDF Server Plug-in, Event logs are kept for a period of time which can be set from **System** tab in the **System > System Settings** screen.

The Firewall Events screen displays the current Firewall events, along with the following information columns:

- **Firewall Event icon**: Indicates the event type. Events can be any of the following:

  Single Event

  Single Event with data

  Folded Event

  Folded Event with data

Note: Event folding occurs when multiple events of the same type occur in succession. This saves disk space and protects against DoS attacks that may attempt to overload the logging mechanism.

- **Time**: Time the event took place on the computer.
- **Computer**: The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason**: Log entries on this screen are generated either by Firewall Rules or by Stateful Configuration settings. If an entry is generated by a Firewall Rule, the column entry will be prefaced by "Firewall Rule:" followed by the name of the Firewall Rule. Otherwise the column entry will display the Stateful Configuration setting that generated the log entry.
- **Tag(s)**: Tags associated with the event.
- **Action**: The action taken by the Firewall Rule or Stateful Configuration. Possible actions are: Allow, Deny, Force Allow, and Log Only.
- **Rank**: The Ranking system provides a way to quantify the importance of DPI and Firewall Events. By assigning "asset values" to computers, and assigning "severity values" to DPI Rules and Firewall Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank when viewing DPI or Firewall Events.
- **Direction**: The direction of the affected packet (incoming or outgoing).
- **Interface**: The MAC address of the interface through which the packet was traveling.
- **Frame Type**: The frame type of the packet in question. Possible values are **"**IP**"**, "ARP", "REVARP", and "Other: XXXX" where XXXX represents the four digit hex code of the frame type.

- **Protocol**: Possible values are **"**ICMP**"**, **"**IGMP**"**, **"**GGP**"**, **"**TCP**"**, **"**PUP**"**, **"**UDP**"**, "IDP", "ND", "RAW", "TCP+UDP", "N/A", and "Other: nnn" where nnn represents a three digit decimal value.
- **Flags**: Flags set in the packet.
- **Source IP**: The packet's source IP.
- **Source MAC**: The packet's source MAC address.
- **Source Port**: The packet's source port.
- **Destination IP**: The packet's destination IP address.
- **Destination MAC**: The packet's destination MAC address.
- **Destination Port**: The packet's destination port.
- **Packet Size**: The size of the packet in bytes.

Note: Log-only rules will only generate a log entry if the packet in question is not subsequently stopped either by a deny rule, or an allow rule that excludes it. If the packet is stopped by one of those two rules, those rules will generate a log entry and not the log-only rule. If no subsequent rules stop the packet, the log-only rule will generate an entry.

From the Firewall Events screen you can:

- **View** () the properties of a particular event
- **Filter the list**: Use the Period and Computer toolbars to filter the list of events
- **Export** () the event list data to a CSV file
- **Search** () for a particular event

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s)**: Add an Event Tag to this event (see *Event Tagging* on page 12-4)
- **Remove Tag(s)**: Remove exiting event Tags
- **Computer Details**: View the Details screen of the computer that generated the log entry
- **Firewall Rule Properties**: View the properties of the Firewall Rule associated with this event
- **Whois Source IP**: Perform a whois on the source IP
- **Whois Destination IP**: Perform a whois query on the destination IP

Viewing Firewall Event Properties

Double-clicking an event displays the Properties window for that entry which displays all the information about the event on one screen. The Tags tab displays tags that have been attached to this Event. To configure Event Tagging, go to **System > Tags**. For More information on Event tagging, see *Event Tagging* on page 12-4.

Filtering the List and/or Searching for an Event

Selecting **Open Advanced Search** from the **Advanced Search** drop-down menu toggles the display of the advanced search options.

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer domain or computer Security Profiles.

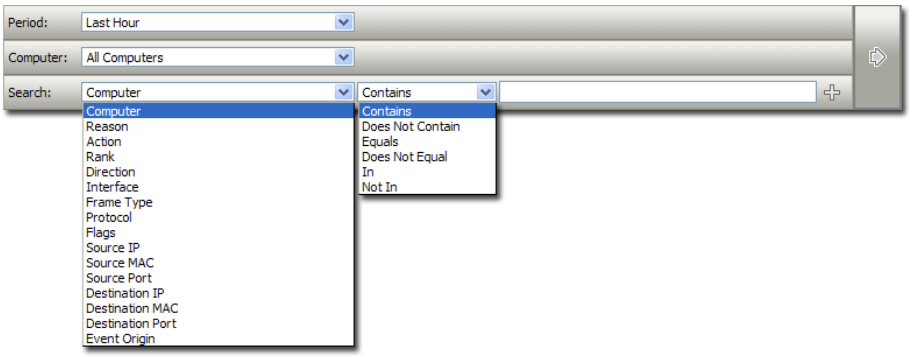


FIGURE 8-1. Computers Toolbar

Advanced Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string

- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Exporting Events

Clicking the **Export...** button exports all or selected events to a CSV file.

Tagging Firewall Events

Event Tagging allows you to manually tag Firewall Events with custom labels ("Assigned to Tom for review", etc.). Event tagging enables specialized views of events, dashboards, and reports and can be applied to a single event, similar events, or even to all future similar events.

To apply a tag to one or more selected Events:

PATH: IDF MAIN MENU | FIREWALL > FIREWALL EVENTS

1. Select the events in the **Events** list, then right-click and select **Add Tag(s)...**.
2. Type a name for the tag. (IDF Server Plug-in will suggest matching names of existing tags as you type.)
3. Select **1 Selected System Event**. (If you selected multiple events from the Events list, the number of selected events will be displayed.) Click **Next**.
4. Enter some optional comments and click **Finish**.

Looking at the Events list, you can see that the Event has now been tagged.

To tag multiple similar Events:

1. Right-click on a representative event from the **Events** list and select **Add tag(s)...**.
2. Type a name for the tag. (IDF Server Plug-in will suggest matching names of existing tags as you type.)
3. Select **Also apply to similar Firewall Events**.

4. If you want to narrow your event selection, select **Include Advanced Options**.
5. Click **Next**.
6. If you selected Advanced Options, make your selections. For example, you could look for similar events only on a specific computer, or domain of computers. If this is the case, make your selections and click **Next**.
7. Select which attributes will be examined to determine whether Events are similar or not. For the most part, the attribute options are the same as the information displayed in the columns of the Events list screen. When you have selected which attributes to include in the Event selection process, click **Next**.
8. Select what type of similar Firewall Events should this rule be applied to.

Note: Notice the Save Auto-Tag Rule option. The selection criteria you have specified can be saved so that you can apply them again at a future date when new events have accumulated. Saved auto-tag rules can be found in the System > Tags screen.

---

9. Click **Next**.
10. Enter some optional comments and click **Next**.
11. Review the Summary of your Event selection criteria and click **Finish**.

Looking at the Events list, you can see that your original Event and all similar Events have been tagged.

To tag multiple similar Events as well as future similar Events:

The procedure for tagging multiple similar as well as future Events is the same as above except for step 8, where you also select **New Firewall Events**. Selecting **New Firewall Events** causes the IDF Server Plug-in to scan its database every five seconds (or more) for new Events and tag the appropriate ones.

Note: Tagging only occurs after Events have been retrieved from the Client Plug-ins to the IDF Server Plug-in's database.

Firewall Rules

Firewall Rules examine the control information in individual packets. The Rules either block or allow those packets based on rules that are defined on these screens. Firewall Rules are assigned directly to computers or to Security Profiles which are in turn assigned to a computer or collection of computers.

About Firewall Rules

IDF Firewall Rules have both a rule action and a rule priority. Used in conjunction, these two properties allow you to create very flexible and powerful rule-sets. Unlike rule-sets used by other firewalls, which may require that the rules be defined in the order in which they should be run, IDF Firewall Rules are run in a deterministic order based on the rule action and the rule priority, which is independent of the order in which they are defined or assigned.

Rule Action

Each rule can have one of the following actions:

- **Bypass**: If a packet matches a bypass rule, it is passed through both the firewall and the DPI Engine regardless of any other rule (at the same priority level).
- **Log Only**: If a packet matches a log only rule it is passed and the event is logged.
- **Force Allow**: If a packet matches a force allow rule it is passed regardless of any other rules (at the same priority level).
- **Deny**: If a packet matches a deny rule it is dropped.
- **Allow**: If a packet matches an allow rule, it is passed. Any traffic not matching one of the allow rules is denied.

Adding an ALLOW rule will deny everything else:

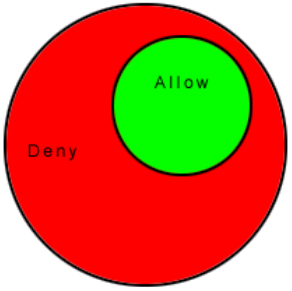


FIGURE 8-2. ALLOW Rule

A DENY rule can be implemented over an ALLOW to block certain kinds of traffic:

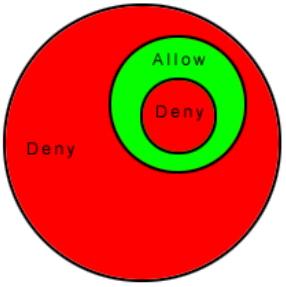


FIGURE 8-3. DENY Rule

The FORCE ALLOW rule can be placed over the denied traffic to allow certain exceptions to pass through:

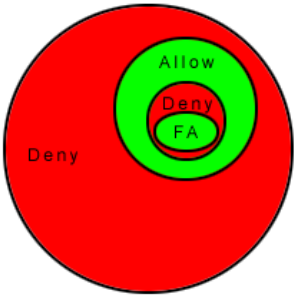


FIGURE 8-4. FORCE ALLOW Rule

Rule Priority

Rule actions of type deny and force allow can be defined at any one of 5 priorities to allow further refinement of the permitted traffic defined by the set of allow rules. Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action (force allow, deny, allow, log only).

The priority context allows you to successively refine traffic controls using deny/force allow combinations to achieve a greater flexibility. Within the same priority context an allow rule can be negated with a deny rule, and a deny rule can be negated by a force allow rule.

Note: Rule Actions of type allow run only at priority 0 while rule actions of type log only run only at priority 4.

Putting Rule Action and Priority Together

Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action. The order in which rules of equal priority are processed is as follows:

- Bypass

- Log Only
- Force Allow
- Deny
- Allow

Note: Remember that Rule Actions of type allow run only at priority 0 while rule actions of type log only run only at priority 4.

Note: It is important to remember that if you have a force allow rule and a deny rule at the same priority the force allow rule takes precedence over the deny rule and therefore traffic matching the force allow rule will be permitted.

Stateful Filtering

When stateful analysis is enabled, packets are analyzed within the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols (e.g. UDP and ICMP) a pseudo-stateful mechanism is implemented based on historical traffic analysis.

- A packet is passed through the stateful routine if it is explicitly allowed via static rules.
- The packet is examined if it belongs to an existing connection by checking the connection table for matching end points
- The TCP header is examined for correctness (e.g. sequence numbers, flag combination)

Once enabled, the stateful engine is applied to all traffic traversing the interface.

UDP pseudo-stateful inspection, by default, rejects any incoming “unsolicited” UDP packets. If a computer is running a UDP server, a force allow rule must be included in the policy to permit access to that service. For example, if UDP stateful inspection is enabled on a DNS server, a force allow rule permitting UDP traffic to port 53 is required.

ICMP pseudo-stateful inspection, by default, rejects any incoming unsolicited ICMP request-reply and error type packets. A force allow must be explicitly defined for any unsolicited ICMP packet to be allowed. All other ICMP (non request-reply or error type) packets are dropped unless explicitly allowed with static rules.

Bypass Rule

There is a special type of Firewall Rule called a Bypass Rule. It is designed for media intensive protocols where filtering may not be desired. You create a Bypass Rule by selecting "bypass" as the rule's "Action" when creating a new Firewall Rule.

The "Bypass" action on Firewall Rules differs from a Force Allow rule in the following ways:

- Packets matching Bypass will not be processed by DPI Rules
- Unlike Force Allow, Bypass will not automatically allow the responses on a TCP connection when Stateful Configuration is on (see below for more information)
- Some Bypass rules are optimized, in that traffic will flow as efficiently as if our Client Plug-in was not there (see below for more information)

Note: When a Bypass Firewall Rule is sent to a Client Plug-in older than version 5.0, it will be treated as a Force Allow, which will not skip DPI Rule processing.

Using Bypass When Stateful Configuration Is On

If you plan to use a Bypass Rule to skip DPI Rule processing on incoming traffic to TCP destination port N and Stateful Configuration is set to perform stateful inspection on TCP, you must create a matching outgoing rule for source port N to allow the TCP responses. (This is not required for Force Allow rules because force-allowed traffic is still processed by the stateful engine.)

All Bypass rules are unidirectional. Explicit rules are required for each direction of traffic.

Optimization

The Bypass Rule is designed to allow matching traffic through at the fastest possible rate. Maximum throughput can be achieved with (all) the following settings:

- **Priority**: Highest

- **Frame Type**: IP
- **Protocol**: TCP, UDP, or other IP protocol. (Do not use the **"**Any**"** option.)
- **Source and Destination IP and MAC**: all **"**Any**"**
- If the protocol is TCP or UDP and the traffic direction is "incoming", the Destination Ports must be one or more specified ports (not "Any"), and the Source Ports must be "Any".
- If the protocol is TCP or UDP and the traffic direction is "outgoing", the Source Ports must be one or more specified ports (Not "Any"), and the Destination Ports must be "Any".
- **Schedule**: None.

Logging

Packets that match the bypass rule will not be logged. This is not a configurable option.

Firewall Rule Sequence

Packets arriving at a computer running a Client Plug-in get processed first by Firewall Rules, then the Stateful Configuration conditions, and finally by the DPI Rules.

This is the order in which Firewall Rules are applied (incoming and outgoing):

1. Firewall Rules with priority 4 (highest)
   a. Bypass
   b. Log Only (Log Only rules can only be assigned a priority of 4 (highest))
   c. Force Allow
   d. Deny
2. Firewall Rules with priority 3 (high)
   a. Bypass
   b. Force Allow
   c. Deny
3. Firewall Rules with priority 2 (normal)
   a. Bypass
   b. Force Allow

   c. Deny

4. Firewall Rules with priority 1 (low)
   a. Bypass
   b. Force Allow
   c. Deny
5. Firewall Rules with priority 0 (lowest)
   a. Bypass
   b. Force Allow
   c. Deny
   d. Allow (Note that an Allow rule can only be assigned a priority of 0 (lowest))

Within the same priority context, a deny rule will override an allow rule, and a force allow rule will override a deny rule. By using the rule priorities system, a higher priority deny rule can be made to override a lower priority force allow rule.

Consider the example of a DNS server policy that makes use of a force allow rule to allow all incoming DNS queries over TCP/UDP port 53. Creating a deny rule with a higher priority than the force allow rule lets you specify a particular range of IP addresses that must be prohibited from accessing the same public server.

Priority-based rule sets allow you set the order in which the rules are applied. If a deny rule is set with the highest priority, and there are no force allow rules with the same priority, then any packet matching the deny rule is automatically dropped and the remaining rules are ignored. Conversely, if a force allow rule with the highest priority flag set exists, any incoming packets matching the force allow rule will be automatically allowed through without being checked against any other rules.

A Note on Logging

Bypass Rules will never generate a log entry. This is not configurable.

Log-only rules will only generate a log entry if the packet in question is not subsequently stopped by either:

- a deny rule, or
- an allow rule that excludes it.

If the packet is stopped by one of those two rules, those rules will generate the log entry and not the log-only rule. If no subsequent rules stop the packet, the log-only rule will generate an entry.

Putting It All Together To Design a Firewall Policy

Generally speaking, there are two approaches when defining a firewall policy for a computer:

- **Prohibitive**: That which is not expressly allowed is prohibited. Prohibitive policies can be created by using a combination of allow rules to describe allowed traffic and deny rules to further restrict permitted traffic.
- **Permissive**: That which is not expressly prohibited is allowed. Permissive policies can be created through the exclusive used of deny rules to describe the traffic that should be dropped.

In general, prohibitive policies are preferred and permissive policies should be avoided.

Force allow rules should only be used in conjunction with allow and deny rules to allow a subset of traffic that has been prohibited by the allow and deny rules. Force allow rules are also required to allow unsolicited ICMP and UDP traffic when ICMP and UDP stateful are enabled.

Take the example of how a simple firewall policy can be created for a Web server.

1. First enable stateful inspection for TCP, UDP, and ICMP using a global stateful configuration with these options enabled.
2. Add a Firewall Rule to allow TCP and UDP replies to requests originated on the workstation. To do this create an incoming allow rule with the protocol set to "TCP + UDP" and select the Not checkbox and the **Syn** checkbox under Specific Flags. At this point the policy only allows TCP and UDP packets that are replies to requests initiated by a user on the workstation. For example, in conjunction with the stateful analysis options enabled in step 1, this rule allows a user on this computer to perform DNS lookups (via UDP) and to browse the Web via HTTP (TCP).
3. Add a Firewall Rule to allow ICMP replies to requests originated on the workstation. To do this, create an incoming allow rule with the protocol set to "ICMP" and select the **Any Flags** checkbox. This means that a user on this computer can ping other workstations and receive a reply but other users will not be able to ping this computer.

4. Add a Firewall Rule to allow incoming TCP traffic to port 80 and 443 with the **Syn** checkbox checked in the Specific Flags section. This means that external users can access a Web server on this computer.

   At this point we have a basic firewall policy that allows solicited TCP, UDP and ICMP replies and external access to the Web server on this computer all other incoming traffic is denied.

   For an example of how deny and force allow rule actions can be used to further refine this profile consider how we may want to restrict traffic from other computers in the network. For example, we may want to allow access to the Web server on this computer to internal users but deny access from any computers that are in the DMZ. This can be done by adding a deny rule to prohibit access from servers in the DMZ IP range.rule

5. Next we add a deny rule for incoming TCP traffic with source IP 10.0.0.0/24 which is the IP range assigned to computers in the DMZ. This rule denies any traffic from computers in the DMZ to this computer.

   We may, however, want to refine this policy further to allow incoming traffic from the mail server which resides in the DMZ.

6. To do this we use a force allow for incoming TCP traffic from source IP 10.0.0.100. This force allow overrides the deny rule we created in the previous step to permit traffic from this one computer in the DMZ.

Important Things To Remember

- All traffic is first checked against Firewall Rules before being analyzed by the stateful inspection engine. If the traffic clears the Firewall Rules, the traffic is then analyzed by the stateful inspection engine (provided stateful inspection is enabled in the stateful configuration).
- Allow rules are prohibitive. Anything not specified in the allow rules is automatically dropped. This includes traffic of other frame types so you need to remember to include rules to allow other types of required traffic. For example, don't forget to include a rule to allow ARP traffic if static ARP tables are not in use.
- If UDP stateful inspection is enabled a force allow rule must be used to allow unsolicited UDP traffic. For example, if UDP stateful is enabled on a DNS server then a force allow for port 53 is required to allow the server to accept incoming DNS requests.

- If ICMP stateful inspection is enabled a force allow rule must be used to allow unsolicited ICMP traffic. For example, if you wish to allow outside ping requests a force allow rule for ICMP type 3 (Echo Request) is required.
- A force allow acts as a trump card only within the same priority context.
- If you do not have a DNS or WINS server configured (which is common in test environments) a force allow incoming UDP port 137 rule may be required for NetBios.

Note: When troubleshooting a new firewall policy the first thing you should do is check the Firewall Rule logs on the Client Plug-in. The Firewall Rule logs contain all the information you need to determine what traffic is being denied by Firewall elements that have been defined so that you can further refine your policy as required.

Creating and Applying New Firewall Rules

The Firewall Rules screen allows you to view, create, and edit Firewall Rules. The screen displays a list of current Firewall Rules, along with information columns that include:

- Firewall icon: Indicates the following for each rule:

  Normal Firewall Rules

  Firewall Rules that operate according to a schedule
- **Action**: Whether the Client Plug-in will allow packets matching the rule's criteria through regardless of any other rules that would block them ("force allow"); block packets matching the rule's criteria ("deny"); exclusively allow only packets matching the rule's criteria and block all others ("Allow"); or log packets matching the rule's criteria and let them pass ("log only"). Within a priority level (see next item), rules are applied in this order:
  a. "bypass"
  b. "force allow"
  c. "deny"
  d. "allow"
  e. "log only"

- **Priority**: Firewall Rules can have a priority of 0 (lowest) to 4 (highest). High priority rules are applied first.
- **Packet Direction**: Whether the packet is incoming or outgoing.
- **Packet Source**: All the information that describes the packet's source (frame type, protocol, IPs, ports, flags, etc.)
- **Packet Destination**: All the information that describes the packet's destination (frame type, protocol, IPs, ports, flags, etc.).
- **Specific Flags**: Which particular to flags have to be set for the rule to trigger. (Flags will vary depending on protocol.)

From the Firewall Rule screen you can:

- Create New Firewall Rules from scratch (New)
- Import () Firewall Rules from an XML file
- Examine or modify the Properties of an existing Firewall Rule ()
- Duplicate (and then modify) existing Firewall Rules ()
- Delete a Firewall Rule ()
- Export () one or more Firewall Rules to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Note: Firewall Rules that are assigned to one or more computers or that are part of a Security Profile cannot be deleted.

Clicking **New** (New) or **Properties** () displays the Firewall Rules Properties window.

To create or edit a Firewall Rule:

PATH: IDF MAIN MENU | FIREWALL > FIREWALL RULES

1. Click **New** to create new Firewall Rules from scratch, or select an existing Firewall Rule and click **Properties** () to modify the Firewall Rule.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the Firewall Rule.

- **Description**: A detailed description of the Firewall Rule.
- **Action**: Your Firewall Rule can behave in four different ways. These are described here in order of precedence:
  - The traffic can bypass the firewall completely. This is a special rule that can cause the packets to bypass the firewall and DPI engine entirely. Use this setting for media intensive protocols where filtering may not be desired. To find out more about the bypass rule, see *Bypass Rule* on page 8-12.
  - It can log only. This means it will only make an entry in the logs and not interfere with the traffic.
  - It can force allow defined traffic (it will allow traffic defined by this rule without excluding any other traffic.)
  - It can deny traffic (it will deny traffic defined by this rule.)
  - It can allow traffic (it will exclusively allow traffic defined by this rule.)

Note: Only one rule action is applied to any particular packet, and rules (of the same priority) are applied in the order listed above.

- **Priority**: If you have selected **"**force allow**"**, **"**deny**"**, or **"**log only**"** as your rule action, you can set a priority here of 0 (low) to 4 (highest). Setting a priority allows you to combine the actions of rules to achieve a cascading rule effect. Log only rules can only have a priority of 4, and Allow rules can only have a priority of 0.

Note: The priority determines the order in which rules are applied. High priority rules get applied before low priority rules. For example, a port 80 incoming deny rule with a priority of 3 will drop a packet before a port 80 incoming force allow rule with a priority of 2 ever gets applied to it.

- **Packet Direction**: Select whether this rule will be applied to incoming or outgoing traffic.
- **Frame Type**: Select or specify the frame type your rule will be looking for. Use the checkbox to specify whether you will be filtering for this frame type or anything but this frame type.

Note: For a list of frame types, see the Internet Assigned Numbers Authority (IANA) Web site.

- **Protocol**: Select or specify the protocol your rule will be looking for. Use the checkbox to specify whether you will be filtering for this protocol or anything but this protocol.

Note: You can choose from the drop down list of predefined common protocols, or you can select "Other" and enter the protocol code yourself (a three digit decimal value from 0 to 255).

3. In the "Packet Source" area, specify any option to apply to the packet header's source information.
   - **IP**: Specify an IP address, a masked IP address, an IP range, or select an IP list from one you defined in the IP Lists screen.
   - **MAC**: Specify a MAC address or select a MAC list from one you defined in the MAC Lists screen.
   - **Port**: You can specify a comma separated list of ports or a dash separated port range in the port(s) option as well as just a single port (e.g., 80, 443, 1-100) or select a Port list from one you defined in the Port Lists screen.
4. In the "Packet Destination" area, specify any options to apply to the packet header's destination information.
   - **IP**: Specify an IP address, a masked IP address, an IP range, or select an IP list from one you defined in the IP Lists screen.
   - **MAC**: Specify a MAC address or select a MAC list from one you defined in the MAC Lists screen.
   - **Port**: You can specify a comma separated list of ports or a dash separated port range in the port(s) option as well as just a single port (e.g., 80, 443, 1-100) or select a Port list from one you defined in the Port Lists screen.
5. In the "Specific Flags" area, if you have selected TCP, ICMP, or TCP+UDP as your protocol in the "General Information" section above, you can direct your Firewall Rule to watch for specific flags.
6. In the popup window, specify any desired information in "General Information" area of the **General** tab.

7. Click the **Options** tab and specify any desired information.
   - **Alert**: Select whether or not this Firewall Rule should trigger an alert when it is triggered. If you only wish this rule to be active during specific periods, assign a schedule from the drop-down list.

     Note: Only Firewall Rules whose "Action" is set to "Deny" or "Log Only" can be configured to trigger an alert. (This is because alerts are triggered by counters which are incremented with data from log files.)

   - **Schedule**: Select whether the Firewall Rule should only be active during a scheduled time.

     Note: Firewall Rules that are active only at scheduled times are displayed in the Firewall Rules screen with a small clock over their icon ().

   - **Context**: Rule Contexts are a powerful way of implementing different security policies depending on the computer's network environment. You will most often use Contexts to create Security Profiles which apply different Firewall and DPI Rules to computers (usually mobile laptops) depending on whether that computer is in or away from the office.

     Contexts are designed to be associated with Firewall and DPI Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied.

     To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller. For more information on Contexts, see *Contexts* on page 10-6.

     Note: For an example of a Security Profile that implements Firewall Rules using Contexts, look at the properties of the "Windows Mobile Laptop" Security Profile.

8. Click the **Assigned To** tab to view a list of Security Profiles which include this Firewall Rule as well as any computers to which this Firewall Rule has been assigned directly. Firewall Rules can be assigned to Security Profiles in the Security Profiles screen and to computers in the Computers screen.
9. Click **OK**.

Now you have to assign the new Firewall Rule to a computer. The best way to manage the application of Firewall Rules to computers is by way of Security Profiles. Having a Security Profile called "Developer Laptop", for example, allows you to create a set of Firewall Rules all designed for the particular environment "developer laptops" operate in. You can then assign them all to the "Developer Laptop" Security Profile, and then assign that Security Profile to that collection of computers. Anytime you need to create and assign a new Firewall Rule to your "developer laptops", you just assign it to the Security Profile, and all "Developer Laptop" computers will be updated with the new Firewall Rule.

To include a new Firewall Rule in a Security Profile:

PATH: IDF MAIN MENU | SECURITY PROFILES

1. Double-click the Security Profile to which you want to assign a new rule. This will open the Profile's Details window.
2. Click **Firewall Rules** in the navigation pane on the left.
3. Find your new Firewall Rule in the list and put a check in its checkbox.
4. Click **Save**.

If the "Automatically update all affected computers after changing any aspect of the IDF System." option is enabled on the Computers tab in the **System > System Settings** screen, all computers to which that Security Profile has been assigned will be updated with the new rule.

To assign a new Firewall Rule directly to a computer:

PATH: IDF MAIN MENU | COMPUTERS

1. Double-click the computer to which you want to assign the new rule.
2. Click **Firewall Rules** in the navigation pane on the left.
3. Find your new Firewall Rule in the list and put a check in its checkbox.
4. Click **Save**.

As before, if the "Automatically update all affected computers after changing any aspect of the IDF System." option is enabled on the **Computers** tab in the **System > System Settings** screen, all computers to which that Security Profile has been assigned will be updated with the new rule.

Note: If you apply other settings to a computer (for example, adding additional Firewall Rules, or modifying stateful configuration settings), an asterisk will appear next to the name of the Security Profile (in the Security Profile column in the Computers screen) indicating that the default settings have been changed.

Stateful Configurations

IDF's Stateful Configuration mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis. Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static Firewall Rule conditions,
2. The packet is examined to determine whether it belongs to an existing connection by checking a connection table created by the stateful mechanism for matching end points, and
3. The TCP header is examined for correctness (e.g. sequence numbers, flag combinations, etc.).

Managing Stateful Configurations

The Stateful Configuration screen lets you define multiple stateful inspection configurations which you can then include in your Security Profiles. The screen lists current stateful configurations, along with information that includes the name, description, and Normal Stateful Configurations icon ( ).

From the toolbar or context menu you can:

- Create New (New) Stateful Configurations from scratch
- Import ( ) Stateful Configuration from an XML file

- Examine or modify the Properties ( ) of an existing Stateful Configuration
- Duplicate ( ) (and then modify) existing Stateful Configurations
- Delete a Stateful Configuration ( )
- Export ( ) one or more Stateful Configurations to an XML file. (Either export them all by click the Export... button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking New (New) or Properties ( ) displays the Stateful Configuration properties window.

To create or edit a Stateful Configuration:

PATH: IDF MAIN MENU | FIREWALL > STATEFUL CONFIGURATIONS

1. Click **New** to create a new Stateful Configuration from scratch, or select an existing configuration and click **Properties** ( ) to modify it.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the Stateful Configuration.
   - **Description**: Type a description of the Stateful Configuration. This description will only appear here.
3. In the "IP Packet Inspection" area, choose whether to Deny all incoming fragmented packets: If this option is enabled, all fragmented packets are dropped with the following log entry: "IP fragmented packet". The one exception to this rule is the presence of packets with a total length smaller than the IP header length. Such packets are dropped silently.

   WARNING! Attackers sometimes create and send fragmented packets in an attempt to bypass Firewall Rules.

   The Firewall Rule engine, by default, performs a series of checks on fragmented packets. This is default behavior and cannot be reconfigured. Packets with the following characteristics are dropped:

   - **Invalid fragmentation flags/offse**t: A packet is dropped when either the DF and MF flags in the IP header are set to 1, or the header contains the DF flag set to 1 and an Offset value different than 0.

- **First fragment too small**: A packet is dropped if its MF flag is set to 1, its Offset value is at 0, and it has total length of less than 120 bytes (the maximum combined header length).
- **IP fragment out of boundary**: A packet is dropped if its Offset flag value combined with the total packet length exceeds the maximum datagram length of 65535 bytes.
- **IP fragment offset too small**: A packet is dropped if it has a non-zero Offset flag with a value that is smaller than 60 bytes.

4. Click the **TCP** tab and specify any desired information in the "TCP Packet Inspection" area.
   - **Deny TCP packets containing CWR, ECE flags**: These flags are set when there is network congestion.

     RFC 3168 defines two of the six bits from the Reserved field to be used for ECN (Explicit Congestion Notification), as follows:
     - Bits 8 to 15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
     - TCP Header Flags Bit Name Reference:
     - Bit 8: CWR (Congestion Window Reduced) [RFC3168]
     - Bit 9: ECE (ECN-Echo) [RFC3168]

     WARNING! Automated packet transmission (such as that generated by a denial of service attack, among other things) will often produce packets in which these flags are set.

   - **Enable TCP stateful inspection**: Enable stateful inspection at the TCP level. If you enable stateful TCP inspection, the following options become available:
     - **Enable TCP stateful logging**: TCP stateful inspection events will be logged.
     - **Limit the number of incoming connections from a single computer to**: Limiting the number of connections from a single computer can lessen the effect of a denial of service attack.
     - **Limit the number of outgoing connections to a single computer to**: Limiting the number of outgoing connections to a single computer can significantly reduce the effects of Nimda-like worms.

- **Limit the number of half-open connections from a single computer to**: Setting a limit here can protect you from DoS attacks like SYN Flood. Although most servers have timeout settings for closing half-open connections, setting a value here can prevent half-open connections from becoming a significant problem. If the specified limit for SYN-SENT(remote) entries is reached, subsequent TCP packets from that specific computer will be dropped.

Note: When deciding on how many open connections from a single computer to allow, choose your number from somewhere between what you would consider a reasonable number of half-open connections from a single computer for the type of protocol being used, and how many half-open connections from a single computer your system can maintain without getting congested.

- **Enable Syn-Flood protection when the number of half-open connections exceeds**: Unlike setting a hard limit on the number of half-open connections from a single computer, the Syn-Flood protection mechanism starts to use Syn-cookies once the set number of open connections is reached (regardless of whether the connections come a single computer or not). The use of Syn-cookies means that connections are not rejected. However, no entry is created for them in the state table, and they are not passed to the application until an appropriate SYN-ACK is received from the destination computer.

Note: SYN Flood protection is only supported on versions 7.5 or earlier of the Windows Client Plug-ins. It is not supported on versions 7.5 SP1 or later of the Windows Client Plug-ins.

- **Enable ACK Storm protection when the number of already acknowledged packets exceeds**: Set this option to log an event that an ACK Storm attack has occurred.
- **Drop Connection when ACK Storm detected**: Set this option to drop the connection if such an attack is detected.

5. In the "FTP Options" area, specify any desired information.
   - **Active FTP**
     - **Allow Incoming**: Allow Active FTP when this computer is acting as a server.
     - **Allow Outgoing**: Allow Active FTP when this computer is acting as client.
   - **Passive FTP**
     - **Allow Incoming**: Allow Passive FTP when this computer is acting as a server.
     - **Allow Outgoing**: Allow Passive FTP when this computer is acting as a client.

Tip: Generally speaking, Active FTP is more secure from the server point of view, and Passive FTP is more secure from the client point of view.

---

6. Click the **UDP** tab and specify any desired information in the "UDP Packet Inspection" area.
   - **Enable UDP stateful inspection**: Check to enable stateful inspection of UDP traffic.

Note: The UDP stateful mechanism drops unsolicited incoming UDP packets. For every outgoing UDP packet, the rule will update its UDP "stateful" table and will then only allow a UDP response if it occurs within 60 seconds of the request. If you wish to allow specific incoming UDP traffic, you will have to create a Force Allow rule. For example, if you are running a DNS server, you will have to create a Force Allow rule to allow incoming UDP packets to destination port 53.

WARNING! **Without stateful inspection of UDP traffic, an attacker could masquerade as a DNS server and send unsolicited UDP "replies" from source port 53 to computers behind a firewall.**

   - **Enable UDP stateful logging**: Checking this option will enable the logging of UDP stateful inspection events.

7. Click the **ICMP** tab and specify any desired information in the "ICMP Packet Inspection" area.
   - **Enable ICMP stateful inspection**: Check to enable stateful inspection of ICMP traffic.

Note: The ICMP (pseudo-)stateful mechanism drops incoming unsolicited ICMP packets. For every outgoing ICMP packet, the rule will create or update its ICMP "stateful" table and will then only allow a ICMP response if it occurs within 60 seconds of the request. (ICMP pair types supported: Type 0 & 8, 13 & 14, 15 & 16, 17 & 18.)

WARNING! **With stateful ICMP inspection enabled, you can, for example, only allow an ICMP echo-reply in if an echo-request has been sent out. Unrequested echo-replies could be a sign of several kinds of attack including a Smurf amplification attack, a Tribe Flood Network communication between master and daemon, or a Loki 2 back-door.**

   - **Enable ICMP stateful logging**: Checking this option will enable the logging of ICMP stateful inspection events.

8. Click the **Assigned To** tab and specify any desired information.

   The Assigned To tab lists the Security Profiles and computers that are making use of this stateful inspection configuration.

Chapter 9

Using Deep Packet Inspection

This chapter describes how to use Trend Micro™ Intrusion Defense Firewall™ Deep Packet Inspection to protect your network and computers from security risks.

Topics in this chapter:

About Deep Packet Inspection

When first applying a new set of DPI Rules you can choose to set the DPI behavior to "Detect". When in Detect mode, the DPI engine will apply all the same DPI Rules to traffic but instead of dropping packets, it will only log an Event and let the traffic pass. Use this behavior to ensure the new DPI Rules will not interfere with legitimate traffic.

This setting only applies when the Network Engine is operating Inline; that is, live traffic is being streamed through the IDF network engine. The alternative to Inline mode is Tap mode, where the live traffic is cloned, and it is only this cloned traffic that is analyzed by the network engine. Prevent mode is impossible when in Tap mode because the network engine does not control the live traffic stream.

Packet Processing Sequence

Both incoming and outgoing network traffic gets fed through a pipeline of modules:

FIGURE 9-1. Module Pipeline

- **Verification**: Basic checks for validity of the packet
- **Micro Filter**: Basic firewall bypass rules are enforced at this layer
- **Blacklist**: Maintains a list of known bad IPs as used by the Traffic Analysis feature
- **Fragmentation**: Fragments packets that are larger than the MTU
- **Firewall Rules**: All packets not processed by the Micro Filter are processed by the Firewall
- **Stateful Inspection, SSL Decryption, and DPI Rules**: Acts as one module where the following functions are performed:
  - **Stateful Inspection**: Maintains known connections that are valid for a response. This feature also controls the connection limits and does SYN Flood and ACK Storm protection
  - **SSL Decryption**: If required and configured this feature decrypts the SSL protected traffic for analysis by the DPI engine

- **DPI**: Deep Packet Inspection engine that does pattern matching and custom code operations
- **Reassembly**: Reassembles fragmented packets for later use by the DPI engine

Although incoming and outgoing traffic flow through the pipeline in the same order, the internal sub-order inside the Stateful Inspection, SSL, and DPI module depends on traffic direction:

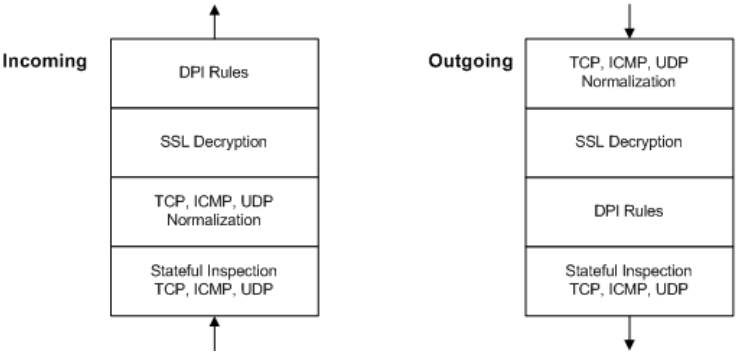


FIGURE 9-2. Module Pipeline

Turning Deep Packet Inspection On or Off

To turn the Deep Packet Inspection on or off:

PATH: IDF MAIN MENU | DEEP PACKET INSPECTION

1. In the "Deep Packet Inspection" area, choose **On** or **Off**.
2. Set the Inline DPI behavior to "Prevent" or "Detect".

   To switch between Inline and Tap mode, go to **System > System Settings > Firewall and DPI**.
3. Choose whether to enable Recommendation Scans.

   Client Plug-ins can be configured to perform regular Recommendation Scans which scan a computer and make recommendations about the application of various Security Rules. Selecting this checkbox will automatically assign recommended rules for the computer and automatically unassign rules that are not required.

Note: If you select this option, you should also opt to allow IDF Rule Updates to automatically assign new DPI Rules. Go to System > System Settings > Updates and select Allow IDF Rule Updates to automatically assign new DPI Rules in the IDF Rule Updates area.

To perform periodic Recommendation Scans, go to **System > System Settings > Scan**.

DPI Events

By default, the IDF Server Plug-in collects Firewall and DPI Event logs from the IDF Client Plug-ins at every heartbeat. (This can be turned off from the Firewall and DPI tab in the System > System Settings screen.) The data from the logs is used to populate the various reports, graphs, and charts in the IDF Server Plug-in.

Once collected by the IDF Server Plug-in, Event logs are kept for a period of time which can be set from System tab in the System > System Settings screen. The default setting is one week.

From the main screen you can:

- View ( ) the properties of a particular event
- Filter the list: Use the Period and Computer toolbars to filter the list of events
- Export ( ) the event log data to a CSV file
- Search ( ) for a particular event

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s)**: Add an Event Tag to this event (see *Event Tagging* on page 12-4.)
- **Remove Tag(s)**: Remove exiting event Tags
- **Computer Details**: View the Details screen of the computer that generated the log entry
- **DPI Rule Properties**: View the all the properties of a particular log entry on open Properties window
- **Whois Source IP**: Perform a whois on the source IP
- **Whois Destination IP**: Perform a whois on the destination IP

Filtering the List and/or Searching for an Event

Selecting "Open Advanced Search" from the "Advanced Search" drop-down menu toggles the display of the advanced search options.

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer domain or computer Security Profiles.

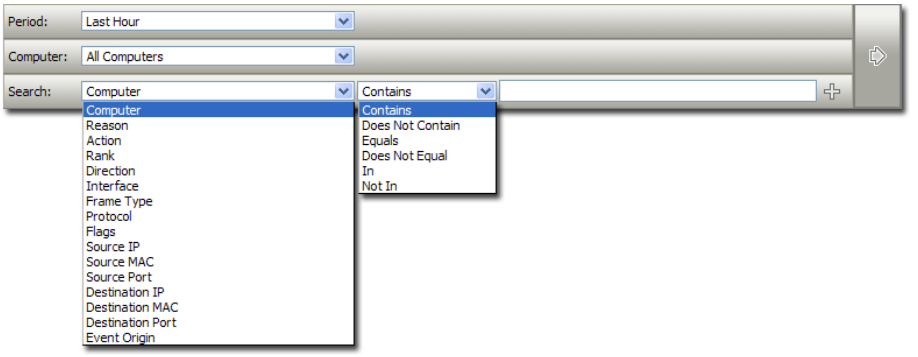


FIGURE 9-3. Computers Toolbar

Advanced Search functions (searches are not case sensitive):

- **Contains**: The entry in the selected column contains the search string
- **Does Not Contain**: The entry in the selected column does not contain the search string
- **Equals**: The entry in the selected column exactly matches the search string
- **Does Not Equal**: The entry in the selected column does not exactly match the search string
- **In**: The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In**: The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Viewing DPI Event Properties

Double-clicking an event displays the Properties window for that entry. The Tags tab displays tags that have been attached to this Event. For More information on Event tagging, see **System > Tags**, and *Event Tagging* on page 12-4.

To view DPI Event information:

PATH: IDF MAIN MENU | DEEP PACKET INSPECTION

Columns for the DPI Events display:

- **Time**: Time the event took place on the computer.
- **Computer**: The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason**: The DPI Rule associated with this event.
- **Tag(s)**: Tags associated with the event.
- **Application Type**: The Application Type associated with the DPI Rule which caused this event.
- **Action**: What action the DPI Rule took (Allow, Deny, Force Allow, Log Only, or Detect Only (if the rule is in Detect Only mode)).
- **Rank**: The Ranking system provides a way to quantify the importance of DPI and Firewall Events. By assigning "asset values" to computers, and assigning "severity values" to DPI Rules and Firewall Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank when viewing DPI or Firewall Events.
- **Severity**: The Rule Severity level: Critical, High, Medium, Low, or Error.
- **Direction**: The direction of the packet (incoming or outgoing).
- **Flow**: The source of the packet. "Connection Flow" indicates that the packet comes from the initiator of the TCP connection. "Reverse Flow" indicates that the packet comes from the receiver of the TCP connection.
- **Interface**: The MAC address of the interface through which the packet was passing.

- **Protocol**: Possible values are **"**ICMP**"**, **"**IGMP**"**, **"**GGP**"**, **"**TCP**"**, **"**PUP**"**, **"**UDP**"**, "IDP", "ND", "RAW", "TCP+UDP", "N/A", and "Other: nnn" where nnn represents a three-digit decimal value.
- **Flags**: Flags set in the packet.
- **Source IP**: The packet's source IP.
- **Source MAC**: The packet's source MAC address.
- **Source Port**: The packet's source port.
- **Destination IP**: The packet's destination IP address.
- **Destination MAC**: The packet's destination MAC address.
- **Destination Port**: The packet's destination port.
- **Packet Size**: The size of the packet in bytes.

Exporting the Event Log

Clicking the **Export...** button exports all event log entries to a CSV file.

Tagging DPI Events

Event Tagging allows you to manually tag DPI Events with custom labels ("Assigned to Tom for review", etc.). Event tagging enables specialized views of events, dashboards, and reports and can be applied to a single event, similar events, or even to all future similar events.

To apply a tag to one or more selected Events:

PATH: IDF MAIN MENU | DEEP PACKET INSPECTION > DPI EVENTS

1. Select the events in the **Events** list, then right-click and select **Add Tag(s)...**.
2. Type a name for the tag. (IDF Server Plug-in will suggest matching names of existing tags as you type.)
3. Select **1 Selected System Event**. (If you selected multiple events from the Events list, the number of selected events will be displayed.) Click **Next**.
4. Enter some optional comments and click **Finish**.

Looking at the Events list, you can see that the Event has now been tagged.

To tag multiple similar Events:

1. Right-click on a representative event from the **Events** list and select **Add tag(s)...**.
2. Type a name for the tag. (IDF Server Plug-in will suggest matching names of existing tags as you type.)
3. Select **Also apply to similar DPI Events**.
4. If you want to narrow your event selection, select **Include Advanced Options**.
5. Click **Next**.
6. If you selected Advanced Options, make your selections. For example, you could look for similar events only on a specific computer, or domain of computers. If this is the case, make your selections and click **Next**.
7. Select which attributes will be examined to determine whether Events are similar or not. For the most part, the attribute options are the same as the information displayed in the columns of the Events list screen. When you have selected which attributes to include in the Event selection process, click **Next**.
8. Select what type of similar DPI Events should this rule be applied to.

Note: Notice the Save Auto-Tag Rule option. The selection criteria you have specified can be saved so that you can apply them again at a future date when new events have accumulated. Saved auto-tag rules can be found in the System > Tags screen.

---

9. Click **Next**.
10. Enter some optional comments and click **Next**.
11. Review the Summary of your Event selection criteria and click **Finish**.

Looking at the Events list, you can see that your original Event and all similar Events have been tagged.

To tag multiple similar Events as well as future similar Events:

The procedure for tagging multiple similar as well as future Events is the same as above except for step 8, where you also select **New DPI Events**. Selecting **New DPI Events** causes the IDF Server Plug-in to scan its database every five seconds (or more) for new Events and tag the appropriate ones.

Note: Tagging only occurs after Events have been retrieved from the Client Plug-ins to the IDF Server Plug-in's database.

DPI Rules

Whereas Firewall Rules and Stateful Configurations examine a packet's control information (data that describes the packet), DPI Rules examine the actual content of the packet (and sequences of packets). Based on the conditions set within the DPI Rule, various actions are then carried out on these packets: from replacing specifically defined or suspicious byte sequences, to completely dropping packets and resetting the connection.

The DPI Rules screen lists the current DPI Rules and information, including the following:

DPI Rule icon:

Normal DPI Rules

DPI Rules that operate according to a schedule

DPI Rules that have configuration options

DPI Rules that require configuration

The DPI Rules screen lets you create and manage DPI Rules. From the toolbar or the right-click context menu you can:

- Create New DPI Rules from scratch (New)
- Import ( ) DPI Rules from an XML file
- Examine or modify the Properties of an existing DPI Rule ( )
- Duplicate (and then modify) existing DPI Rules ( )
- Delete a DPI Rule ( )
- Export ( ) one or more DPI Rules to an XML file. (Either export them all by click the Export... button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or **Properties** ( ) displays the DPI Rule Properties window.

Note: Note the Configuration tab. DPI Rules from Trend Micro are not directly editable through IDF Server Plug-in. Instead, if the DPI Rule requires (or allows) configuration, those configuration options will be available on the Configuration tab. Custom DPI Rules that you write yourself will be editable, in which case the Rules tab will be visible.

Creating and Editing DPI Rule Properties

To create or edit DPI Rule properties:

PATH: IDF MAIN MENU | DEEP PACKET INSPECTION > DPI RULES

1. Click **New** to create new DPI Rules from scratch, or select an existing DPI Rule and click **Properties** () to modify the DPI Rule.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the DPI Rule.
   - **Description**: The description of the DPI Rule.
   - **Minimum Client Plug-in Version**: The minimum version of the IDF Client Plug-in required to implement this DPI Rule.
3. In the "Details" area, specify any desired information.
   - **Application Type**: The Application Type this DPI Rule will be grouped under. You can select an existing type, or create a new one.

     Note: You can also edit existing types from this panel. Remember that if you edit an existing Application Type from here, the changes will be applied to all security elements making use of it.

   - **Priority**: The priority level of the DPI Rule. Higher priority rules are applied before lower priority rules.

- **Severity**: Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as a sorting criteria when viewing a list of DPI Rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See **System > System Settings > Ranking**.)
- **CVSS Score**: A measure of the severity of the vulnerability according the National Vulnerability Database.
- **Detect Only**: Use this checkbox when testing new rules. By checking this box, the rule will create a log entry prefaced with the words "detect only:" but will not interfere with traffic. If you set the "disable logging" checkbox in the next panel (below), the rule's activity will not be logged regardless of whether "Detect Only" is checked or not.

Note: Some DPI Rules are designed to only operate in "Detect Only" mode and cannot be configured to block traffic. For theses rules, the "Detect Only" option will be set and locked so it cannot be changed.

---

4. In the "Events" area, specify any desired information.
   - **Disable Logging**: Check to disable Event logging.
     - **Generate Event on Packet Drop**: Log the dropping/blocking of a packet.
     - **Always Include Packet Data**: Includes the packet data in the log entry.
     - **Enable Debug Mode**: Logs multiple packets preceding and following the packet that triggered the rule. Trend Micro recommends only using this option if instructed to do so by your support provider.
5. In the "Identification" area (displayed for downloaded rules only), specify any desired information.
   - **Type**: Can be either Smart (one or more known and unknown (zero day) vulnerabilities), Exploit (a specific exploit, usually signature based), or Vulnerability (a specific vulnerability for which one or more exploits may exist).
   - **Issued**: The date the Rule was released (not downloaded).
   - **Identifier**: The rule's unique identifier tag.
   - **Last Updated**: The last date the Rule was updated.

6. Click the **Vulnerability** tab (displayed for Trend Micro rules only), to view information about this particular vulnerability.

   When applicable, the Common Vulnerability Scoring System (CVSS) is displayed. (For information on this scoring system, see the CVSS page at the National Vulnerability Database.)

7. Click the **Configuration** tab (displayed for Trend Micro rules only), to set any configuration options for the download rule.

   - **Configuration Options**: If the downloaded rule has any configurable options, they will be displayed here. Examples of options might be header length, allowed extensions for http, cookie length, etc. If you apply a rule without setting a required option, an alert will be triggered telling you which rule on which computer(s) requires configuration. (This also applies to any rules that are downloaded and automatically applied by way of a Security Update.)

     Note: DPI Rules that have configuration options are displayed in the DPI Rules screen with a small checkmark over their icon ().

   - **View Rules** (available for custom DPI Rules only): The **View Rules...** button will be available for DPI Rules that have not been marked confidential by Trend Micro. (Please contact Trend Micro for information on writing your own DPI Rules.)

8. Click the **Options** tab to vie w the options.
9. In the "Alert" area, select whether or not this DPI Rule should trigger an alert when it is triggered. If you only wish this rule to be active during specific periods, assign a schedule from the drop-down list.
10. In the "Schedule" area, select whether the DPI Rule should only be active during a scheduled time.

    Note: DPI Rules that are active only at scheduled times are displayed in the DPI Rules screen with a small clock over their icon ().

11. In the "Context" area, make any desired settings.

    Contexts are a powerful way of implementing different security policies depending on the computer's network environment. You will most often use Contexts to

create Security Profiles which apply different Firewall and DPI Rules to computers (usually mobile laptops) depending on whether that computer is in or away from the office.

Contexts are designed to be associated with Firewall and DPI Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied.

To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller. For more information on Contexts, see *Contexts* on page 10-6.

12. In the "Recommendation Options" area, choose whether to exclude this DPI Rule from Rule recommendations made after Recommendation Scans.
13. In the **Assigned To** tab, you can view the list of computers and Security Profiles to which this DPI Rule is assigned.

Creating Custom DPI Rules

IDF provides an XML-based language designed for examining packet contents and deciding whether to log an event or reset the connection.

Considerations for DPI Rules

DPI rules operate on network data as packets are processed in the kernel before delivery to the application (for incoming packets) or before transmission on the network (for outgoing packets). For this reason efficiency of rules is very important and DPI Rules are restricted to simple instruction like operations.

Hello World

Here is an example of a simple rule to detect the occurrence of a pattern:

```
<rule pat="hello">
    log "hello found"
</rule>
```

This pattern-rule is triggered by the presence of the string hello in a packet. When the rule is triggered the action block of code is executed to log an Event to the IDF Server Plug-in. The string "hello found" is supplied as a note in the DPI Event in the IDF Server Plug-in.

Note: Pattern rules are case insensitive by default, i.e., this rule will trigger on any variation of the string "hello", "HELLO", "hElLo".

Note: The DPI engine does not apply pattern rules directly on raw packet data. A malicious payload could be separated into multiple segments or packet fragments, transmitted out of order or in one byte segments. The DPI engine protects against such possible attacks by analyzing the data stream before pattern rule analysis.

XML Quoting

Some characters have special meaning in XML and must be quoted if they are to be used in patterns or note strings. This quoting is required for the following characters:

< > & " '

TABLE 9-1. XML Quoting

CHARACTER	XML QUOTING
<	<
>	>
&	&
"	"
'	'

For example to match the string one&"2" use:

```
<rule pat="one&amp;&quot;2&quot;">
```

```
    log "onetwo"
</rule>
```

Sometimes it may be more convenient to use hex encoded patterns. (See *More About Patterns* on page 9-20.)

If these characters are not quoted properly a "Computer Updated" system error will result when they are assigned.

Application Types and Rule Directions

By default, rules are triggered as patterns found in the forward connection direction. The meaning of the direction depends on where the rule is to be deployed.

On a Web server listening traffic incoming http requests arriving on port 80 would be considered the forward direction and outgoing http responses from the Web server would be considered the backward direction.

On a Web client outgoing http requests destined for port 80 would be considered the forward direction whilst incoming replies would be the backwards direction.

DPI Rules can contain multiple pattern-rules that look for strings in forward or backwards direction.

```
<fwd pat="hello">log "hello found"</fwd>
<bwd pat="goodbye"> log "goodbye"</bwd>
```

Using State to Refine Rules

In the above example the "goodbye" event triggers regardless of whether "hello" has been seen or not. We can revise this rule so that "goodbye" is only significant if "hello" has already been seen:

```
<fwd pat="hello">
    stateset 1
</fwd>
<!-- this rule resets the connection when goodbye is seen after
hello -->
<bwd pat="goodbye" state="1">
```

```
    log "goodbye"
    stateset 0
</bwd>
```

These rules illustrate the use of the "stateset" action instruction and the "state" rule constraint attribute to implement a simple state computer that continually recognizes the occurrence of "hello" followed by "goodbye" in the reverse direction on the same connection.

Any number of pattern rules can be defined together to track state in this way.

Adding Comments

As rules start to get complex it is helpful to add comments as shown above. Comments can also be used to temporarily block out some sections when testing. Standard XML comments are used with the form <!-- ... -->.

More Rule Actions

Resetting a Connection (drop)

To reset a connection, use the drop instruction:

```
<rule pat="bad">
    drop "bad"
</rule>
```

When a connection is reset with the "drop" instruction then no further rules will be executed on that connection or any further content even in the same packet (and the connection is reset to both endpoints and no further packets will be permitted)

Understanding Detect and Prevent Modes

A single DPI rule can be placed in detect mode. In this case a drop instruction executed by such a DPI rule is logged but does not cause the connection to be reset. Since the connection is not reset, further rules will still be executed because there may be other DPI rules that are operating in prevent mode.

Additionally, the DPI Engine can also be placed into "Detect Mode". In this mode connections are not reset but processing of further rules does stop.

Deferred Reset of a Connection (setdrop)

Sometimes it's useful to postpone the reset of a connection to allow further rules to execute.

```
<fwd pat="bad">
    setdrop "bad"
</fwd>
<fwd pat="worse">
    drop "worse"
</fwd>
```

In this case we will reset a connection if the content contains "bad" or "worse" but if it contains both then the reason will always be "worse".

As well it's possible to cancel a deferred reset:

```
<fwd pat="good">
    clrdrop
</fwd>
```

Note that setdrop defers the drop until the end of the packet. The occurrence of "worse" may not be the reason since that pattern may come in another packet. This is because the DPI engine does not know that "worse" is to follow and if the initial packet is determined to be malicious, it will be dropped.

More About Rule Attributes

There are several constraint attributes that can be used to constrain a rule from triggering unless preconditions are met:

State

The state attribute specifies that the rule's action is only to be executed if a previous action has set the current state to the specified value. The value can be in the range 0-255.

If the state attribute is not specified then the action is triggered regardless of the current state.

Case-sensitive Matching

The case attribute can be used to require an exact case match:

```
<fwd pat="hello" case="1"> ... </fwd>
```

Distance Constraints

The `dist` attribute can be used to require that two patterns occur within a specified range of each other:

```
<fwd pat="hello"> ... </fwd>

<fwd pat="goodbye" dist="10,20">
    log "goodbye"
</fwd>

<fwd pat="salut" distmax="10">
    log "salut"
</fwd>

<fwd pat="ciao" distmin="10">
    log "ciao"
</fwd>
```

The first form of the attribute specifies that "goodbye" will be detected but only if it is between 10 and 20 bytes from the occurrence of another pattern.

The second form `distmax` specifies only the upper bound and no lower bound on the distance.

The last form specifies no upper bound, only a lower bound.

Note: Distance constraints work with patterns in the connection direction, it is not possible to use distance constraint between a forward occurrence pattern and a backwards pattern.

Using Counters

Sometimes it is useful to trigger a rule in the absence of a pattern within a certain distance, for example, to limit the maximum size of a header field. One pattern rule can be used to start a counter, and if desired another rule can clear the counter. Counters can be used to trigger a rules without a specific pattern:

```
<fwd pat="HELLO">
    startcount 1024
</fwd>

<!-- reset if the line is longer than 256 bytes -->
<counter>
    stateset 0
</counter>

<!-- clear the counter when newline is found -->
<fwd pat="\n">
    clrcount
</fwd>
```

Only one counter can be active at a time in the same domain of rules. If another counter is started while one is pending then the pending counter is automatically cleared.

Note: If a rule starts a counter, it must be followed by a `<counter> ...</counter>`. This is enforced by the rule compiler.

More About Patterns

Patterns are restricted to fixed length strings. These may include wildcard characters as follows:

TABLE 9-2. Patterns

\A (\A)	ALPHA, A-Z A-Z (NON-ALPHA)
\w (\W)	Alphanumeric a-zA-Z0-9 (non-alpha-numeric)
\d (\D)	Digit 0-9 (non digit)
\s (\S)	Whitespace (not whitespace) [\r,\n,\t,0x32]
\p (\P)	Punctuation character, printable ascii other than above
\c (\C)	Control character, < 32, >= 127 not including whitespace
\.	Any

Special reserved or binary characters must be quoted or escaped as follows:

TABLE 9-3. Reserved Characters

\xDD	HEX BYTE 0xDD
\\	'\' escape
|	Pipe '|' escape
|xx xx xx...|	Hex pipe (Byte sequence)

Additional rules:

- Patterns cannot consist solely of wildcards.
- Hex-encoded sequences are still case-insensitive by default.
- Regular expression-style variable-length sequences like +,* are not permitted.

Examples:

```
<rule pat="|90 E8 C0 FF FF FF|/bin/sh" case="1">
    drop "IMAP overflow"
</rule>
<rule pat="port\s\d\d"> ...</rule>
```

Advanced Rule Actions

When a pattern rule triggers and the constraints are met, the rule's action is executed. So far we have seen the simple "log", "drop", and "stateset" actions. Actions can be used to define constraints that are more complex than those that can be expressed using the simple distance, case attributes.

Actions are defined mostly as a sequence of low level instructions. The instructions have access to a set of virtual registers and can perform simple arithmetic and comparison operations. Actions can also have conditional if-then-else blocks. Each instruction has one of the formats:

```
instruction STRING
instruction REG OPAND
```

For example,

```
<fwd pat="login">
    add r5 0x100 <!-- r5 <- hex 100 (=256) -->
</fwd>

<fwd pat="two">
    add r4 256 <!-- r4 <- decimal 256 -->
    load r6 r4 <!-- r6 <- -->
```

```
    <if>eq r4 r5<then/>
       log "ok"
    </if>
</fwd>
```

Register Assignments

The following virtual registers r0-r7 and c0-c7 are defined for use in instructions

TABLE 9-4. Virtual Registers

REGISTER #	FILTER REGISTER (R0-R7)	CONNECTION REGISTER (C0-C7)
0	State	Connection State
1	Cursor	UTC time/seconds
2	Reserved	Packet count
3	Reserved	Reserved
4 - 7	User defined	User defined

The state register is another way of referring to the state as used by the state attribute.

The packet count register c2 register keeps track of the number of packets processed in each connection direction. The c1 register keeps track of the current time (in seconds since 1970.) These registers can be used to express time or packet based constraints.

Additional details on registers:

- Registers c0-c3 and r0-r3 have predefined meaning.
- Registers r4-r7 can be used for any purpose.
- The connection registers c0-c7 are shared across all rules on the same connection (each connection has its own set).
- The registers r0-r7 are private to each domain of rules in a DPI Rule.
- All registers can contain 32-bit values.

Accessing Registers

Values can be put in registers and moved between registers using the load instruction:

```
<rule pat="test">
    load r4 100 <!-- load value 100 decimal into r4 -->
    load r5 r4 <!-- copy contents of register r4 into r5 -->
</rule>
```

Since `r0` is the state register, the `stateset` instruction is really just a shorthand for the load instruction; the following are equivalent:

```
<rule pat="test">
    load r0 1
    load stateset 1 <!-- same as above -->
</rule>
```

Comparing Registers

Registers can be compared using if blocks and comparison instructions. For example the following rule will reset a connection when the pattern "login" occurs more than three times:

```
<rule pat="login">
   add r4 1
   <if>
      gt r4 3<then/>
      drop "repeated3"
   </if>
</rule>
```

if-Statement

The if statement has the general format:

```
<if> (condition) <then/>
    <!-- if blocks can be nested -->
```

```
    <if> (condition) <then/>
       (statements)
</if>

<elseif/> (else condition) <then/>
    (elseif statements)
<else/>
    (else statements) </if>
```

break

The break instruction stops processing further instructions for the action. This is sometimes helpful to simplify a nested if-block

```
<if>lt r4 0<then/>
    break
</if>

<if>gt r4 10<then/>
    drop "range"
</if>
```

The following instructions can be used to compare registers:

Equality

TABLE 9-5. Equality

INSTRUCTION	TRUE IF
eq	REG == OPERAND
!eq	REG != OPERAND

Signed Comparison

The following instructions perform comparison, treating the register and operand as signed 32-bit quantities:

TABLE 9-6. Signed Comparison

INSTRUCTION	DESCRIPTION
gt	True if REG > OPERAND
!gt	True if REG <= OPERAND
lt	True if REG < OPERAND
!lt	True if REG >= OPERAND

Unsigned Comparison

The following instructions perform comparison, treating the register and operand as unsigned 32-bit quantities:

TABLE 9-7. Unsigned Comparison

INSTRUCTION	DESCRIPTION
ugt	Unsigned: REG > OPERAND
!ugt	Unsigned: REG <= OPERAND
ult	Unsigned: REG < OPERAND

TABLE 9-7. Unsigned Comparison

INSTRUCTION	DESCRIPTION
!ult	Unsigned: REG >= OPERAND

Modulo32 Comparison

The following instructions treat the register and operand as modulo32 quantities. Protocols like TCP use sequence numbers that wrap around across 32-bit boundaries.

TABLE 9-8. Modulo32 Comparison

INSTRUCTION	DESCRIPTION
mlt	Mod32: REG < OPERAND
!mlt	Mod32: REG >= OPERAND
mgt	Mod32: REG > OPERAND
!mgt	Mod32: REG <= OPERAND

Basic Arithmetic Instructions

The arithmetic instructions allow for addition, subtraction, multiplication, division and modulo (remainder) operations:

TABLE 9-9. Basic Arithmetic Instructions

INSTRUCTION	DESCRIPTION
add	REG += OPERAND
sub	REG -= OPERAND
mul	REG *= OPERAND
div	REG /= OPERAND
mod	REG %= OPERAND

Bitwise Instructions

The `bitwise` logical instructions treat the operand and registers as a set of 32 bits:

TABLE 9-10. Bitwise Instructions

INSTRUCTION	DESCRIPTION	
and	REG &= OPERAND	bitwise and
or	REG |= OPERAND	bitwise or
xor	REG ^= OPERAND	bitwise exclusive or
shiftl	REG <<= OPERAND	bitshift left (zero filled)
shiftr	REG >>= OPERAND	bitshift right (zero filled)

Order Of Execution

The DPI Engine analyzes all patterns simultaneously and executes them according to the order of pattern occurrence in the traffic stream. The engine stops processing all rules after a connection is reset, so in the case that there are two rules that might drop a connection, only the first one of these will be executed and the possible effect of the second one is masked.

If two patterns might occur at the same position then the engine will execute the rules in order of definition:

```
<rule pat="goodbye">drop "goodbye"</rule>
<rule pat="bye">drop "bye"</rule>
```

In this example the first defined rule will always execute before the second rule.

If the pattern rules are defined in separate DPI Rules then the order of definition can be controlled through priorities in IDF Server; patterns in higher priorities rules will execute before patterns in lower priorities at the same position.

UDP Pseudo Connections

Rules can be assigned to UDP traffic as well as TCP traffic. UDP traffic is not connection oriented by definition however request-response sequences between the same source/destination IPs and ports can be inspected in a similar way to TCP data. The following differences apply:

- UDP messages are never re-ordered by the DPI engine
- UDP pseudo connections cannot explicitly be reset like TCP

If a rule uses the drop instruction on a UDP pseudo connection, then traffic will be blocked between these endpoints for the UDP timeout period (default 10 seconds).

Web Rules for URIs

Standard Rules can be written to check for access to particular Web server resources. However the same URI can be encoded in many different ways, for example all the following are the same:

```
http://server/index.html
http://server/./index.html
http://server/index%2ehtml
http://server/i%6edex.html
```

The DPI engine provides support for normalizing URIs. This feature is only enabled when the Web Protocol Decoding rules are assigned.

The following pattern rules apply only to URIs after they have been normalized, this rule will match all the above encodings:

```
<uri pat="index">
    log "index"
</uri>
```

It is not necessary to constrain these rules from executing in the HTTP body or header using additional rules. The Web decoding rules take care of tracking the state of the HTTP protocol.

Web Resource and Query Rules

Sometimes it is useful to distinguish between the first part of a URI before a ? and the parameter part following the query. `uri` rules only run on the part of the URI before the ?. To match on parameters use the `uriquery` rule:

```
<uriquery pat="client=firefox">
   log "firefox"
</uriquery>
```

URI parameters can be encoded in the body of an HTTP POST request. `uriquery` rules match the parameters in the post body as well as the part of the URI after the ?.

Considerations for Web Rules

Be careful about mixing `uri` rules with normal rules and using state. URI rules are executed after decoding and normalization of the URI. The URI in the request line is generally not decoded until the full request line, however other rules on the raw traffic can still be executed. If there are patterns that match on the raw request line, then these will generally be triggered before the `uri` rules.

Application Types

The applications defined by Application Types are identified by the direction of traffic, the protocol being used, and the port through which the traffic passes. Application Types are a useful way of grouping DPI Rules. They are used to organize DPI Rules with a common purpose into groups. This simplifies the process of selecting a set of DPI Rules to assign to a computer. For example, consider the set of DPI Rules required to protect HTTP traffic to an Oracle Report Server. By grouping DPI Rules into Application Types it is easy to select rules in the "Web Server Common" and "Web Server Oracle Report Server" sets while excluding, for example, the set of rules that are specific to IIS Servers.

The Application Types screen lists the defined Application Types, along with the following information columns:

Application Type icon:

 Normal Application Types

Application Types that have configuration options

From the main screen you can:

- Define a New ( ) Application Type
- View or edit the Properties ( ) of an existing Application Type
- Duplicate (and then modify) existing Application Types ( )
- Delete ( ) an Application Type

Clicking New (New) or Properties ( ) displays the Application Type Properties window.

To create or edit Application Types:

PATH: IDF MAIN MENU | DEEP PACKET INSPECTION > APPLICATION TYPES

1. Click **New** to create new Application Types from scratch, or select an existing Application Type and click **Properties** ( ) to modify the Application Type.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the Application Type.
   - **Description**: The description of the Application Type.
   - **Minimum Client Plug-in Version**: The minimum version of the IDF Client Plug-in required to implement this Application Type.
3. In the "Connection" area, specify any desired information.
   - **Direction**: The direction of the initiating communication. That is, the direction of the first packet that establishes a connection between two computers. For example, if you wanted to define an Application Type for Web browsers, you would select "Outgoing" because it is the Web browser that sends the first packet to a server to establish a connection (even though you may only want to examine traffic traveling from the server to the browser). The DPI Rules associated with a particular Application Type can be written to examine individual packets traveling in either direction.
   - **Protocol**: The protocol this Application Type applies to.
   - **Port**: The port(s) this Application Type monitors. (Not the port(s) over which traffic is exclusively allowed.)

4. In the **Configuration** tab, you can control how DPI Rules associated with this Application Type behave.

   For example, the "Web Server Common" Application Type has an option to "Monitor responses from Web Server". If this option is deselected, DPI Rules associated with this Application Type will not inspect response traffic over source port 80.

5. In the **Options** tab, you can set how the IDF Server Plug-in uses and applies the Application Type.

   For example, most Application Types have an option to exclude them from Recommendation Scans. This means that if the "Exclude from Recommendations" options is selected, a Recommendation Scan will not recommend this Application Type and its associated DPI Rules for a computer even if the application in question is detected.

6. In the **Assigned To** tab, you can view the DPI Rules associated with this Application Type.

Chapter 10

Components

This chapter describes the Trend Micro™ Intrusion Defense Firewall™ components.

Topics in this chapter:

About Components

Components allow you to create reusable lists for the following:

- **IP Lists**: Reusable lists of IPs.
- **MAC Lists**: Reusable lists of MAC addresses.
- **Port Lists**: Reusable lists of ports.
- **Contexts**: Contexts which specify the circumstances under which a Firewall or DPI Rule is in effect.
- **Schedules**: Reusable schedules.

IP Lists

Use the IP Lists screen to create reusable lists of IP addresses for use by multiple Firewall Rules.

From the main screen you can:

- Create New IP Lists from scratch (New)
- Import () IP Lists from an XML file
- Examine or modify the Properties of an existing IP List ()
- Duplicate (and then modify) existing IP Lists ()
- Delete an IP List ()
- Export () one or more IP lists to an XML file. (Either export them all by clicking the Export... button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking New ( New) or Properties () displays the IP List Properties window.

IP List Properties

To create or edit IP List properties:

PATH: IDF MAIN MENU | COMPONENTS > IP LISTS

1. Click **New** to create new IP List Properties from scratch, or select an existing IP List and click **Properties** () to modify the IP List.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the IP List.
   - **Description**: The description of the IP List.
3. In the "IP(s)" area of the **General** tab, type the IP addresses, masked IP addresses, and IP address ranges that are going to be on your list. Only put one of these per line.

   As well as individual addresses, you can enter IP ranges and masked IPs. Use the examples in the "Supported Formats" area to properly format your entries. (You can insert comments into your IP list by preceding the text with a hash sign ("#").)
4. In the **Assigned To** tab, you can view a list of rules making use of this IP List. Clicking the names of the rules displays their Properties window.

MAC Lists

Use the MAC Lists section to create reusable lists of MAC addresses.

From the main screen you can:

- Create New () MAC lists from scratch
- Import () MAC lists from an XML file
- Examine or modify the Properties of an existing MAC list ()
- Duplicate (and then modify) existing MAC lists ()
- Delete a MAC list ()
- Export () one or more MAC lists to an XML file. (Either export them all by clicking the Export... button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or Properties () displays the **MAC List Properties** window.

MAC List Properties

To create or edit MAC List properties:

PATH: IDF MAIN MENU | COMPONENTS > MAC LISTS

1. Click **New** to create new MAC List Properties from scratch, or select an existing MAC List and click **Properties** () to modify the MAC List.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the MAC List.
   - **Description**: The description of the MAC List.
3. In the "MAC(s)" area, type the MAC addresses that are going to be on your list. Only put one of these per line.

   The MAC(s) list supports MAC addresses in both hyphen- and colon-separated formats. Use the examples in the "Supported Formats" area to properly format your entries. (You can insert comments into your MAC list by preceding the text with a pound sign ("#").)
4. In the **Assigned To** tab, you can view a list of rules making use of this MAC list. Clicking the names of the rules displays their Properties window.

Port Lists

Use the Port Lists screen to create reusable lists of ports.

From the main screen you can:

- Create New port lists from scratch (New)
- Import () port lists from an XML file
- Examine or modify the Properties of an existing port list ()
- Duplicate (and then modify) existing port lists ()
- Delete a port list ()
- Export () one or more port lists to an XML file. (Either export them all by click the Export... button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking New (New) or Properties () displays the Port List properties window.

Port List Properties

To create or edit Port List properties:

PATH: IDF MAIN MENU | COMPONENTS > PORT LISTS

1. Click **New** to create new Port List Properties from scratch, or select an existing Port List and click **Properties** () to modify the Port List.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the Port List.
   - **Description**: The description of the Port List.
3. In the "Ports(s)" area, enter the ports that are going to be on your list. Only put one of these per line.

   For a listing of which ports are used for what, see the Internet Assigned Numbers Authority (IANA).

   Individual ports and port ranges can be included on the list. Use the examples in the "Supported Formats" area to properly format your entries. (You can insert comments into your port list by preceding the text with a pound sign ("#").)
4. In the **Assigned To** tab, you can view a list of rules making use of this port list. Clicking the names of the rules displays their Properties window.

Configuring Port Scan Settings

By default, the range of ports that are scanned is the range known as the "Common Ports", 1-1024, but you can define a different set of ports to scan.

Note: Port 4118 is always scanned regardless of port range settings. It is the port on the computer to which Server Plug-in initiated communications are sent. If communication direction is set to "Client Plug-in Initiated" for a computer (System > System Settings > Computers), port 4118 is closed.

To define a new port range to be scanned:

1. Go to **Components > Port Lists** and click **New** in the menu bar. The **New Port List** screen will appear.
2. Type a name and description for the new port list and then define the ports in the **Port(s)** text box using the accepted formats. (For example, to scan ports 100, 105, and 110 through 120, you would type "100" on the first line "105" on the second, and "110-120" on the third.) Click **OK**.
3. Now go to **System > System Settings > Scan** and click the "Ports to Scan" drop-down menu. Your newly defined Port List will be one of the choices.

Contexts

Contexts are a powerful way of implementing different security policies depending on the computer's network environment.

Contexts are designed to be associated with Firewall and DPI Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied. (To link a Security Rule to a Context, go to the Options tab in the Security Rule's Properties window and select the Context from the "Context" drop-down menu.)

Contexts can be used to provide Client Plug-ins with "location awareness". To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller and connectivity to the internet. Select the "Context applies when Domain Controller connection is: " option and choose from the following:

- **Locally Connected to Domain**: True only if the computer can connect to its domain controller directly
- **Remotely Connected to Domain**: True if the computer can only connect to its domain controller via VPN
- **Not Connected to Domain**: True if the computer cannot connect to its domain controller by any means
- **Not Connected to Domain, No Internet Connectivity:** True if the computer cannot connect to its domain controller by any means and the computer has no Internet connectivity. (The test for Internet connectivity can be configured in **System > System Settings > Contexts**.)

By assessing the ability of the computer to connect with its domain controller or the Internet, the Client Plug-in can then implement rules such as restricting HTTP traffic to non-routable ("private") IP addresses only.

For an example of a Security Profile that implements Firewall Rules using Contexts, examine the properties of the "Location Aware - High" Security Profile.

From the toolbar or the right-click context menu on the Contexts screen, you can:

- Create New (New) Contexts from scratch
- Import ( ) Contexts from an XML file
- Examine or modify the Properties of an existing Context ( )
- Duplicate (and then modify) existing Contexts ( )
- Delete a Context ( )
- Export ( ) one or more Contexts to an XML file. (Either export them all by clicking the Export... button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or **Properties** ( ) displays the Context Properties window.

Context Properties

To create or edit Context properties:

PATH: IDF MAIN MENU | COMPONENTS > CONTEXTS

1. Click **New** to create new Context Rule Properties from scratch, or select an existing Context Rule and click **Properties** ( ) to modify the Context Rule.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the Context Rule.
   - **Description**: The description of the Context Rule.
   - **Minimum Client Plug-in Version**: Shows the earliest version of the IDF Client Plug-in the rule is compatible with.
3. In the "Options" area, configure the following:

- **Context applies when Domain Controller connection is**: Specifying an option here will determine whether or not the Firewall Rule is in effect depending on the ability of the computer to connect to its Domain Controller or its Internet Connectivity. (Conditions for testing Internet Connectivity can be configured in **System > System Settings > Contexts**.)

  If the Domain Controller can be contacted directly (via ICMP), the connection is "Local". If it can be contacted via VPN only, then the connection is "Remote (VPN)".

  The time interval between Domain Controller connectivity test is the same as the Internet Connectivity Test interval which is also configurable in **System > System Settings > Contexts.**

  Note: The Internet Connectivity Test is only performed if the computer is unable to connect to its Domain Controller.

- **Context Applies to Interface Isolation Restricted Interfaces**: This context will apply to network interfaces on which traffic has been restricted through the use of Interface Isolation. (Primarily used for Allow or Force Allow Firewall Rules.)

4. In the **Assigned To** tab, you can view a list of rules making use of this Context.

Schedules

Schedules are rule components used to define when a particular Firewall or DPI rule is in effect. Schedules can also be used to specify when the Server Plug-in can communicate with Client Plug-ins to update a Security Profile.

Other non-rule based Scheduled Tasks such as downloading and applying new Security Updates can be defined from **System > Tasks**.

From the toolbar or the right-click context menu you can:

- Create New schedules from scratch (New)
- Import () schedules from an XML file
- Examine or modify the Properties of an existing schedule ()
- Duplicate (and then modify) existing schedules ()

- Delete a schedule ()
- Export () one or more schedules to an XML file. (Either export them all by clicking the Export... button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** ( New) or **Properties** () displays the Schedule properties window.

Schedule Properties

To create or edit Schedule properties:

PATH: IDF MAIN MENU | COMPONENTS > SCHEDULES

1. Click  **New** to create new Schedule Properties from scratch, or select an existing Schedule and click **Properties** () to modify the Schedule.
2. In the popup window, specify any desired information in "General Information" area of the **General** tab.
   - **Name**: The name of the Schedule.
   - **Description**: The description of the Schedule.
3. Define the schedule. Schedule periods are defined by hour-long time blocks. Clicking a time block selects it, and shift-clicking de-selects it.
4. In the **Assigned To** tab, you can view a list of rules making use of this schedule.

Chapter 11

Managing the IDF Server Plug-in

This chapter describes Trend Micro™ Intrusion Defense Firewall™ server management and configurations.

Topics in this chapter:

Securing the IDF Server Plug-in

Protecting the IDF Server Plug-in with a Client Plug-in

Protect IDF Server Plug-in by installing a Client Plug-in on its computer and apply the **IDF Server Plug-in** Security Profile.

Configuring a Client Plug-in on the IDF Server Plug-in's computer

1. Install an OfficeScan Client on the same computer as the Server Plug-in.
2. Make sure the computer is listed as a "Networked Computer" on the OfficeScan Web console.
3. Go to the **Computers** screen and click the **Synchronize with OfficeScan** button.
4. Double-click the new computer in the **Computers** screen to display its **Details** window and go to **Deep Packet Inspection > SSL Configurations**.
5. A listing of the SSL Configurations for this computer will be displayed. Click **New** to start the wizard to create a new SSL Configuration.
6. Specify the interface used by the Server Plug-in. Click **Next**.
7. On the **Port** screen, choose to protect the port used by the IDF Server Plug-in Web Application GUI over HTTPS. (4119 by default, unless you chose another port during installation. To confirm which port the Server Plug-in is using, check the URL you're using to access it.) Click **Next**.
8. Specify whether SSL DPI analysis should take place on all IP addresses for this computer, or just one. (This feature can be used to set up multiple virtual computers on a single computer.)
9. Next, choose to "Use the SSL Credentials built into the IDF Server Plug-in". (This option only appears when creating an SSL Configuration for the Server Plug-in's computer.) Click **Next**.
10. Finish the wizard and close the **SSL Configuration** screen.
11. Back in the computer's **Details** window, apply the **IDF Server Plug-in** Security Profile which includes the Firewall Rules and DPI Rules required for the IDF Server Plug-in to operate on port 4119.

You have now protected the Server Plug-in's computer and are now filtering the traffic (including SSL) to the Server Plug-in.

Note: After configuring the Client Plug-in to filter SSL traffic, you may notice that the IDF Client Plug-in will return several Renewal Error events. These are certificate renewal errors caused by the new SSL certificate issued by the Server Plug-in computer. You should therefore restart your browser session with the Server Plug-in to acquire the new certificate from the Server Plug-in computer.

The IDF Server Plug-in Security Profile has the basic Firewall Rules assigned to enable remote use of the Server Plug-in. Additional Firewall Rules may need to be assigned if the Server Plug-in's computer is being used for other purposes. The Security Profile also includes the DPI Rules in the Web Server Common Application Type. Additional DPI Rules can be assigned as desired.

Because the Web Server Common Application Type typically filters on the HTTP Port List and does not include port 4119, port 4119 is added as an override to the ports setting in the DPI Rules screen of the Security Profile's Details window.

Upgrading the Server Plug-in

The OfficeScan Plug-in Manager screen will inform you if a new version of the Intrusion Defense Firewall Server Plug-in is available. The new version will be listed above the current version. To upgrade to the new version, click the **Download** button. When the new version has finished downloading, click **Upgrade** to upgrade your Server Plug-in.

Note: Before upgrading the IDF Server Plug-in, make sure that you have already installed the required minimum version of OfficeScan and Plug-in Manager. (See the *Intrusion Defense Firewall Deployment Guide*.)

Migrating To a Larger Database

IDF installs Microsoft SQL Server 2005 to use as its database. SQL Server 2005, with its 4GB limit, may be too small for your needs. The following instructions are for migrating to a larger SQL Server Enterprise database. For assistance with migrating to other supported databases, please contact Trend Micro Support.

Note: Normally you do not have to activate the SQL Browser service, but in some instances you have to switch it on, particularly if you are using the "default" instance. Please refer to the Microsoft page SQL Browser Service.

Note: Remote connection via Windows authentication is not supported. IDF connection to the DB should be either Mixed Mode or SQL Server authentication.

1. Back up the data in question. This can be done via a scheduled task. Go to **System > Scheduled Tasks > New**.
2. Select **Once Only** as the frequency.
3. Choose the Backup task type. e.g. to `"C:\dbbackup"`.
4. Let the task run.
5. Monitor the System Events for the Backup Finished event.
6. When the event shows up, immediately shut down the Intrusion Defense Firewall service in the Windows Services control panel. This will ensure new logs/data are not created after your backup.
7. Find your database backup file e.g. `"C:\dbbackup\IDFBackup.bak"`, and copy the file (or make it available) to the machine where the new database will be saved.
8. Restore the backup. For example, create a new database called "`idf-restore1`". Right-click the file and select **Tasks > Restore...**, then link up the file in the "Devices" area, and chose to **Overwrite Existing Database** on the **Options** tab.

   Note: Your exact settings here may vary.

9. Once the database has been migrated, you need to point your IDF to use the new database. Edit the following file on your IDF server host:

   ```
   C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense
   Firewall\webclient\webapps\ROOT\WEB-INF\dsm.properties
   ```

10. Update the file:

    A simple dsm.properties file looks like this:

    ```
    #Wed Jun 11 16:19:19 EDT 2008
    ```

```
database.SqlServer.user=sa
database.name=IDF
database.directory=null\\
database.SqlServer.password=$1$87251922972564e6bb3e2da9e688c
d4ceb42b9bfb17a942c3c8ad99ff05938c81
database.SqlServer.instance=IDF
mode.demo=false
database.SqlServer.namedPipe=true
database.type=SqlServer
database.SqlServer.server=.
manager.node=1
```

It should be modified to look like this:

```
#Wed Jun 11 16:19:19 EDT 2008
database.SqlServer.user=sa
database.name=idf-restore1
database.directory=null\\
database.SqlServer.password=<cleartext password>
database.SqlServer.instance=
mode.demo=false
database.SqlServer.namedPipe=false
database.type=SqlServer
database.SqlServer.server=bdurie-desktop
manager.node=1
```

Note: Your options may vary, but ensure that if you choose named pipes, the proper windows authentication/trust exists between the IDF Server host and the database host. If you choose TCP, ensure it is enabled on the database.

11. Restart the Intrusion Defense Firewall service on the IDF Server.

Note: Upgrades should work normally and continue to point to the new database instance, but the old database will be retained. It is not necessary to remove the old database, although it could be removed if desired.

Migrating Managed Computers to a New IDF Server

Computers with existing Client Plug-ins can be successfully migrated to another Intrusion Defense Firewall Server without losing their configuration as long as the Client Plug-ins have remained installed and have not been deactivated.

Note: The deactivation instruction (carried out from the Computers screen by right-clicking a Computer and selecting Actions > Deactivate) unbinds the Client Plug-in from the exclusive control of the current Server Plug-in and removes all filters and rules that were in effect.

The migration operation is essentially identical to a Backup and Restore Operation (see *Backing Up and Restoring IDF* on page 11-10) but with the added step of informing the Server Plug-in of its new hostname.

To migrate computers to a new Intrusion Defense Firewall:

1. Perform a Backup operation on the original Intrusion Defense Firewall installation as described in *Backing Up and Restoring IDF* on page 11-10.
2. Install the Intrusion Defense Firewall Server Plug-in onto the new OfficeScan server using the same procedures as described in the Intrusion Defense Firewall installation instructions.
3. Copy the file named `IDFBackup.bak` from Microsoft SQL Server's backup directory (typically `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\IDFBackup.bak`) from the original installation to the new Intrusion Defense Firewall's SQL Server backup directory.
4. Perform a Restore operation as described in *Backing Up and Restoring IDF* on page 11-10.
5. Inform the new restored Intrusion Defense Firewall Server Plug-in of its new hostname by executing the following `idf_c.exe` command from the Intrusion Defense Firewall root directory, replacing "NewComputerName" with the updated hostname. (This can be a static IP or a fully qualified name.)

   ```
   idf_c -action changesetting -name "configuration.dsmUrl"
   -value "NewComputerName"
   ```

   For example, to change the hostname to OfficeScan_Win2K, you would execute:

```
idf_c -action changesetting -name "configuration.dsmUrl"
-value "OfficeScan_Win2K"
```

The new installation of the Intrusion Defense Firewall will detect and recognize the Client Plug-ins from the previous installation and operations will continue as before.

Migrating a Single Managed Computer to a New IDF Server

Single Computers can be migrated to a new Intrusion Defense Firewall but they will not retain any configuration information unless the new Intrusion Defense Firewall Server Plug-in has been "restored" with the backed-up files from the original Intrusion Defense Firewall (see *Backing Up and Restoring IDF* on page 11-10).

To migrate a single computer from one Intrusion Defense Firewall to another:

1. Right-click the computer in the **Computers** screen of the current Server Plug-in and select **Actions > Deactivate Client Plug-in(s)** to deactivate the Client Plug-in.
2. Use the "Move Client" feature of the OfficeScan management console to move the computer to the Server. (Computers listed in the OfficeScan server are automatically listed in the **Computers** screen of the IDF Server Plug-in.)
3. Right-click the computer in the Computers screen of the new IDF Server Plug-in and select **Actions > Activate/Reactivate Client Plug-in(s)** to activate the Client Plug-in.

The Client Plug-in has now been activated by the new Server Plug-in. The old Server Plug-in will no longer be able to communicate with the Client Plug-in.

Optimizing the Embedded Database

The IDF Server Plug-in installs and uses Microsoft SQL Server Express for data storage. The following information will

MS SQL Server Express's 4GB Limitation

It is not possible to increase the database capacity for SQL Server Express, but it is possible to migrate to a database that has no space constraints such as SQL Server database. A set of migration steps have been established. (See *Migrating To a Larger Database* on page 11-3 for instructions.) Contact your support provider for additional assistance.

Archiving the Logs

SQL Server Express's cap GB of data makes it unsuitable for archiving. For audit and compliance requirements, you should periodically backup your database. For information on creating scheduled backups, see *Backing Up and Restoring IDF* on page 11-10.

Minimizing the Space Used by the Database

IDF Server stores events in the database and automatically purges events when they reach a certain age. The maximum age of these events is fully configurable from IDF Server. This allows an administrator to tune how long they want to keep certain types of events in IDF Server, and hence allows an administrator to effectively tune how their database space is utilized.

Prune settings are configured in IDF Server by going to **System > System Settings**, selecting the **System** tab, and then editing the settings within the "Prune" section. Changes to these settings are effective immediately, but it will take IDF Server up to an hour to do the actual pruning, as it is done every hour.

To decide what prune settings would benefit from being shortened, you can use a SQL Server database tool to inspect your database and find out which tables are taking up the majority of the space:

http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en

If you intend to use the tool indicated above, install it on the IDF Server host, launch the tool and login to the IDF instance, expand the "IDF" database, view the tables, and then fetch the properties of the tables listed below to determine their size. Considering

that SQL Server Express has a maximum size of 4GB, you should consider any table below that is over 1GB to be "too large", and its pruning settings should be lowered if possible.

The following tables are included in the "Firewall/DPI events" prune settings:

`packetlogs`

`payloadlogs`

`payloadlogdatas`

The following tables are included in the "system/client plug-in events" prune settings:

`systemevents`

`agentevents`

The following tables are included in the "counters" prune settings:

`counter3s`

`counter3ports`

`counter3ips`

Shrinking the Size of the IDF Database

SQL Server Express database by default has a maximum data capacity of 4GB, but its database log file (IDF_Log.mdf) can grow as large as needed. In some extreme cases it can grow up to the size of the main database file (4GB).

In some situations it may be helpful to shrink the database so it consumes less actual disk space.

The only way to perform this operation on the IDF database is by using a SQL Server tool. This can be done using the SQL Server Express Management tool, or via a similar command line tool – both tools are provided free from Microsoft:

`http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en`

`http://www.microsoft.com/DownLoads/details.aspx?familyid=FA87E828-173F-472E-A85C-27ED01CF6B02&displaylang=en`

After installing the command-line tool on the IDF Server machine, the following command will shrink the database:

```
sseutil –shrink name=IDF –server .\IDF –m
```

Usually the shrink is performed on the logical logs. They grow more rapidly than the database and sometimes are not flushed.

To release logical log space:

1. Perform a full backup.
2. Perform logical logs backup.
3. Run the following two SQL queries to release the space:

```
USE idf
GO
Checkpoint
USE idf
DBCC SHRINKFILE(idf_log, 1)
BACKUP LOG WITH TRUNCATE_ONLY
DBCC SHRINKFILE(idf_log, 1)
```

Note: Another option, discouraged by Microsoft but still technically an option to keep the files small, is to switch the IDF database into "Auto-Shrink" mode. You can do this using the latter GUI tool mentioned above by selecting the **Databases->IDF** node, right-click and select **Properties**, choose **Options**, and then configuring the "Auto Shrink" mode to be "True".

Migrating IDF Data To Another Database

A set of migration steps have been established (see *Migrating To a Larger Database* starting on page 11-3. Contact your support provider team for additional assistance.

Backing Up and Restoring IDF

Intrusion Defense Firewall uses Microsoft SQL Server Express as its database. The database stores all the Intrusion Defense Firewall data:

- All Logs and Events
- Security Profiles

- IPS Filters
- Firewall Rules
- Stateful Configurations
- All Components (IP Lists, MAC Lists, Port Lists, etc.)
- Alert Configurations
- System Settings
- The configurations of the Client Plug-ins on all Computers

Note: Intrusion Defense Firewall can always restore the first eight of these items to any OfficeScan Server, but to restore #9, "The configurations of all Client Plug-ins on all Computers", the OfficeScan Server must have the same list of Networked Computers with the same OfficeScan-generated unique IDs as it did when the Intrusion Defense Firewall backup was executed. If that is the case, the Server Plug-in will push out the backed up Security Profiles (any other elements) out to the Client Plug-ins during the next Update operation and the Client Plug-ins will be in the same state with the same configuration they were in at the time of the backup.

If the OfficeScan Server has had to re-populate its Networked Computers list from scratch (and therefore assigned new unique IDs to each Computer), the Server Plug-in has no way of recognizing the Computers and will not be able to restore their previous configurations.

Backup

To schedule regular database backups, go to **System > Scheduled Tasks** and click **New** in the toolbar to start the Scheduled Task Wizard. Select **Backup** from the drop-down list and then use the next two screens to specify how often you want a backup to be performed. When you are prompted for the output location, specify the SQL Server backup directory which is typically located at:

```
C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\
```

The next step of the Wizard will prompt you to name the new Scheduled Task and give you the option to run task after closing the Scheduled Task Wizard.

Backups are stored in a single SQL Server backup file named `IDFBackup.bak`. Each time a backup is performed, data is added to the backup file. Each backup "instance" that is added to the backup file will be retained in the backup file for 15 days, after which that backup "instance" will be overwritten the next time a backup is performed.

Restore

To restore from the last backup:

1. Stop the "Intrusion Defense Firewall" service from the Services Microsoft Management Console snap-in.
2. Run `IDFRestore.bat` from the Intrusion Defense Firewall root directory (typically `C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall`).
3. Start the "Intrusion Defense Firewall" service.

When restoring, `IDFRestore.bat` will attempt to restore from `IDFBackup.bak` found in the SQL Server backup directory.

Modifying Backup and Restore Options

Backup

Intrusion Defense Firewall comes with a file called `IDFBackup.bat` which can be used to perform backups manually. It is located in the Intrusion Defense Firewall root directory (`C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall`).

Use IDFBackup.bat if you want to modify the directory where backups are stored, the name of the backup file, or the number of days that backups are kept (15 days by default).

To change the directory where backup files will be stored, or to change the number of days that a backup "instance" should be retained you will need to edit `IDFBackup.bat` in a text editor.

The `backUpFile` parameter specifies the file name and location of the backup file. The `retainDays` parameter specifies the number of days a backup "instance" should be retained for.

For example, to change the backup file to `C:\IDF Backups\MyIDFBackup.bak`, and the number of days to 7, you would make the following changes to `IDFBackup.bat`:

```
CALL sqlcmd -S localhost\IDF -E -v backUpFile="C:\IDF
Backups\MyIDFBackup.bak" retainDays=7 -i "IDFBackup.sql"
```

Note: The directory in which backups will be stored must already exist prior to running the backup. For the above example that would be C:\IDF Backups\

Setting Up Scheduled Backups Using IDFBackup.bat

To schedule regular backups using IDFBackup.bat, a Windows scheduled task will need to be created. Windows Scheduled Tasks can be accessed from the Control Panel within Windows.

When creating the scheduled backup task, you will need to select IDFBackup.bat as the program you want Windows to run. This will require browsing to the Intrusion Defense Firewall root directory (typically `C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall`). Within the Windows Scheduled Task Wizard, you can select the time and frequency you want the backup to run.

Restore

To change the directory and file from which backups will restored, you will need to edit `IDFRestore.bat` in a text editor. The `backUpFile` parameter will need to be changed.

For example, to change the backup file to `C:\IDF Backups\MyIDFBackup.bak`, you would make the following changes to `IDFRestore.bat`:

```
CALL sqlcmd -S localhost\IDF -E -v backUpFile="C:\IDF
Backups\MyIDFBackup.bak" -i "IDFRestore.sql"
```

Uninstalling the Server Plug-in

From the OfficeScan Plug-In Manager click **Uninstall** in the Intrusion Defense Firewall panel.

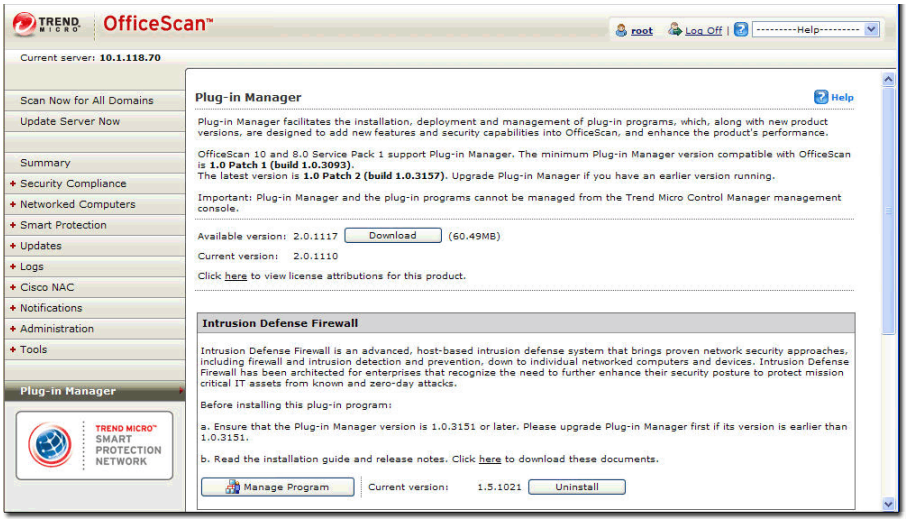


FIGURE 11-1. Uninstall Server Plug-in

Note: The IDF Server Plug-in cannot be uninstalled using the Control Panel Add or Remove Programs applet.

Chapter 12

System

This chapter describes how to monitor and manage the Trend Micro™ Intrusion Defense Firewall™ System.

Topics in this chapter:

About the System

The System screen allows you to manage all of the following:

- **System Events**: Use the System Events screen to examine system-related events (as opposed to security-related events).
- **System Settings**: The Settings section lets you control the administration of the IDF system.
- **Tags**: All currently defined tags are displayed in the Tags screen.
- **Tasks**: The Tasks section provides the ability to configure recurring automated and event-based tasks.
- **License**: The license page displays details about your Trend Micro product license such as which IDF Modules are available and how many computers you are licensed to install Client Plug-in software on.
- **Updates**: The Updates section allows you to manage security and software updates.

Viewing System Events

The System Events screen lists the System Event log, which is a record of system-related events (as opposed to security-related events). For a list of possible System Events, see *System Events* on page C-8. The System Event screen displays the following information for each event:

- **Time**: The time according to the system clock on the computer hosting the IDF Server Plug-in.
- **Level**: The severity level of event that occurred. Event levels include Info, Warning, and Error.
- **Event ID**: The event type's unique identifier.
- **Event**: The name of the event (associated with the event ID.)
- **Target**: The system object associated with the event will be identified here. Clicking the object's identification will display the object's properties sheet.
- **Event Origin**: The source of the event.
- **Action By**: The user who initiated the event, if initiated by a user.
- **Server Plug-in**: The hostname of the IDF Server Plug-in computer.

From the main screen you can:

- **View** ( ) the details (properties) of a system event
- **Search** ( ) for a particular system event
- **Export** ( ) currently displayed system events to a CSV file

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s)**: Add an Event Tag to this event (see *Event Tagging* on page 12-4)
- **Remove Tag(s)**: Remove exiting Event Tags

To view details for a system event:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM EVENTS

1. Select an event and click **View** ( ) to display the Event Viewer Properties window.
2. In the "General Information" area, you can view information about the selected event.
3. In the "Description" area, the specific details of what action was performed to trigger this entry in the system event log will be displayed here, if appropriate.
4. Click the **Tags** tab to display tags that have been attached to this Event.

   To view more tag information, see **System > System Settings > Tags**. For information on tagging events, see *Event Tagging* on page 12-4.

Filtering the List and Searching for an Event

The Period toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The Computers toolbar lets you organize the display of event log entries by computer domain or computer Security Profiles.

Clicking **Advanced Search** toggles the display of the search bar.

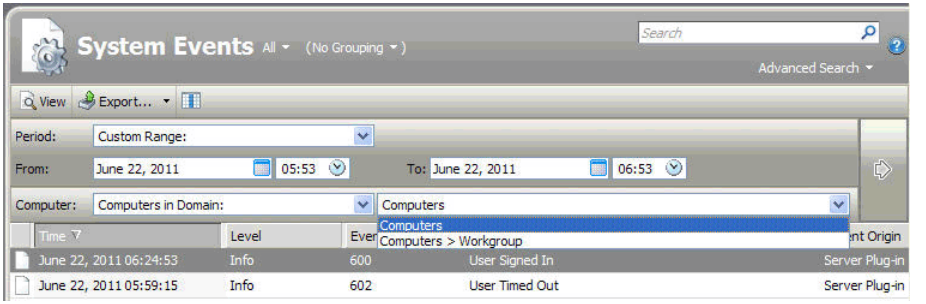


FIGURE 12-1. Computers Toolbar

Pressing the "Add Search Bar" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the "Submit Request" button (at the right of the toolbars with the right-arrow on it).

Exporting Events

You can export displayed events to a CSV file. (Paging is ignored, all pages will be exported.) You have the option of displaying the displayed list or the selected items.

Event Tagging

Event Tagging allows administrators to manually tag events with custom labels ("Assigned to Tom for review", etc.).

In addition to the manual tagging of events, automated event tagging can be accomplished via the use of a "Reference Computer". For example, a planned rollout of a patch can be applied to the reference computer, the events associated with the application of the patch can be tagged as "Patch X", similar events raised on other systems can automatically be deemed to be "acceptable changes" and suppressed to reduce the number of events subjected to scrutiny by an administrator.

Event tagging enables specialized views of events, dashboards, and reports and can be applied to a single event, similar events, or even to all future similar events.

Tagging Events

Event Tagging allows you to manually tag System Events with custom labels ("Assigned to Tom for review", etc.). Event tagging enables specialized views of events, dashboards, and reports and can be applied to a single event, similar events, or even to all future similar events.

To apply a tag to one or more selected Events:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM EVENTS

1. Select the events in the **Events** list, then right-click and select **Add Tag(s)...**.
2. Type a name for the tag. (IDF Server Plug-in will suggest matching names of existing tags as you type.)
3. Select **1 Selected System Event**. (If you selected multiple events from the Events list, the number of selected events will be displayed.) Click **Next**.
4. Enter some optional comments and click **Finish**.

Looking at the Events list, you can see that the Event has now been tagged.

To tag multiple similar Events:

1. Right-click on a representative event from the **Events** list and select **Add tag(s)...**.
2. Type a name for the tag. (IDF Server Plug-in will suggest matching names of existing tags as you type.)
3. Select **Also apply to similar System Events**. Click **Next**.
4. Select which attributes will be examined to determine whether Events are similar or not. For the most part, the attribute options are the same as the information displayed in the columns of the Events list screen. When you have selected which attributes to include in the Event selection process, click **Next**.
5. Select what type of similar System Events should this rule be applied to.

Note: Notice the Save Auto-Tag Rule option. The selection criteria you have specified can be saved so that you can apply them again at a future date when new events have accumulated. Saved auto-tag rules can be found in the System > Tags screen.

---

6. Click **Next**.
7. Enter some optional comments and click **Next**.

8. Review the Summary of your Event selection criteria and click **Finish**.

Looking at the Events list, you can see that your original Event and all similar Events have been tagged.

To tag multiple similar Events as well as future similar Events:

The procedure for tagging multiple similar as well as future Events is the same as above except for step 5, where you also select **New System Events**. Selecting **New System Events** causes the IDF Server Plug-in to scan its database every five seconds (or more) for new Events and tag the appropriate ones.

Note: Tagging only occurs after Events have been retrieved from the Client Plug-ins to the IDF Server Plug-in's database.

System Settings

The **System > System Settings** screen lets you control the administration of the IDF system. This section is for managing system configuration settings such as session timeouts, system alerts, communications between Client Plug-ins and the Server Plug-in, heartbeat settings, etc.

Note: The Settings screen has a Save button at the bottom right. Changes made to these settings (all tabs) must be saved before they take effect.

- Computers
- Firewall and DPI
- Interface Isolation
- Contexts
- Reconnaissance Scan
- Notifications
- Ranking
- Updates
- System

Computers

To configure computer settings:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Computers** tab, if it is not already open.
2. In the "Communication Direction" area, select one of the following:
   - **Bidirectional**: By default, communications are bi-directional. This means that the Client Plug-in normally initiates the heartbeat but still listens on the Client Plug-in port for Server Plug-in connections. The Server Plug-in is still free to contact the Client Plug-in in order to perform operations as required. This allows the Server Plug-in to apply changes to the security configuration to the Client Plug-in as they occur.
   - **Server Plug-in Initiated**: With this option selected, all Server Plug-in to Client Plug-in communications are initiated by the Server Plug-in. This includes security configuration updates, heartbeat operations, and requests for Event logs.
   - **Client Plug-in Initiated**: With this option selected, the Client Plug-in does not listen on port 4118. Instead it contacts the Server Plug-in on the heartbeat port (4120 by default) as dictated by the heartbeat settings. Once the Client Plug-in has established a TCP connection with the Server Plug-in all normal communication takes place: the Server Plug-in first asks the Client Plug-in for its status and for any events. (This is the heartbeat operation). If there are outstanding operations that need to be performed on the computer (e.g., the Security Profile needs to be updated), these operations are performed before the connection is closed. In this mode, communications between the Server Plug-in and the Client Plug-in only occur on every heartbeat. If a Client Plug-in's security configuration has changed, it will not be updated until the next heartbeat.

Note: Client Plug-ins look for the IDF Server Plug-in on the network by the Server Plug-in's hostname. Therefore the Server Plug-in's hostname must be in your local DNS for Client Plug-in initiated or bidirectional communication to work.

To enable communications between the Server Plug-in and the Client Plug-ins, the Server Plug-in automatically implements a (hidden) Firewall Rule (priority four,

Bypass) which opens port 4118 on the Client Plug-ins to incoming TCP/IP traffic. The default settings open the port to any IP address and any MAC address. You can restrict incoming traffic on this port by creating a new priority 4, Force Allow or Bypass Firewall Rule, which only allows incoming TCP/IP traffic from specific IP and/or MAC addresses. This new Firewall Rule will replace the hidden Firewall Rule if the settings match the following:

- **action**: force allow or bypass
- **priority**: 4 - highest
- **packet's direction**: incoming
- **frame type**: IP
- **protocol**: TCP
- **packet's destination port**: 4118 (or a list or range that includes 4118)

As long as these settings are in effect, the new rule will replace the hidden rule. You can then type Packet Source information for IP and/or MAC addresses to restrict traffic to the computer.

3. In the "Hostnames" area, choose whether to update the "Hostname" entry if an IP is used as a hostname and a change in IP is detected on the computer after Client Plug-in-initiated communication or discovery: Turn this option on if, for example, your network has no DNS and you are using dynamic IPs. (IDF Server Plug-in always identifies computers/Client Plug-ins by their unique fingerprint, not their IP addresses.)
4. In the "Remote Activation" area, choose whether to enable Remote Activation.

   The default process of installing and activating a Client Plug-in on a computer is as follows: the Client Plug-in is installed on a computer and then a user uses the IDF Server Plug-in to "activate the Client Plug-in". This activation sends a unique encrypted fingerprint from the Server Plug-in to the Client Plug-in. The Client Plug-in now knows not to accept any instructions not identified as coming from the Server Plug-in by that fingerprint. There may be circumstances, however, where it is desirable for the activation to be initiated by the Client Plug-in rather than by the Server Plug-in. (Large, distributed installations, for example.) In this case the Server Plug-in must be configured to allow Client Plug-ins to communicate with it and initiate activation. Use the Remote Activation panel to set restrictions on which computers can initiate their own Client Plug-in activations.

Client Plug-in initiated activation is performed from the command-line. The following are the Client Plug-in's activation-related command-line options:

TABLE 12-1. Client Plug-in's activation-related command-line options

USAGE: DSA_CONTROL [/A <STR>] [/G <STR>] [/C <STR>] [/R]	
/a <str>	Activate Client Plug-in with IDF Server at specified URL. URL format must be "dsm://hostOrIp:port/" "port" is the Server Plug-in's Heartbeat port. (4120 by default.)
/g <str>	Client Plug-in URL. Defaults to "https://127.0.0.1:4118/"
/c <str>	Certificate file
/r	Reset Client Plug-in configuration

Note: You can instruct IDF Server Plug-in to send a default Security Profile to self-activating Client Plug-ins which do not already have a Security Profile assigned to them. Use the Security Profile to assign (when no Security Profile is currently assigned) to select a Security Profile.

5. In the "Heartbeat" area, set the following options:
   - **Heartbeat Interval (in minutes)**: How much time passes between heartbeats.
   - **Number of Heartbeats that can be missed before an alert is raised**: Several missed heartbeats in a row may indicate a problem with the Client Plug-in or the computer. This setting determines how many missed heartbeats are allowed to go by before the Server Plug-in triggers an alert. (For example, entering three will cause the Server Plug-in to trigger an alert on the fourth missed heartbeat.)
   - **Maximum change (in minutes) of the local system time on the computer between heartbeats before an alert is raised**: For Client Plug-ins that are capable of detecting changes to the system clock (Windows Client Plug-ins) these events are reported to the Server Plug-in as Client Plug-in Event 5004. If the change exceeds the clock change listed here then an alert is triggered. For

Client Plug-ins that do not support this capability (non-Windows Client Plug-ins), the Server Plug-in monitors the system time reported by the Client Plug-in at each heartbeat operation and will trigger an alert if it detects a change greater than the permissible change specified in this setting.

Note: Once a Computer-Clock-Changed alert is triggered, it must be dismissed manually.

6. In the "Automatically Update Computers" area, specify whether to automatically update computers.

   By default, any time you make a change to any element in the IDF system, all affected computers are immediately updated. For example, if you edit a port list, all computers already making use of that port list will get updated immediately. (If you make such a change and then look at the Computers screen, you will see the updates happening.) Not setting the Automatically update all affected computers after changing any aspect of the IDF System option means that after any changes, you will have to find affected computers on the Computers screen, right-click them and choose **Update Client Plug-in(s) Now** from the context menu.

   Note: This applies to Security Updates as well. If a Security Update includes, for example, an updated port list for Oracle servers, the updated port list will be deployed to all computers currently making use of that port list unless you have selected the manual option.

Firewall and DPI Settings

To configure Firewall and DPI settings:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Firewall and DPI** tab.
2. In the "Network Engine Mode" area, choose whether the Client Plug-in's network engine can operate Inline or in Tap Mode.

   When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that DPI Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In

Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.

3. In the "Events" area, configure events as follows:

   You can set the maximum size of each individual log file and how many of the most recent files are kept. Event log files will be written to until they reach the maximum allowed size, at which point a new file will be created and written to until it reaches the maximum size and so on. Once the maximum number of files is reached, the oldest will be deleted before a new file is created. Event log entries usually average around 200 bytes in size and so a 4MB log file will hold about 20,000 log entries. How quickly your log files fill up depends on the number of rules in place.

   - **Maximum size of the event log files (on Client Plug-in)**: Adjust these settings if you begin to see "Insufficient Disk Space" alerts for one or more computers.
   - **Number of event log files to retain (on Client Plug-in)**: Adjust these settings if you begin to see "Insufficient Disk Space" alerts for one or more computers.
   - **Collect Firewall Events from Client Plug-in**: Retrieve the latest Firewall Events from the Client Plug-in at every Heartbeat.
   - **Collect DPI Events from Client Plug-in**: Retrieve the latest DPI Events from the Client Plug-in at every Heartbeat.

   Note: Events are records of individual events. Counters are a record of the number of times individual events have occurred. Events are used to populate the Events screens. Counters are used to populate the Dashboard Widgets (number of Firewall Events over the last 7 days, etc.) and the Reports. You might want to collect only counters if, for example, you are using syslog for event collection; events can potentially take up a lot of disk space and you may not want to store the data twice.

   - **Do Not Record Events with Source IP of**: This option is useful if you want IDF to not make record Events for traffic from certain trusted computers.

Note: The following three settings let you fine tune Event aggregation. To save disk space, IDF Client Plug-ins will take multiple occurrences of identical events and aggregate them into a single entry and append a "repeat count", a "first occurrence" timestamp, and a "last occurrence" timestamp. To aggregate event entries, IDF Client Plug-ins need to cache the entries in memory while they are being aggregated before writing them to disk.

- **Cache Size**: Determines how many types of events to track at any given time. Setting a value of 10 means that 10 types of events will be tracked (with a repeat count, first occurrence timestamp, and last occurrence timestamp). When a new type of event occurs, the oldest of the 10 aggregated events will be flushed from the cache and written to disk.
- **Cache Lifetime**: Determines how long to keep a record in the cache before flushing it to disk. If this value is 10 minutes and nothing else causes the record to be flushed, any record that reaches an age of 10 minutes gets flushed to disk.
- **Cache Staletime**: Determines how long to keep a record whose repeat count has not been recently incremented. If Cache Lifetime is 10 minutes and Cache Staletime is two minutes, an event record which has gone two minutes without being incremented will be flushed and written to disk.

Note: Regardless of the above settings, the cache is flushed whenever Events are sent to the IDF Server Plug-in.

- **Generate Firewall Events for packets that are "Out Of Allowed Policy"**: Select whether you wish to log packets that are dropped because they have not been specifically permitted by an Allow rule or Firewall Rule. (Note that turning this option on can significantly increase the size of your log files.
- **Allow DPI Rules to capture data for the first hit of each rule (in period)**: Keep the data from the packet that triggered a log entry. (The packet's data can be viewed with the log entry. Each rule will only capture data once in a five second period to avoid unduly large log files.)

4. In the "Advanced" area, configure the **Use Custom Driver Settings**:
   - **CLOSED timeout**: For gateway use. When a gateway passes on a **"**hard close**"** (RST), the side of the gateway that received the RST will keep the connection alive for this amount of time before closing it.

- **SYN_SENT Timeout**: How long to stay in the SYN-SENT state before closing the connection.
- **SYN_RCVD Timeout**: How long to stay in the SYN_RCVD state before closing the connection.
- **FIN_WAIT1 Timeout**: How long to stay in the FIN-WAIT1 state before closing the connection.
- **ESTABLISHED Timeout**: How long to stay in the ESTABLISHED state before closing the connection.
- **ERROR Timeout**: How long to maintain a connection in an Error state. (For UDP connections, the error can be caused by any of a variety of UDP problems. For TCP connections, the errors are probably due to packets being dropped by the firewall.)
- **DISCONNECT Timeout**: How long to maintain idle connections before disconnecting.
- **CLOSE_WAIT Timeout**: How long to stay in the CLOSE-WAIT state before closing the connection.
- **CLOSING Timeout**: How long to stay in the CLOSING state before closing the connection.
- **LAST_ACK Timeout**: How long to stay in the LAST-ACK state before closing the connection.
- **ACK Storm timeout**: The maximum period of time between retransmitted ACKs within an ACK Storm. In other words, if ACKs are being retransmitted at a lower frequency then this timeout, they will NOT be considered part of an ACK Storm.
- **Boot Start Timeout**: For gateway use. When a gateway is booted, there may already exist established connections passing through the gateway. This timeout defines the amount of time to allow non-SYN packets that could be part of a connection that was established before the gateway was booted to close.
- **Cold Start Timeout**: Amount of time to allow non-SYN packets that could belong to a connection that was established before the stateful mechanism was started.
- **UDP Timeout**: Maximum duration of a UDP connection.
- **ICMP Timeout**: Maximum duration of an ICMP connection.

- **Allow Null IP**: Allow or block packets with no source and/or destination IP address.
- **Block IPv6**: Block or Allow IPv6 packets. (DPI Filtering of IPv6 traffic is not supported. It can only be blocked or allowed.)
- **Connection Cleanup Timeout**: Time between cleanup of closed connections (see next).
- **Maximum Connections per Cleanup**: Maximum number of closed connections to cleanup per periodic connection cleanup (see previous).
- **Block Same Src-Dest IP Address**: Block or allow packets with same source and destination IP address. (Doesn't apply to loopback interface.)
- **Maximum TCP Connections**: Maximum simultaneous TCP Connections.
- **Maximum UDP Connections**: Maximum simultaneous UDP Connections.
- **Maximum ICMP Connections**: Maximum simultaneous ICMP Connections.
- **Maximum Events per Second**: Maximum number of events that can be written per second.
- **TCP MSS Limit**: The MSS is the Maximum Segment Size (or largest amount of data) that can be sent in a TCP packet without being fragmented. This is usually established when two computers establish communication. However, in some occasions, the traffic goes through a router or switch that has a smaller MSS. In this case the MSS can change. This causes retransmission of the packets and the Client Plug-in logs them as "Dropped Retransmit". In cases where there are large numbers of Dropped Retransmit event entries, you may wish to lower this limit and see if the volume is reduced.
- **Number of Event Nodes**: The maximum amount of kernel memory the driver will use to store log/event information for folding at any one time.

Note: Event folding occurs when many Events of the same type occur in succession. In such cases, the Client Plug-in will "fold" all the events into one.

- **Ignore Status Code**: This option lets you ignore certain types of Events. If, for example, you are getting a lot of "Invalid Flags" you can simply ignore all instances of that Event.
- **Ignore Status Code**: Same as above.

- **Ignore Status Code**: Same as above.
- **Advanced Logging Policy**:
  - **Bypass: No filtering of Events**. Overrides the **"**Ignore Status Code**"** settings (above) and other advanced settings, but does not override logging settings defined in the IDF Server Plug-in. For example, if Stateful Configuration logging options set from a Stateful Configuration Properties window in the IDF Server Plug-in will not be affected.
  - **Default**: Will switch to **"**Tap Mode**"** (below) if the engine is in Tap Mode, and will switch to "Normal" (above) if the engine is in Inline Mode. Normal: All Events are logged except dropped retransmits.
  - **Backwards Compatibility Mode**: For support use only.
  - **Verbose Mode**: Same as **"**Normal**"** but including dropped retransmits.
  - **Stateful and Normalization Suppression**: Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, unsolicited udp, unsolicited ICMP, out of allowed policy.
  - **Stateful, Normalization, and Frag Suppression**: Ignores everything that "Stateful and Normalization Suppression" ignores as well as events related to fragmentation.
  - **Stateful, Frag, and Verifier Suppression**: Ignores everything **"**Stateful, Normalization, and Frag Suppression" ignores as well as verifier-related events.
  - **Tap Mode**: Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, max ack retransmit, packet on closed connection.

Note: For a more comprehensive list of which Events are ignored in Stateful and Normalization Suppression; Stateful, Normalization, and Frag Suppression; Stateful, Frag, and Verifier Suppression; and Tap modes, see *Advanced Logging Policy Modes* on page 13-19.

- **Silent TCP Connection Drop**: When Silent TCP Connection Drop is on, a RST packet is only sent to the local stack. No RST packet is sent on the wire. This reduces the amount of information sent back to a potential attacker.

Note: If you enable the Silent TCP Connection Drop you must also adjust the DISCONNECT Timeout. Possible values for DISCONNECT Timeout range from 0 seconds to 10 minutes. This must be set high enough that the connection is closed by the application before it is closed by the IDF Client Plug-in. Factors that will affect the DISCONNECT Timeout value include the operating system, the applications that are creating the connections, and network topology.

- **Enable Debug Mode**: When in debug mode, the Client Plug-in captures a certain number of packets (specified by the setting below: Number of Packets to retain in Debug Mode). When a rule is triggered and debug mode is on, the Client Plug-in will keep a record of the last X packets that passed before the rule was triggered. It will return those packets to the Server Plug-in as Debug Events.

Note: Debug mode can very easily cause excessive log generation and should only be used under Client Services supervision.

- **Number of Packets to retain in Debug Mode**: The number of packets to retain and log when debug mode is on.
- **Log All Packet Data**: All internally defined logs (i.e., not FW/DPI/verifier) which have not been aggregated will attach the full packet data to their log. This and the following two settings are equivalent to the matching DPI and FW log settings.
- **Log only one packet within period**: If the above is not set, but this is set, then most logs will only contain the header data with a full packet being attached only periodically.
- **Period for Log only one packet within period**: The period between when full packet data will be logged if the above is set.
- **Maximum data size to store when packet data is captured**: The maximum size of header or packet data to be attached to a log.
- **Generate Connection Events for TCP**: Generates a Firewall Event every time a TCP connection is established.
- **Generate Connection Events for ICMP**: Generates a Firewall Event every time an ICMP connection is established.

- **Generate Connection Events for UDP**: Generates a Firewall Event every time a UDP connection is established.
- **Bypass CISCO WAAS Connections**: This mode bypasses stateful analysis of TCP sequence numbers for connections initiated with the proprietary CISCO WAAS TCP option selected. This protocol carries extra information in invalid TCP Sequence and ACK numbers that interfere with stateful firewall checks. Only enable this option if you are using CISCO WAAS and you are seeing connections with Invalid SEQ or Invalid ACK in the firewall logs. When this option is selected, TCP stateful sequence number checks are still performed for non WAAS enabled connections.
- **Drop Evasive Retransmit**: Incoming packets containing data that has already been processed will be dropped to avoid possible evasive retransmit attack techniques.
- **Verify TCP Checksum**: The segment's checksum field data will be used to assess the integrity of the segment.
- **Minimum Fragment Offset**: Defines the minimum acceptable IP fragment offset. Packets with offsets less than this will be dropped with reason "IP fragment offset too small". If set to 0 no limit is enforced. (default 60)
- **Minimum Fragment Size**: Defines the minimum acceptable IP fragment size. Fragmented packets that are smaller than this will be dropped with reason "First fragment too small" as potentially malicious. (default 120)
- **Fragment Timeout**: How long to keep fragmented packets.
- **Maximum number of fragmented IP packets to keep**: If configured to do so, the DPI Rules will edit the content of a packet (or packet fragment) if that content is considered suspicious. This setting determines how long after editing to wait for the remaining packet fragments before discarding the packet.
- **Send ICMP to indicate fragmented packet timeout exceeded**: Whether not to indicate to remote computer with an ICMP packet that a connection timeout has been exceeded.

Interface Isolation Settings

Interface Isolation allows you to force a computer to use only one interface at any one time. This feature was designed to prevent attackers from bridging across two interfaces.

To configure Interface Isolation settings:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Interface Isolation** tab.
2. In the "Interface Isolation" area, choose whether to enable Interface Isolation.
3. In the enforce interface isolation, in the "Interface Patterns" area, enter string patterns that will match the names of the interfaces on a computer (in order of priority). You can use standard regular expression syntax when creating your list of interfaces.

Note: If you enter a string pattern that matches more than one interface on a computer, then traffic will be allowed on all of those matching interfaces. To make sure that only one interface is active, set the Limit to one active interface option.

Note: This is an option you may not want to set at the global level, but at more granular levels for particular Security Profiles or computers only. To do this, set the global settings to not enforce interface isolation and then override the setting on the Security Profile or the computer. For more information on overriding settings, see *Inheritance and Overrides* on page 6-28.

Contexts Settings

Contexts determine whether a protected computer has Internet connectivity or not. Some IDF Rules can be applied conditionally depending on the computer's network connectivity conditions. This is known as "Location Awareness". The Internet connectivity condition options for a particular rule can be configured on the Options tab of the rule's Properties window. The Internet Connectivity Test can also be used when implementing Interface Isolation. (See *Contexts Settings* on page 12-18.)

To configure Contexts settings:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Contexts** tab.
2. In the "Internet Connectivity Test" area, configure the following options:

- **URL for testing Internet Connectivity Status**: The URL to which an HTTP request will be sent to test Internet Connectivity. (You must include "http://".)
- **Regular Expression for returned content used to confirm Internet Connectivity Status**: A regular expression which will be applied to the returned content to confirm that HTTP communication was successful.
- **Test Interval**: The time interval between connectivity tests.

Reconnaissance Settings

The Reconnaissance screen allows you to enable and configure traffic analysis settings on all or selected computers.

For each type of attack, the Client Plug-in can be instructed to send the information to the IDF Server Plug-in where an alert will be triggered. You can configure the Server Plug-in to send an email notification when the alerts are triggered. (Go to **System > System Settings > Notifications**. The Alerts are: **"**Network or Port Scan Detected**"**, "Computer OS Fingerprint Probe Detected", "TCP Null Scan Detected", "TCP FIN Scan Detected", and "TCP Xmas Scan Detected.") Select **Notify IDF Server Immediately** for this option. For more information on Notifications, see *Notifications Settings* on page 12-21.

Note: Stateful Inspection must be on and TCP and UDP Logging enabled for Reconnaissance protection to function. Stateful Inspection and logging can be enabled in the **Firewall > Stateful Configurations** screen.

Once an attack has been detected, you can instruct the Client Plug-ins to block traffic from the source IPs for a period of time. Use the Block Traffic drop-down lists to set the number of minutes.

"Computer OS Fingerprint Probe" and "Network or Port Scans" differ from the other three types of reconnaissance in that they cannot be recognized by a single packet.

The Client Plug-in reports a computer or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally a Client Plug-in computer will only see traffic destined for itself, so a port scan is by far the most common type of probe that will be detected. However, if a computer is acting as a router or bridge it could see

traffic destined for a number of other computers, making it possible for the Client Plug-in to detect a computer scan (ex. scanning a whole subnet for computers with port 80 open).

Detecting these scans can take several seconds since the Client Plug-in needs to be able to track failed connections and decide that there are an abnormal number of failed connections coming from a single computer in a relatively short period of time.

The statistical analysis method used in computer/port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" published by Sprint/Nextel and presented at the Malware workshop, held in conjunction with IPCCC, Phoenix, AZ, USA in April, 2006.

Note: IDF Client Plug-ins running on Windows computers with browser applications may occasionally report false-positive reconnaissance scans due to residual traffic arriving from closed connections.

For the "Notify IDF Server Immediately" option to work, the Client Plug-ins must be configured for Client Plug-in initiated or bi-directional communication. (See **System > System Settings > Computers**.) If enabled, the Client Plug-in will initiate a heartbeat to the IDF Server Plug-in immediately upon detecting the attack or probe.

To configure Reconnaissance settings:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Reconnaissance** tab.
2. In the "Reconnaissance Scans" area, configure the following options:
   - **Reconnaissance Scan Detection Enabled**: Perform detection.
   - **Computers/Networks on which to perform detection**: Choose from the drop-down list the IPs to protect. Choose from existing IP Lists. (You can use the Components > IP Lists screen to create an IP List specifically for this purpose.)
   - **Do not perform detection on traffic coming from**: Select from a set of IP Lists which computers and networks to ignore. (As above, you can use the **Components > IP Lists** screen to create an IP List specifically for this purpose.)

- **Computer OS Fingerprint Probe:** The Client Plug-ins will recognize and react to active TCP stack OS fingerprinting attempts.
- **Network or Port Scan**: The Client Plug-ins will recognize and react to port scans.
- **TCP Null Scan**: The Client Plug-ins will refuse packets with no flags set.
- **TCP SYNFIN Scan**: The Client Plug-ins will refuse packets with only the SYN and FIN flags set.
- **TCP Xmas Scan**: The Client Plug-ins will refuse packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

Scan Settings

To configure Scan settings:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Scan** tab.
2. In the "Scanning for Open Ports" area, select a port list to be used when the IDF Server Plug-in performs a port scan on discovered computers. (The port lists in the drop-down list are the same ones defined in the Port Lists screen in the Components section.)
3. In the "Scanning for Recommendations" area, choose whether to perform ongoing scans and set the interval

   Periodically, the Client Plug-ins can scan their computer for common applications and then make rule recommendations based on what is detected. This setting sets the interval between scans on computers that have been configured to allow them.

Notifications Settings

To configure Notifications:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Notifications** tab.
2. In the "Alert Notification (from the Server Plug-in)" area, enter an email address to which all alert emails will be sent regardless. (Which alerts will trigger the sending of an email can be configured from the **System > System Settings > System** screen.)

3. In the "Notification Frequency (From the Client Plug-in)" area, select how often events are sent from the Client Plug-in to alert recipients.
4. In the "Firewall and DPI Event Notification (from the Client Plug-in)" area, select Forward Events to a Remote Computer (via Syslog) if you wish to store your logs on a dedicated syslog server, type the required information in these fields. For information on configuring Syslog, see *Configuring Syslog Integration* on page 13-3.
5. In the "System Event Notification (from the Server Plug-in)" area, configure the following options if desired:
   - **Forward System Events to a Remote Computer (via Syslog)**: Notifications can be sent to a Syslog server. Type the details of your syslog server here. For information on configuring Syslog, see *Configuring Syslog Integration* on page 13-3.
   - **Forward System Events to a Remote Computer (via SNMP)**: IDF also supports SNMP. The MIB file (`DeepSecurity.mib`) is located in: `\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall\util`

Ranking Settings

The Ranking system provides a way to quantify the importance of DPI and Firewall Events. By assigning "asset values" to computers, and assigning "severity values" to DPI Rules and Firewall Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank when viewing DPI or Firewall Events.

To configure Ranking:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Ranking** tab.
2. In the "Firewall Rule Severity Values" area, configure any of the following:
   - **Firewall Rule Severity Values**: Severity values for Firewall Rules are linked to their actions: Deny, Log Only, and Packet Rejection. (The latter refers to packets rejected because of a stateful configuration setting.) Use this panel to edit the severity values which will be multiplied by a computer's asset value to determine the rank of a Firewall Event. (A Firewall Rule's actions can viewed and edited in the Rule's Properties window.)

- **DPI Rule Severity Values**: DPI Rule Severity Values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer‘s asset value to determine the rank of a DPI Event. A DPI Rule's severity setting can be viewed in the Rule's Properties window.
- **Asset Values**: Asset Values are not associated with any of their other properties like DPI Rules or Firewall Rules. Instead, Asset Values are properties in themselves. A computer's Asset Value can be viewed and edited from the computer's Details window. To simplify the process of assigning asset values, you can predefine some values that will appear in the Asset Importance drop-down list in the first screen of the computer's Details window. To view existing predefined computer Asset Values, click the View Asset Values... button in this panel. The Asset Values window displays the predefined settings. These values can be changed, and new ones can be created. (New settings will appear in the drop-down list for all computers.)

Updates

To ensure maximum protection you must keep your pattern files and software components current. The Updates tab on the **System > System Settings** screen allows you to set how DPI Rules are applied when IDF Server Plug-in checks for updates. To see the status of current updates, go to the **System > Updates** screen.

To configure Updates:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Updates** tab.
2. In the “IDF Rule Updates” area, configure any of the following:
   - **Allow IDF Rule Updates to automatically assign new DPI Rules**: New DPI Rules in Security Updates are associated with Application Types (HTTP Server, DNS Client, MS SQL Server, etc.). If this option is checked, new DPI Rules can automatically be assigned to computers on which the new DPI Rule's associated Application Type is active. Two conditions must be met for a rule to be automatically assigned to a computer:
     - This option must be selected on this screen.

- The rule itself, created by Trend Micro, must be designed to allow auto-assignment. (Some rules, although associated with an Application Type, are not intended to be auto-assigned. The IDF Server Plug-in will recognize these rules and not apply them even if this option is checked.)

- **Allow IDF Rule Updates to set an alert on new DPI Rules**: Some new DPI Rules are considered important enough by Trend Micro that they are set to trigger an alert by default. Clearing this will override that default behavior.

System

To configure the System:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **System** tab.
2. In the "Alert Configuration" area, configure all of IDF Server Plug-in's possible Alerts. For the most part, this means turning them on or off, setting their severity levels, and configuring the Alert's email notification settings.
3. In the "SMTP" area, type the address of your SMTP mail (with the port if required). Enter a "From" email address from which the emails should be sent. Optionally enter a "bounce" address to which delivery failure notifications should be sent if the alert emails can't be delivered to one or more users. If your SMTP mail server requires outgoing authentication, enter the username and password credentials. Once you've entered the necessary information, use the Test SMTP Settings to test the settings.
4. In the "Prune" area, define how long to store Event records and Counters, older Security Updates, and older versions of Client Plug-in software before a purge removes them from the database.

   With respect to the Event settings, your decisions should be based on the robustness of the database system you are using, the amount of available storage space, and which events you have decided to log. Some tips on logging:

   - Disable log collection for computers that are not of interest. This can be done through the Advanced Settings in the computer Details window or the Security Profile Details window.
   - Consider reducing the logging of Firewall Rule activity by disabling the logging options in the Stateful Configuration. (For example, disabling the UDP logging will eliminate the unsolicited UDP log entries)

- For DPI Rules the best practice is to log only dropped packets. Logging packet modifications may result in a lot of log entries.
- For DPI Rules, only include packet data (an option in the DPI Rule's Properties window) when you are interested in examining the source of attacks. Otherwise leaving packet data on will result in much larger log sizes.

Note: Logs are used to populate the Events pages. Counters are data aggregated from the logs. They are used to generate Reports and populate the Dashboard widgets.

---

5. In the "Export" area, you can select the encoding used when you export data files from the IDF Server Plug-in.
6. In the "Whois" area, you can specify the whois lookup to be used when logging DPI and Firewall Events.

Tags

Event Tagging allows administrators to manually tag events with predefined labels ("attack", "suspicious", "patch", "acceptable change", "false positive", "high priority", etc.) and the ability to define custom labels ("Assigned to Tom for review", etc.).

In addition to the manual tagging of events, automated event tagging can be accomplished via the use of a "Reference Computer". For example, a planned rollout of a patch can be applied to the reference computer, the events associated with the application of the patch can be tagged as "Patch X", similar events raised on other systems can automatically be deemed to be "acceptable changes" and suppressed to reduce the number of events subjected to scrutiny by an administrator.

Event tagging enables specialized views of events, dashboards, and reports and can be applied to a single event, similar events, or even to all future similar events.

For more information on tagging, including how to add tags, see *Event Tagging* on page 12-4.

Viewing Tags

All currently defined tags are displayed in the **System > Tags** screen. This includes predefined as well as custom tags. (Only tags that are currently in use are displayed.)

- **Delete Tags**: Deleting a tag removes the tag from all events to which it is attached.

- **View Auto-Tag Rules**: Auto-Tag Rules are created by selecting events and choosing to tag similar items.

Tasks

Tasks let you schedule certain common tasks. Scheduled Tasks will initiate a procedure according to a defined schedule.

To create a task:

PATH: IDF MAIN MENU | SYSTEM > TASKS

1. Click **New** () and select **New Scheduled Task.** The wizard that appears will guide you through the steps of creating a new Task. You will be prompted for different information depending on the type of task.
2. The wizard allows you to schedule the following tasks:
   - **Run Script**: If the Syslog and SNMP options do not meet your event notification requirements, it may be possible for Trend Micro to provide a solution using custom-written scripts. Please contact Trend Micro for more information.
   - **Update Computers**: Periodically perform an update operation on selected computers. An update operation ensure that all configuration changes made in the IDF Server Plug-in have been applied.
   - **Component Update**: Periodically update components. An update operation ensures that all components updates have been applied for IDF Rule updates.
   - **Scan Computers for Recommendations**: Causes the IDF Server Plug-in to scan the computer(s) for common applications and then make recommendations based on what is detected.
   - **Check for New Software**: Check if new versions of the Server Plug-in, Client Plug-ins or Filter Driver are available.
   - **Backup**: Perform regular database backups. (This option is only available if you are using a Derby or Microsoft SQL Server database.)

To view or edit a task:

PATH: IDF MAIN MENU | SYSTEM > TASKS

1. Select a task and click (), or right-click and select **Properties...** from the popup menu.
2. In the properties window, edit the information in the "Schedule Information" area as desired, and click **OK**. or **Apply**.

To duplicate a task:

PATH: IDF MAIN MENU | SYSTEM > TASKS

1. Select a task and click Duplicate (), or right-click and select **Duplicate...** from the popup menu.
2. To rename the task, click (), or right-click and select **Properties...** from the popup menu and enter a new name in the Properties window.

To delete a task:

PATH: IDF MAIN MENU | SYSTEM > TASKS

- Select a task and click Delete (), or right-click and select Delete from the popup menu.

To run a scheduled task:

PATH: IDF MAIN MENU | SYSTEM > TASKS

- Select a task and click Run Task Now (), or right-click and select **Run Task Now** from the popup menu.

Licenses

The Licenses screen displays details about your Trend Micro IDF product licenses. You can see the license status by clicking View detailed license online. Contact Trend Micro if you wish to upgrade your license. If Trend Micro has provided you with a new activation code, click New Activation Code and enter it there. Newly licensed features will be immediately available. For complete upgrade instructions, click View license upgrade instructions. Alerts will be raised if any module is about to expire or has expired.

Updates

The Updates screen displays the status of current updates. To configure updates, go to **System > System Settings > Updates**.

Security Updates

Security Updates include new rules as well as modifications of existing DPI Rules.

- **Last Check for Security Updates**: When the last check for security updates was performed. Click Download to check for updates.
- **Current Applied Version**: Currently applied version of the Security Update.

The **View Security Updates...** button displays a list of the most recent DPI Rules. If required you can reapply the current Rule set to computers being protected by IDF or rollback to a previous Rule set. You can configure the number of Rule updates that are kept in the IDF Server Plug-in's database by going to the Prune area in the **System > System Settings > System** tab.

Applying Security Updates

Updates to Intrusion Defense Firewall come from the same OfficeScan server update source. (The URL of the Trend Micro servers can be changed from **Updates > Server > Update Source** in the OfficeScan console. Consult your OfficeScan documentation for details.)

To manually check for, download, and apply the latest Security Updates:

PATH: IDF MAIN MENU > SYSTEM > UPDATES

1. Click the **Download** button to check for and retrieve the latest update.
2. Once the update is downloaded, click the **View Security Updates...** button to open a new window displaying all downloaded updates. The listed updates will have a green check mark in the "Applied" column indicating if they have been applied to the Client Plug-ins.
3. Select the latest Security Update from the list and click **Apply...** (or **Reapply...**) in the menu bar. A new window will open displaying information about the update that will be applied.
4. Click **Finish** to deploy the update.

Note: You can revert to a previous Security Update by selecting it and clicking **Reapply...** in the menu bar.

To automatically check for and download the latest Update:

1. Navigate to the S**ystem > Tasks** screen.
2. Click **New** on the tool bar and select **New Scheduled Task** to open the New Scheduled Task Wizard.
3. Select **Component Update** from the **Type** drop-down list.
4. Follow the steps in the wizard to select how often and at what time to carry out this task. Updates will be automatically downloaded.
5. To automatically apply the latest Security Updates, check **Apply IDF Rule Updates Automatically**.
6. Click **Finish**.

Client Plug-in Updates

Client Plug-in Updates apply the latest version of the Client Plug-in and driver.

- **Last Check for Client Plug-in Updates**: When the last check for Client Plug-in updates was performed. Click Download to check for updates.
- **Latest 32 Bit Driver Version**: Latest version of the 32-bit driver available from Trend Micro.
- **Latest 64 Bit Driver Version**: Latest version of the 64-bit driver available from Trend Micro.
- **Latest Client Plug-in Deployment**: Number of computers running the latest version of the Client Plug-in.

Note: Updates to IDF Client Plug-ins can all be deployed using the IDF Server Plug-in. New versions of the IDF Server Plug-in, however, must be updated through the OfficeScan Web console's Plug-in Manager. For information on upgrading the Server Plug-in, see *Upgrading the Server Plug-in* on page 11-3.

Click **Deploy Latest** to deploy the latest version of the Client Plug-in and drivers.

Server Diagnostics

You can create a diagnostic package for support. The Diagnostic Package Wizard leads you through the process, allowing you to choose the information that will be included in the package. Click **Generate Diagnostic Package...** to start the wizard.

Chapter 13

Logging

This chapter describes how to configure Trend Micro™ Intrusion Defense Firewall™ logs.

Topics in this chapter:

About Logging

IDF can be instructed to send information to a Syslog server: the Client Plug-in sends DPI and Firewall Event information, and the Server Plug-in sends System Information. IDF can be configured to send notifications, send information to a Syslog server, and to operate in a Logging Policy mode.

Configuring Logs

By default, IDF Server Plug-in collects logs from the Client Plug-ins via the heartbeat. The number of computers this feature can support depends on the frequency of the heartbeat interval (every 10 minutes by default), how active your computers are, and the log settings.

Here are some tips to help maximize the effectiveness of log collection:

- Disable log collection for computers that are not of interest. Do this by going to System > System Settings and then the Firewall and DPI tab in either the computers' Details windows or the Security Profiles' Details windows.
- Consider reducing the logging of Firewall Rule activity by disabling some logging options in the Stateful Configuration Properties window. For example, disabling the UDP logging will eliminate the "Unsolicited UDP" log entries.
- For DPI Rules the best practice is to log only dropped packets. Logging packet modifications may result in a lot of log entries.
- For DPI Rules, only include packet data (an option in the DPI Rule's Properties window) when you are interested in examining the source of attacks. Otherwise leaving packet data inclusion on will result in much larger log sizes.

Configuring Notifications

In addition to alert emails via SMTP and logging to the database chosen during install (internal Derby, SQL Server, or Oracle), the IDF system provides several ways of integrating with third-party recording and notification mechanisms.

Syslog

Both the Client Plug-ins and the Server Plug-in can be instructed to send information to a Syslog server. The Client Plug-in will send DPI and Firewall Event information, and the Server Plug-in will send System Information. To configure the Syslog settings, go to System > System Settings > Notifications.

Notice that there are two panels for configuring Event Notification: one for Firewall and DPI Event Notification and one for System Event Notification.

For information on configuring Syslog, see *Configuring Syslog Integration* on page 13-3.

SNMP

The Server Plug-in also has the option of sending System Event Notifications from the Server Plug-in to an SNMP server. Use the same screen to enter SNMP settings. The MIB file (`DeepSecurity.mib`) is located in `\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall\util`

Scripts

If the Syslog and SNMP options do not meet your event notification requirements, it may be possible for Trend Micro to provide a solution using custom-written scripts. Please contact Trend Micro for more information.

Configuring Syslog Integration

IDF supports Common Event Format 1.0, a format sponsored by ArcSight (www.arcsight.com). Although IDF supports two other syslog formats (Basic Syslog, and Common Event Format (legacy)), these formats are made available for legacy installations and should not be used for new integration projects.

Note: Enabling Syslog forwarding in the IDF Server Plug-in does not affect default logging. That is, enabling syslog will not "turn off" the normal logging mechanisms.

Setting up a Syslog on Red Hat Enterprise

The following steps describe how to configure Syslog on Red Hat Enterprise to receive logs from IDF Client Plug-ins.

1. Log in as root.
2. Execute: vi /etc/syslog.conf
3. Add the following two lines of text to the end of the syslog.conf:

   #Save IDF Server Plug-in logs to IDF Server.log

   Local4.* /var/log/IDF Server.log
4. Save the file and exit.
5. Create the /var/log/IDF Server.log file by typing touch /var/log/IDF Server.log.
6. Set the permissions on the IDF Server log so that syslog can write to it.
7. Execute: vi /etc/sysconfig/syslog
8. Modify the line "SYSLOGD_OPTIONS" and add a "-r" to the options.
9. Save the file and exit.
10. Restart syslog: /etc/init.d/syslog restart.

When Syslog is functioning you will see logs populated in: /var/log/IDF Server.log

IDF Server Plug-in Settings

You can configure IDF Server Plug-in to instruct all managed computers to send logs to the Syslog computer, or you can configure individual computers independently.

To configure the Server Plug-in to instruct all managed computers to use Syslog:

PATH: IDF MAIN MENU | SYSTEM > SYSTEM SETTINGS

1. Click the **Notifications** tab.
2. In the panel called "System Event Notification" area, set the "Forward System Events to a remote computer (via Syslog)" option.
3. Type the hostname or the IP address of the Syslog computer.
4. Enter which UDP port to use (usually 514).
5. Select which Syslog facility to use (Local4 from the Red Hat example above.)

6. Select the "Common Event Format 1.0" log format. (The "Basic Syslog" and "Common Event Format (legacy)" formats are listed only for legacy support and should not be used for new integrations.)

Note: Common Event Format 1.0 is a format sponsored by ArcSight (www.arcsight.com). The specification can be requested through their Web site.

You have now configured the IDF Server Plug-in to instruct all existing and new computers to use remote Syslog by default.

This default setting can be overridden for specific Security Profiles and on individual computers. To override on a computer, find the computer you want to configure in the Computers screen and double-click it to view its Details window. Go to **System > System Settings** and click the **Notifications** tab. Like many other settings on a computer, you can instruct it to inherit default settings, or override them. To instruct this computer to ignore any inheritable default settings, select the "Forward Events To:" option and enter the details for a different Syslog server, or to not forward logs at all. Follow the same procedure to override the setting on a Security Profile.

Parsing Syslog Messages

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

To determine whether the log entry comes from the IDF Server Plug-in or an IDF Client Plug-in, look at the "Device Product" field:

Sample Log Entry: Jan 18 11:07:53 dsmhost CEF:0|Third Brigade|IDF Server Plug-in|5.0.1659|600|Administrator Signed In|4|suser=Master…

To further determine what kind of rule triggered the event, look at the "Signature ID" and "Name" fields:

Sample Log Entry: Mar 19 15:19:15 chrisds7 CEF:0|Trend Micro|IDF Client Plug-in|7.0.0.2036|123|Out Of Allowed Policy|5|cn1=1...

The following "Signature ID" values indicate what kind of event has been triggered:

TABLE 13-1. Signature IDs

SIGNATURE IDS	DESCRIPTION
10	Custom DPI Rule
20	Log Only Firewall Rule
21	Deny Firewall Rule
100-299	Out of "Allowed" Policy Firewall Rule
300-399	SSL Events
500-899	Stateful Configuration Events
1,000,000-1,999,999	Trend Micro DPI Rule

Note: All the CEF extensions described in the tables below will not necessarily be included in each log entry. As well, they may not be in the order described below. If you are using regular expressions (regex) to parse the entries, make sure your expressions do not depend on each key/value pair to be there or for the key/value pairs to be in a particular order.

Note: Syslog messages are limited to 1024 characters by the syslog protocol specification. In rare cases data may be truncated if long rule and interface names are used.

Firewall Event Log Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry (1):
```
03-19-2010          16:19:18
Local0.Info         10.52.116.23       Mar 19 15:19:15 chrisds7
CEF:0|Trend Micro|IDF Client Plug-in|7.0.0.2036|123|Out Of
Allowed Policy|5|cn1=1 cn1Label=Computer ID act=Deny
```

```
dmac=00:0C:29:8D:F1:C9 smac=00:1C:23:01:85:37
TrendMicroDsFrameType=IP src=10.52.116.140 dst=10.52.116.23
in=62 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=24431
dpt=23 cs2=0x00 SYN cs2Label=TCP Flags cnt=1
```

Sample Log Entry (2):

```
03-19-2010          16:18:33
Local0.Info         10.52.116.23       Mar 19 15:18:31 chrisds7
CEF:0|Trend Micro|IDF Client Plug-in|7.0.0.2036|123|Out Of
Allowed Policy|5|cn1=1 cn1Label=Computer ID act=Deny
dmac=00:0C:29:8D:F1:C9 smac=00:1C:23:01:85:37
TrendMicroDsFrameType=IP src=10.52.116.140 dst=10.52.116.23
in=66 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=24430
dpt=23 cs2=0x00 SYN cs2Label=TCP Flags cnt=1
TrendMicroDsPacketData=AAwpjfHJABwjAYU3CABFAAA0ZjFAAIAGl4cKNHSM
CjR0F19uABefXY81AAAAAIACIADD8gAAAgQFtAEDAwIBAQQC
```

TABLE 13-2. Firewall Event Extension Fields

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
act	Action	The action taken by the Firewall rule. Can contain: Block, Reset, Insert, Delete, Replace or Log. If the rule or the network engine is operating in detect-only mode, the action value will be proceeded by "IDS:".	act=Block act=Reset

TABLE 13-2. Firewall Event Extension Fields

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
cn1	Computer Identifier	The Client Plug-in Computer internal identifier which can be used to uniquely identify the Client Plug-in Computer from a given syslog event.	cn1=113
cn1Label	Computer ID	The friendly name label for the field cn1.	cn1Label=Computer ID
cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8
cs2	TCP Flags	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set.	cs2=0x10 ACK cs2=0x14 ACK RST
cs2Label	TCP Flags	The friendly name label for the field cs2.	cs2Label=TCP Flags

TABLE 13-2. Firewall Event Extension Fields

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
cs3	Packet Fragmentation Information	The "DF" field will be present if the IP "Don't Fragment" bit is set. The "MF" field will be present if the "IP More Fragments" bit is set.	cs3=MF cs3=DF MF
cs3Label	Fragmentation Bits	The friendly name label for the field cs3.	cs3Label=Fragmentation Bits
cs4	ICMP Type and Code	(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.	cs4=11 0 cs4=8 0
cs4Label	ICMP	The friendly name label for the field cs4.	cs4Label=ICMP Type and Code
dmac	Destination MAC Address	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3
dpt	Destination Port	(For TCP and UDP protocol only) Destination computer connection port.	dpt=80 dpt=135

TABLE 13-2. Firewall Event Extension Fields

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102 dst=10.30.128.2
in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137 in=21
out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216 out=13
proto	Transport protocol	Name of the connection transportation protocol used.	proto=tcp proto=udp proto=icmp
smac	Source MAC Address	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3
spt	Source Port	(For TCP and UDP protocol only) Source computer connection port.	spt=1032 spt=443
src	Source IP Address	Source computer IP Address.	src=192.168.1.105 src=10.10.251.231

TABLE 13-2. Firewall Event Extension Fields

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
TrendMicroDs FrameType	Ethernet frame type	Connection Ethernet frame type.	TrendMicroDsFrameType= IP TrendMicroDsFrameType= ARP TrendMicroDsFrameType= RevARP TrendMicroDsFrameType= NetBEUI
TrendMicroDs PacketData	Packet data	(If include packet data is set) A Base64 encoded copy of the packet data. The "equals" character is escaped. E.g. "\="	TrendMicroDsPacketData =AA...BA\=

DPI Event Log Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: `03-19-2010 17:11:05 Local0.Info 10.52.116.23 Mar 19 16:10:58 chrisds7 CEF:0|Trend Micro|IDF Client Plug-in|7.0.0.2036|1000552|Generic Cross Site Scripting(XSS) Prevention|10|cn1=1 cn1Label=Computer ID dmac=00:0C:29:8D:F1:C9 smac=00:1C:23:01:85:37 TrendMicroDsFrameType=IP src=10.52.116.140 dst=10.52.116.23 in=465 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=26362 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=Log cn3=22 cn3Label=DPI Packet Position cs5=22 cs5Label=DPI Stream Position`

```
cs1=XSS_Attack cs1Label=DPI Note cs6=8 cs6Label=DPI Flags
TrendMicroDsPacketData=R0VUIC8lM0NTQ1JJUFQlM0VhbGVydChkb2N1bWVu
dC5jb2...
```

TABLE 13-3. DPI Event Log Format Extensions

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
act	Action	The action taken by the DPI rule. Can contain: Block, Reset, Insert, Delete, Replace or Log. If the rule or the network engine is operating in detect-only mode, the action value will be proceeded by "IDS:".	act=Block
cn1	Computer Identifier	The Client Plug-in Computer internal identifier which can be used to uniquely identify the Client Plug-in Computer from a given syslog event.	cn1=113
cn1Label	Computer ID	The friendly name label for the field cn1.	cn1Label=Computer ID
cn3	DPI Packet Position	Position within packet of data that triggered the event.	cn3=37
cn3Label	DPI Packet Position	The friendly name label for the field cn3.	cn3Label=DPI Packet Position

TABLE 13-3. DPI Event Log Format Extensions

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8
cs1	DPI Filter Note	(Optional) A note field which can contain a short binary or text note associated with the payload file. If the value of the note field is all printable ASCII characters, it will be logged as text with spaces converted to underscores. If it contains binary data, it will be logged using Base-64 encoding.	cs1=Drop_data
cs1Label	DPI Note	The friendly name label for the field cs1.	cs1Label=DPI Note
cs2	TCP Flags	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set.	cs2=0x10 ACK cs2=0x14 ACK RST

TABLE 13-3. DPI Event Log Format Extensions

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
cs2Label	TCP Flags	The friendly name label for the field cs2.	cs2Label=TCP Flags
cs3	Packet Fragmentation Information	The "DF" field will be present if the IP "Don't Fragment" bit is set. The "MF" field will be present if the "IP Mote Fragments" bit is set.	cs3=MF cs3=DF MF
cs3Label	Fragmentation Bits	The friendly name label for the field cs3.	cs3Label=Fragmentation Bits
cs4	ICMP Type and Code	(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.	cs4=11 0 cs4=8 0
cs4Label	ICMP	The friendly name label for the field cs4.	cs4Label=ICMP Type and Code
cs5	DPI Stream Position	Position within stream of data that triggered the event.	cs5=128 cs5=20
cs5Label	DPI Stream Position	The friendly name label for the field cs5.	cs5Label=DPI Stream Position

TABLE 13-3. DPI Event Log Format Extensions

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
cs6	DPI Filter Flags	A combined value that includes the sum of the following flag values: 1 - Data truncated – Data could not be logged. 2 - Log Overflow – Log overflowed after this log. 4 - Suppressed – Logs threshold suppressed after this log. 8 - Have Data – Contains packet data 16 - Reference Data – References previously logged data.	The following example would be a summed combination of 1 (Data truncated) and 8 (Have Data): cs6=9
cs6Label	DPI Flags	The friendly name label for the field cs6.	cs6=DPI Filter Flags
dmac	Destination MAC Address	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3

TABLE 13-3. DPI Event Log Format Extensions

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
dpt	Destination Port	(For TCP and UDP protocol only) Destination computer connection port.	dpt=80 dpt=135
dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102 dst=10.30.128.2
in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137 in=21
out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216 out=13
proto	Transport protocol	Name of the connection transportation protocol used.	proto=tcp proto=udp proto=icmp
Smac	Source MAC Address	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3
Spt	Source Port	(For TCP and UDP protocol only) Source computer connection port.	spt=1032 spt=443

TABLE 13-3. DPI Event Log Format Extensions

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
Src	Source IP Address	Source computer IP Address.	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	Ethernet frame type	Connection Ethernet frame type.	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	Packet data	(If include packet data is set) A Base64 encoded copy of the packet data. The "equals" character is escaped. E.g. "\="	TrendMicroDsPacketData=AA...BA\=

System Event Log Format

Base CEF Format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry (1): `03-19-2010 17:32:07 Local0.Info 10.52.116.23 Mar 19 17:32:00 chrisds7 CEF:0|Trend Micro|IDF Server Plug-in|7.0.1591|160|Authentication Failed|4|src=10.52.116.23 suser=MasterAdmin target=MasterAdmin msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1`

Sample Log Entry (2): `03-19-2010 17:34:38 Local0.Info 10.52.116.23 Mar 19 17:34:30 chrisds7 CEF:0|Trend Micro|IDF Server Plug-in|7.0.1591|300|Scan for Recommendations|4|src=10.52.116.23 suser=System target=localhost msg=A Scan for Recommendations on computer (localhost) has completed. Any changes to the computer as a result of this Scan for Recommendations will have been reflected in a 'Computer Updated' system event.`

TABLE 13-4. System Event Log Format Extensions

EXTENSION FIELD	NAME	DESCRIPTION	EXAMPLES
src	Source IP Address	Source IDF Server Plug-in IP Address.	src=10.52.116.23
suser	Source User	Source IDF Server Plug-in user account.	suser=MasterAdmin
target	Target entity	The event target entity. The target of the event maybe the administrator account logged into IDF Server Plug-in, or a Computer.	target=MasterAdmin target=server01
msg	Details	Details of the System event. May contain a verbose description of the event.	msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed...

Advanced Logging Policy Modes

To reduce the number of events being logged, the IDF Server Plug-in can be configured to operate in one of several Advanced Logging Policy modes. These modes are set in the System > System Settings > Firewall and DPI screen in the Advanced area.

The following table lists the types of Events are ignored in four of the more complex Advanced Logging Policy modes:

TABLE 13-5. Ignored Events

MODE	IGNORED EVENTS
Stateful and Normalization Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy Dropped Retransmit

TABLE 13-5. Ignored Events

MODE	IGNORED EVENTS
Stateful, Normalization, and Frag Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit

TABLE 13-5. Ignored Events

MODE	IGNORED EVENTS
Stateful, Frag, and Verifier Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Invalid Data Offset No IP Header Unreadable Ethernet Header Undefined Same Source and Destination IP Invalid TCP Header Length

TABLE 13-5. Ignored Events

MODE	IGNORED EVENTS
	Unreadable Protocol Header Unreadable IPv4 Header Unknown IP Version Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit
Tap Mode	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit

Chapter 14

Getting Help

This chapter describes troubleshooting issues that may arise and how to contact support.

Topics in this chapter:

Contacting Trend Micro

Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all registered users.

- Get a list of the worldwide support offices at:

  http://www.trendmicro.com/support

- Get the latest Trend Micro product documentation at:

  http://www.trendmicro.com/download

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

Trend Micro, Inc.

10101 North De Anza Blvd., Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

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

Fax: +1 (408) 257-2003

Web address:

http://www.trendmicro.com

Email: support@trendmicro.com

Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

http://esupport.trendmicro.com

Trend Micro updates the contents of the Knowledge Base continuously and adds new solutions daily. If you are unable to find an answer, however, you can describe the problem in an email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

TrendLabs

TrendLabs[SM] is the global antivirus research and support center of Trend Micro. Located on three continents, TrendLabs has a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Email access to antivirus engineers
- Knowledge Base, the Trend Micro online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

Comprehensive security information is available at the Trend Micro Web site.

http://www.trendmicro.com/vinfo/

Information available:

- List of viruses and malicious mobile code currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

Sending Suspicious Files to Trend Micro

If you think you have an infected file but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us. For more information, refer to the following site:

http://subwiz.trendmicro.com/subwiz

You can also send Trend Micro the URL of any Web site you suspect of being a phish site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and viruses).

- Send an email to the following address and specify "Phish or Disease Vector" as the subject.

  virusresponse@trendmicro.com

- You can also use the Web-based submission form at:

  http://subwiz.trendmicro.com/subwiz

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

Appendix A

Ports Used by IDF

A number of ports must be accessible for the IDF Server Plug-in and the Client Plug-ins to function as expected. The following is a list of the ports used, the description of the function for which the port is used, the related protocols, the application which initializes the connection, the application to which the connection is made, whether the use of a proxy is possible (and what type of proxy), and whether and where the port can be configured:

Port: 4118

- **Use**: Server Plug-in-to-Client Plug-in communication.
- **Protocol**: TCP
- **Initiated By**: IDF Server Plug-in
- **Connected To**: Client Plug-in
- **Proxy**: No
- **Configuration**: This port is not configurable (please contact your support provider if this port assignment is problematic.)

Port: 4119 (default)

- **Use**: Access to IDF Server Plug-in Web browser interface.
- **Protocol**: TCP

- **Initiated By**: Web browser
- **Connected To**: IDF Server Plug-in
- **Proxy**: No
- **Configuration**: This port is configured during the IDF Server Plug-in installation process.

Port: 4120 (default)

- **Use**: Client Plug-in-to-Server Plug-in communication
- **Protocol**: TCP
- **Initiated By**: Client Plug-in
- **Connected To**: IDF Server Plug-in
- **Proxy**: No
- **Configuration**: This port is configured during the IDF Server Plug-in installation process.

Port: 514 (default)

- **Use**: Syslog
- **Protocol**: UDP
- **Initiated By**: Client Plug-in
- **Connected To**: Syslog facility
- **Proxy**: No
- **Configuration**: This port can be configured in System > System Settings > Notifications.

Port: 25 (default)

- **Use**: E-mail Alerts
- **Protocol**: TCP
- **Initiated By**: IDF Server Plug-in
- **Connected To**: Specified SMTP server
- **Proxy**: No

- **Configuration**: This port can be configured in System > System Settings > System.

Port: 80

- **Use**: Connection to Trend Micro ActiveUpdate Server
- **Protocol**: HTTP and SOCKS
- **Initiated By**: IDF Server Plug-in
- **Connected To**: Trend Micro ActiveUpdate Server
- **Proxy**: Yes (optional)
- **Configuration**: The proxy address and port can be configured in System > System Settings > Updates.

Port: 389

- **Use**: LDAP directory addition or IDF Server Plug-in
- **Protocol**: TCP
- **Initiated By**: IDF Server Plug-in
- **Connected To**: LDAP server
- **Proxy**: No
- **Configuration**: This port can be configured in the New Directory wizard.

Port: Randomly selected

- **Use**: DNS lookup for hostnames
- **Protocol**: TCP
- **Initiated by**: IDF Server Plug-in
- **Connected to**: DNS server
- **Proxy**: No
- **Configuration**: The port is randomly selected when the IDF Server Plug-in needs to lookup a hostname.

Appendix B

Computer and Client Plug-in Status

The status column of the IDF Server Plug-in's Computers screen displays the current state of the computer and its Client Plug-in. The status column will usually display the state of the computer on the network followed by the state (in parentheses) of the Client Plug-in providing protection if either is present. If the computer or Client Plug-in is in an error state, that state will also be displayed in the status column. When operations are in progress, the status of the operation will appear in the status column.

The following three tables list possible status and error messages that may appear in the status column of the Computers screen.

Note: In addition to the values below, the status column may also display System or Client Plug-in Events. For a list of the Events, see *Client Plug-in Events* on page C-24 and *System Events* on page C-8.

Computer States

TABLE B-1. Computer States

COMPUTER STATE	DESCRIPTION
Unmanaged	unactivated
Managed	A Client Plug-in is present and activated with no pending operations or errors.
Updating	The Client Plug-in is being updated with a combination of new configuration settings and security updates.
Update Pending (Schedule)	The Client Plug-in will be updated with a combination of new configuration settings and security updates once the computer's access schedule permits.
Update Pending (Heartbeat)	An update will be performed at the next heartbeat.
Update Pending (Offline)	The Server Plug-in cannot currently communicate with the Client Plug-in. An update is ready to be applied once the Client Plug-in comes back online.
Scanning for Open Ports	The Server Plug-in is scanning the Computer for open ports.
Activating	The Server Plug-in is activating the Client Plug-in.
Activating (Delayed)	The activation of the Client Plug-in is delayed by the amount of time specified in the relevant event-based task.
Activated	The Client Plug-in is activated.
Deactivating	The Server Plug-in is deactivating the Client Plug-in. This means that the Client Plug-in is available for activation and management by another IDF Server Plug-in.

TABLE B-1. Computer States

COMPUTER STATE	DESCRIPTION
Deactivate Pending (Heartbeat)	A deactivate instruction will be sent from the Server Plug-in during the next heartbeat.
Locked	The computer is in a locked state. While in in a locked state the Server Plug-in will not communicate with the Client Plug-in or generate any computer-related alerts. Existing computer alerts are not affected.
Multiple Errors	Multiple errors have occurred on this computer. See the computer's system events for details.
Multiple Warnings	Multiple warnings are in effect on this computer. See the computer's system events for details.
Upgrading Client Plug-in	The Client Plug-in software on this computer is in the process of being upgraded to a newer version.
Scanning for Recommendations	A Recommendation Scan is underway.
Scan for Recommendations Pending (Schedule)	A Recommendation Scan will be initiated once the computer's Access Schedule permits.
Scan for Recommendations Pending (Heartbeat)	The Server Plug-in will initiate a Recommendation Scan at the next heartbeat.
Scan for Recommendations Pending (Offline)	The Client Plug-in is currently offline. The Server Plug-in will initiate a Recommendation Scan when communication is reestablished.
Checking Status	The client plug-in state is being checked.
Getting Events	The Server Plug-in is retrieving Events from the Client Plug-in.

TABLE B-1. Computer States

COMPUTER STATE	DESCRIPTION
Upgrade Recommended	A newer version of the Client Plug-in is available. A software upgrade is recommended.

Client Plug-in States

TABLE B-2. Client Plug-in States

CLIENT PLUG-IN STATE	DESCRIPTION
Activated	The Client Plug-in has been successfully activated and is ready to be managed by the IDF Server Plug-in.
Activation Required	An unactivated Client Plug-in has been detected on the target machine. It must be activated before it can be managed by the IDF Server Plug-in.
Unknown	No attempt has been made to determine whether a Client Plug-in is present.
Deactivation Required	The Server Plug-in has attempted to activate a Client Plug-in that has already been activated by another IDF Server Plug-in. The original IDF Server Plug-in must deactivate the Client Plug-in before it can be activated by the new Server Plug-in.
Reactivation Required	The Client Plug-in is installed and listening and is waiting to be reactivated by an IDF Server Plug-in.
Online	The Client Plug-in is online and operating as expected.
Offline	No contact has been made with the Client Plug-in for the number of heartbeats specified in System > Settings > Computers screen.

Computer Errors

TABLE B-3. Computer Errors

ERROR STATE	DESCRIPTION
Communication error	General network error.

TABLE B-3. Computer Errors

ERROR STATE	DESCRIPTION
No route to computer	Typically the remote computer cannot be reached because of an intervening firewall or if an intermediate router is down.
Unable to resolve hostname	Unresolved socket address.
Activation required	An instruction was sent to the Client Plug-in when it was not yet activated.
Unable to communicate with Client Plug-in	Unable to communicate with Client Plug-in .
Protocol error	Communication failure at the HTTP layer.
Deactivation Required	The Client Plug-in is currently activated by another IDF Server Plug-in.
No Client Plug-in	No Client Plug-in was detected on the target.
No valid software version	Indicates that no installer can be found for the platform/version requested.
Send software failed	There was an error in sending a binary package to the computer.
Internal error	Internal error. Please contact your support provider.
Duplicate Computer	Two computers in the Server Plug-in's Computers list share the same IP address.

Appendix C

Events

This chapter describes IDF events.

Topics in this chapter:

Firewall Events

TABLE C-1. Firewall Events

EVENT	NOTES
CE Flags	The CWR or ECE flags were set and the stateful configuration specifies that these packets should be denied.
Dropped Retransmit	Dropped Retransmit.
First Fragment Too Small	A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).
Fragment Offset Too Small	The offsets(s) specified in a fragmented packet sequence is less than the size of a valid datagram.
Fragment Out Of Bounds	The offsets(s) specified in a fragmented packet sequence is outside the range of the maximum size of a datagram.
Fragmented	A fragmented packet was encountered with deny fragmented packets disallowed enabled.
Internal Driver Error	Insufficient resources.
Internal States Error	Internal TCP stateful error.
Invalid ACK	A packet with an invalid acknowledgement number was encountered.
Invalid Adapter Configuration	An invalid adapter configuration has been received.
Invalid Data Offset	Invalid data offset parameter.

TABLE C-1. Firewall Events

EVENT	NOTES
Invalid Flags	Flag(s) set in packet were invalid. This could be due to a flag that does not make sense within the context of a current connection (if any), or due to a nonsensical combination of flags. (Stateful Configuration must be On for connection context to be assessed.)
Invalid IP	Packet's source IP was not valid.
Invalid IP Datagram Length	The length of the IP datagram is less than the length specified in the IP header.
Invalid Port Command	An invalid FTP port command was encountered in the FTP control channel data stream.
Invalid Sequence	A packet with an invalid sequence number or out-of-window data size was encountered.
Invalid IP Header Length	An invalid IP header length (< 5*4 = 20) was set in the IP header.
IP Version Unknown	An IP packet other than IPv4 or IPv6 was encountered.
IPv6 Packet	An IPv6 Packet was encountered, and IPv6 blocking is enabled.
Max Incoming Connections	The number of incoming connections has exceeded the maximum number of connections allowed.
Max Outgoing Connections	The number of outgoing connections has exceeded the maximum number of connections allowed.
Max SYN Sent	The number of half open connections from a single computer exceeds that specified in the stateful configuration.
Maximum ACK Retransmit	This retransmitted ACK packet exceeds the ACK storm protection threshold.

TABLE C-1. Firewall Events

EVENT	NOTES
Null IP	a NULL (0.0.0.0) IP is not allowed by the present firewall configuration
Out Of Allowed Policy	The packet does not meet any of the Allow or Force Allow rules and so is implicitly denied.
Out Of Connection	A packet was received that was not associated with an existing connection.
Overlapping Fragment	This packet fragment overlaps a previously sent fragment.
Packet on Closed Connection	A packet was received belonging to a connection already closed.
Same Source and Destination IP	Source and destination IPs were identical.
SYN Cookie Error	The SYN cookies protection mechanism encountered an error.
Unknown IP Version	Unrecognized IP version.
Unreadable Ethernet Header	Data contained in this Ethernet frame is smaller than the Ethernet header.
Unreadable IPv4 Header	The packet contains an unreadable IPv4 header.
Unreadable Protocol Header	The packet contains an unreadable TCP, UDP or ICMP header.
Unsolicited ICMP	ICMP stateful has been enabled (in stateful configuration) and an unsolicited packet that does not match any Force Allow rules was received.
Unsolicited UDP	Incoming UDP packets that were not solicited by the computer are rejected.

DPI Events

TABLE C-2. DPI Events

EVENT	NOTES
Base 64 Decoding Error	Packet content that was expected to be encoded in Base64 format was not encoded correctly.
Client Attempted to Rollback	A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message.
Corrupted Deflate/GZIP Content	Corrupted Deflate/GZIP Content
Deflate/GZIP Checksum Error	Deflate/GZIP Checksum Error.
Double Decoding Exploit	Double decoding exploit attempt (%25xx, %25%xxd, etc).
Edit Too Large	Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes).
Error Decrypting Pre-master Key	Unable to un-wrap the pre-master secret from the ClientKeyExchange message.
Error Generating Master Key(s)	Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret.
Error Generating Pre-Master Request	An error occurred when trying to queue the pre-master secret for decryption.
Handshake Message (not ready)	The SSL state engine has encountered a handshake message after the handshake has been negotiated.
Illegal Character in URI	Illegal character used in uri.

TABLE C-2. DPI Events

EVENT	NOTES
Incomplete Deflate/GZIP Content	Corrupted deflate/gzip content.
Incomplete UTF8 Sequence	URI ended in middle of utf8 sequence.
Int Min/Max/Choice Constraint Failure	A protocol decoding rule decoded data that did not meet the protocol content constraints.
Internal Error	The protocol decoding engine detected an internal corruption while processing a loop or nested type.
Invalid Hex Encoding	%nn where nn are not hex digits.
Invalid Lexical Instruction	An internal error occurred causing the protocol decoding stack to become corrupt and halt processing for the connection.
Invalid Parameters In Handshake	An invalid or unreasonable value was encountered while trying to decode the handshake protocol.
Invalid Traversal	Tried to use "../../" above root.
Invalid Use of Character	use of disabled char
Invalid UTF8 encoding	Invalid/non-canonical encoding attempt.
Key Exchange Error	The server is attempting to establish an SSL session with temporarily generated key.
Key Too Large	The master secret keys are larger than specified by the protocol identifier.
Max Matches in Packet Exceeded	There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is dropped because this usually indicates a garbage or evasive packet.

TABLE C-2. DPI Events

EVENT	NOTES
Maximum Edits Exceeded	The maximum number of edits (32) in a single region of a packet was exceeded.
Memory Allocation Error	The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory.
Out Of Order Handshake Message	A well formatted handshake message has been encountered out of sequence.
Packet Read Error	Low level problem reading packet data.
Record Layer Message	The SSL state engine has encountered an SSL record before initialization of the session.
Region Too Big	A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol.
Renewal Error	An SSL session was being requested with a cached session key that could not be located.
Runtime Error.	Runtime error.
Search Limit Reached	A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached.
Stack Depth	A rule programming error attempted to cause recursion or use to many nested procedure calls.
Type Nesting Too Deep	A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded.

TABLE C-2. DPI Events

EVENT	NOTES
Unsupported Cipher	An unknown or unsupported Cipher Suite has been requested.
Unsupported Deflate/GZIP Dictionary	Unsupported Deflate/GZIP Dictionary.
Unsupported GZIP Header Format/Method	Unsupported GZIP Header Format/Method.
Unsupported SSL Version	A client attempted to negotiate an SSL V2 session.
URI Path Depth Exceeded	too many "/" separators, max 100 path depth.
URI Path Length Too Long	path length is greater than 512 characters.

System Events

The following table lists the System Events that can be recorded by IDF and their default settings. (Notifications cannot be sent for Events that are not recorded.)

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
0	Error	Unknown Error	On	On
100	Info	IDF Server Plug-in Started	On	On
101	Info	License Changed	On	On
102	Info	Trend Micro IDF Customer Account Changed	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
103	Warning	Check For Updates Failed	On	On
104	Warning	Automatic Software Download Failed	On	On
105	Warning	Scheduled IDF Rule Update Download and Apply Failed	On	On
106	Info	Scheduled IDF Rule Update Downloaded and Applied	On	On
107	Info	IDF Rule Update Downloaded and Applied	On	On
108	Info	Script Executed	On	On
109	Error	Script Execution Failed	On	On
110	Info	System Events Exported	On	On
111	Info	Firewall Events Exported	On	On
112	Info	DPI Events Exported	On	On
113	Warning	Scheduled IDF Rule Update Download Failed	On	On
114	Info	Scheduled IDF Rule Update Downloaded	On	On
115	Info	IDF Rule Update Downloaded	On	On
116	Info	IDF Rule Update Applied	On	On
117	Info	IDF Server Plug-in Shutdown	On	On
118	Warning	IDF Server Plug-in Offline	On	On
119	Info	IDF Server Plug-in Back Online	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
120	Error	Heartbeat Server Failed	On	On
121	Error	Scheduler Failed	On	On
122	Error	Server Plug-in Message Thread Failed	On	On
123	Info	IDF Server Plug-in Forced Shutdown	On	On
124	Info	IDF Rule Update Deleted	On	On
130	Info	Credentials Generated	On	On
131	Warning	Credential Generation Failed	On	On
150	Info	System Settings Saved	On (cannot be turned off)	On
151	Info	Software Added	On	On
152	Info	Software Deleted	On	On
153	Info	Software Updated	On	On
154	Info	Software Exported	On	On
155	Info	Software Platforms Changed	On	On
160	Info	Authentication Failed	On	On
161	Info	IDF Rule Update Exported	On	On
166	Info	Check for New Software Success	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
167	Error	Check for New Software Failed	On	On
168	Info	Manual Update Component Success	On	On
169	Error	Manual Update Component Failed	On	On
170	Error	Server Plug-in Available Disk Space Too Low	On	On
180	Info	Alert Type Updated	On	On
190	Info	Alert Started	On	On
191	Info	Alert Changed	On	On
192	Info	Alert Ended	On	On
197	Info	Alert Emails Sent	On	On
198	Warning	Alert Emails Failed	On	On
199	Error	Alert Processing Failed	On	On
250	Info	Computer Created	On	On
251	Info	Computer Deleted	On	On
252	Info	Computer Updated	On	On
253	Info	Security Profile Assigned to Computer	On	On
254	Info	Computer Moved	On	On
255	Info	Activation Requested	On	On
256	Info	Update Now Requested	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
257	Info	Locked	On	On
258	Info	Unlocked	On	On
259	Info	Deactivation Requested	On	On
260	Info	Scan for Open Ports	On	On
261	Warning	Scan for Open Ports Failed	On	On
262	Info	Scan for Open Ports Requested	On	On
263	Info	Scan for Open Ports Cancelled	On	On
264	Info	Client Plug-in Software Upgrade Requested	On	On
265	Info	Client Plug-in Software Upgrade Cancelled	On	On
266	Info	Warnings/Errors Cleared	On	On
267	Info	Check Status Requested	On	On
268	Info	Get Events Now Requested	On	On
270	Error	Computer Creation Failed	On	On
275	Warning	Duplicate Computer	On	On
276	Info	Components Updated	On	On
280	Info	Computers Exported	On	On
281	Info	Computers Imported	On	On
286	Info	Computer Log Exported	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
290	Info	Domain Added	On	On
291	Info	Domain Removed	On	On
292	Info	Domain Updated	On	On
293	Info	Interface Renamed	On	On
294	Info	Computer Bridge Renamed	On	On
295	Info	Interface Deleted	On	On
296	Info	Interface IP Deleted	On	On
297	Info	Scan for Recommendations Requested	On	On
298	Info	Recommendations Cleared	On	On
299	Info	Asset Value Assigned to Computer	On	On
300	Info	Scan for Recommendations	On	On
301	Info	Client Plug-in Software Deployment Requested	On	On
302	Info	Client Plug-in Software Removal Requested	On	On
303	Info	Computer Renamed	On	On
306	Info	Rebuild Baseline Requested	On	On
307	Info	Cancel Update Requested	On	On
330	Info	SSL Configuration Created	On	On
331	Info	SSL Configuration Deleted	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
332	Info	SSL Configuration Updated	On	On
350	Info	Security Profile Created	On	On
351	Info	Security Profile Deleted	On	On
352	Info	Security Profile Updated	On	On
353	Info	Security Profiles Exported	On	On
354	Info	Security Profiles Imported	On	On
368	Warning	Interfaces Out of Sync	On	On
369	Info	Interfaces in Sync	On	On
410	Info	Firewall Rule Created	On	On
411	Info	Firewall Rule Deleted	On	On
412	Info	Firewall Rule Updated	On	On
413	Info	Firewall Rule Exported	On	On
414	Info	Firewall Rule Imported	On	On
420	Info	Stateful Configuration Created	On	On
421	Info	Stateful Configuration Deleted	On	On
422	Info	Stateful Configuration Updated	On	On
423	Info	Stateful Configuration Exported	On	On
424	Info	Stateful Configuration Imported	On	On
460	Info	Application Type Created	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
461	Info	Application Type Deleted	On	On
462	Info	Application Type Updated	On	On
463	Info	Application Type Exported	On	On
464	Info	Application Type Imported	On	On
470	Info	DPI Rule Created	On	On
471	Info	DPI Rule Deleted	On	On
472	Info	DPI Rule Updated	On	On
473	Info	DPI Rule Exported	On	On
474	Info	DPI Rule Imported	On	On
505	Info	Context Created	On	On
506	Info	Context Deleted	On	On
507	Info	Context Updated	On	On
508	Info	Context Exported	On	On
509	Info	Context Imported	On	On
510	Info	IP List Created	On	On
511	Info	IP List Deleted	On	On
512	Info	IP List Updated	On	On
513	Info	IP List Exported	On	On
514	Info	IP List Imported	On	On
520	Info	Port List Created	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
521	Info	Port List Deleted	On	On
522	Info	Port List Updated	On	On
523	Info	Port List Exported	On	On
524	Info	Port List Imported	On	On
530	Info	MAC List Created	On	On
531	Info	MAC List Deleted	On	On
532	Info	MAC List Updated	On	On
533	Info	MAC List Exported	On	On
534	Info	MAC List Imported	On	On
550	Info	Schedule Created	On	On
551	Info	Schedule Deleted	On	On
552	Info	Schedule Updated	On	On
553	Info	Schedule Exported	On	On
554	Info	Schedule Imported	On	On
560	Info	Scheduled Task Created	On	On
561	Info	Scheduled Task Deleted	On	On
562	Info	Scheduled Task Updated	On	On
563	Info	Scheduled Task Manually Executed	On	On
564	Info	Scheduled Task Started	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
565	Info	Backup Finished	On	On
566	Error	Backup Failed	On	On
567	Info	Sending Outstanding Alert Summary	On	On
568	Warning	Failed To Send Outstanding Alert Summary	On	On
569	Warning	Email Failed	On	On
570	Info	Sending Report	On	On
571	Warning	Failed To Send Report	On	On
572	Error	Invalid Report Jar	On	On
573	Info	Asset Value Created	On	On
574	Info	Asset Value Deleted	On	On
575	Info	Asset Value Updated	On	On
576	Error	Report Uninstall Failed	On	On
577	Error	Report Uninstalled	On	On
580	Warning	Application Type Port List Misconfiguration	On	On
581	Warning	Application Type Port List Misconfiguration Resolved	On	On
582	Warning	DPI Rules Require Configuration	On	On
583	Info	DPI Rules Require Configuration Resolved	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
590	Warning	Scheduled Task Unknown Type	On	On
700	Info	Client Plug-in Software Installed	On	On
701	Error	Client Plug-in Software Installation Failed	On	On
702	Info	Credentials Generated	On	On
703	Error	Credential Generation Failed	On	On
704	Info	Activated	On	On
705	Error	Activation Failed	On	On
706	Info	Client Plug-in Software Upgraded	On	On
707	Warning	Client Plug-in Software Upgrade Failed	On	On
708	Info	Deactivated	On	On
709	Error	Deactivation Failed	On	On
710	Info	Events Retrieved	On	On
711	Info	Client Plug-in Software Deployed	On	On
712	Error	Client Plug-in Software Deployment Failed	On	On
713	Info	Client Plug-in Software Removed	On	On
714	Error	Client Plug-in Software Removal Failed	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
715	Info	Client Plug-in Version Changed	On	On
720	Info	Updated	On	On
721	Error	Update Failed	On	On
722	Warning	Get Interfaces Failed	On	On
723	Info	Get Interfaces Failure Resolved	On	On
724	Warning	Insufficient Disk Space	On	On
725	Warning	Events Suppressed	On	On
726	Warning	Get Client Plug-in Events Failed	On	On
727	Info	Get Client Plug-in Events Failure Resolved	On	On
728	Error	Get Events Failed	On	On
729	Info	Get Events Failure Resolved	On	On
730	Error	Offline	On	On
731	Info	Back Online	On	On
732	Error	Firewall Rule Engine Offline	On	On
733	Info	Firewall Rule Engine Back Online	On	On
734	Warning	Computer Clock Change	On	On
735	Warning	Misconfiguration Detected	On	On
736	Info	Check Status Failure Resolved	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
737	Error	Check Status Failed	On	On
738	Error	DPI Rule Engine Offline	On	On
739	Info	DPI Rule Engine Back Online	On	On
740	Error	Client Plug-in Error	On	On
741	Warning	Abnormal Restart Detected	On	On
742	Warning	Communications Problem	On	On
743	Info	Communications Problem Resolved	On	On
745	Warning	Events Truncated	On	On
750	Warning	Last Automatic Retry	On	On
755	Info	IDF Server Plug-in Version Compatibility Resolved	On	On
756	Warning	IDF Server Plug-in Upgrade Recommended (Incompatible Security Component(s))	On	On
760	Info	Client Plug-in Version Compatibility Resolved	On	On
761	Warning	Client Plug-in Upgrade Recommended	On	On
762	Warning	Client Plug-in Upgrade Required	On	On
763	Warning	Incompatible Client Plug-in Version	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
764	Warning	Client Plug-in Upgrade Recommended (Incompatible Security Component(s))	On	On
765	Warning	Computer Reboot Required	On	On
766	Warning	Network Engine Mode Configuration Incompatibility	On	On
767	Warning	Network Engine Mode Version Incompatibility	On	On
768	Warning	Network Engine Mode Incompatibility Resolved	On	On
770	Warning	Client Plug-in Heartbeat Rejected	On	On
771	Warning	Contact by Unrecognized Client	On	On
780	Info	Scan for Recommendations Failure Resolved	On	On
781	Warning	Scan for Recommendations Failure	On	On
784	Info	Component Update Success	On	On
785	Warning	Component Update Failure	On	On
790	Info	Client Plug-in Initiated Activation Requested	On	On
791	Warning	Client Plug-in Initiated Activation Failure	On	On
800	Info	Alert Dismissed	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
801	Info	Error Dismissed	On	On
850	Warning	Reconnaissance Detected: Computer OS Fingerprint Probe	On	On
851	Warning	Reconnaissance Detected: Network or Port Scan	On	On
852	Warning	Reconnaissance Detected: TCP Null Scan	On	On
853	Warning	Reconnaissance Detected: TCP SYNFIN Scan	On	On
854	Warning	Reconnaissance Detected: TCP Xmas Scan	On	On
900	Info	IDF Server Plug-in Audit Started	On	On
901	Info	IDF Server Plug-in Audit Shutdown	On	On
902	Info	IDF Server Plug-in Installed	On	On
903	Warning	License Related Configuration Change	On	On
910	Info	Diagnostic Package Generated	On	On
911	Info	Diagnostic Package Exported	On	On
912	Info	Diagnostic Package Uploaded	On	On
913	Error	Automatic Diagnostic Package Error	On	On
920	Info	Usage Information Generated	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
921	Info	Usage Information Package Exported	On	On
922	Info	Usage Information Package Uploaded	On	On
923	Error	Usage Information Package Error	On	On
930	Info	Certificate Accepted	On	On
931	Info	Certificate Deleted	On	On
940	Info	Auto-Tag Rule Created	On	On
941	Info	Auto-Tag Rule Deleted	On	On
942	Info	Auto-Tag Rule Updated	On	On
943	Info	Tag Deleted	On	On
970	Info	Command Line Utility Started	On	On
978	Info	Command Line Utility Failed	On	On
979	Info	Command Line Utility Shutdown	On	On
980	Info	System Information Exported	On	On
990	Info	Server Plug-in Node Added	On	On
991	Info	Server Plug-in Node Decommissioned	On	On
992	Info	Server Plug-in Node Updated	On	On
997	Error	Tagging Error	On	On

TABLE C-3. System Events

NUMBER	SEVERITY	EVENT	RECORD	NOTIFY
998	Error	System Event Notification Error	On	On
999	Error	Internal Software Error	On	On
1101	Error	Plug-in Installation Failed	On	On
1102	Info	Plug-in Installed	On	On
1103	Error	Plug-in Upgrade Failed	On	On
1104	Info	Plug-in Upgraded	On	On
1105	Error	Plug-in Start Failed	On	On
1106	Error	Plug-in Uninstall Failed	On	On
1107	Info	Plug-in Uninstalled	On	On

Client Plug-in Events

Client Plug-in Events are displayed within a System Event in the System Events screen. For example, double-clicking the "Events Retrieved" System Event will display a window listing all the Client Plug-in Events that were retrieved.

Events annotated as "Deprecated" are no longer generated by the most recent Client Plug-ins but may still appear if you are running older versions.

TABLE C-4. Client Plug-in Events

NUMBER	SEVERITY	EVENT	NOTES
0	Error	Unknown Client Plug-in Event	
Driver-Related Events			

TABLE C-4. Client Plug-in Events

NUMBER	SEVERITY	EVENT	NOTES
1000	Error	Unable To Open Engine	
1001	Error	Engine Command Failed	
1002	Warning	Engine List Objects Error	
1003	Warning	Remove Object Failed	
1004	Warning	Engine Returned Bad Rule Data	Deprecated
Configuration-Related Events			
2000	Info	Security Configuration Updated	
2001	Warning	Invalid Firewall Rule Assignment	Deprecated
2002	Warning	Invalid Stateful Configuration	Deprecated
2003	Error	Save Security Configuration Failed	
2004	Warning	Invalid Interface Assignment	
2005	Warning	Invalid Interface Assignment	Deprecated
2006	Warning	Invalid Action	
2007	Warning	Invalid Packet Direction	
2008	Warning	Invalid Rule Priority	
2009	Warning	Unrecognized IP Format	Deprecated

TABLE C-4. Client Plug-in Events

NUMBER	SEVERITY	EVENT	NOTES
2010	Warning	Invalid Source IP List	Deprecated
2011	Warning	Invalid Source Port List	Deprecated
2012	Warning	Invalid Destination IP List	Deprecated
2013	Warning	Invalid Destination Port List	Deprecated
2014	Warning	Invalid Schedule	Deprecated
2015	Warning	Invalid Source MAC List	Deprecated
2016	Warning	Invalid Destination MAC List	Deprecated
2017	Warning	Invalid Schedule Length	
2018	Warning	Invalid Schedule String	
2019	Warning	Unrecognized IP Format	Deprecated
2020	Warning	Object Not Found	
2021	Warning	Object Not Found	
2022	Warning	Invalid Rule Assignment	
2050	Warning	Firewall Rule Not Found	Deprecated
2075	Warning	Traffic Stream Not Found	Deprecated
2076	Warning	DPI Rule Not Found	Deprecated
2077	Warning	Pattern List Not Found	Deprecated
2078	Warning	Traffic Stream Conversion Error	Deprecated

TABLE C-4. Client Plug-in Events

NUMBER	SEVERITY	EVENT	NOTES
2079	Warning	Invalid DPI Rule XML Rule	Deprecated
2080	Warning	Conditional Firewall Rule Not Found	Deprecated
2081	Warning	Conditional DPI Rule Not Found	Deprecated
2082	Warning	Empty DPI Rule	Deprecated
2083	Warning	DPI Rule XML Rule Conversion Error	Deprecated
2085	Error	Security Configuration Error	
2086	Warning	Unsupported IP Match Type	
2087	Warning	Unsupported MAC Match Type	
2088	Warning	Invalid SSL Credential	
2089	Warning	Missing SSL Credential	
Hardware-Related Events			
3000	Warning	Invalid MAC Address	
3001	Warning	Get Event Data Failed	
3002	Warning	Too Many Interfaces	
3003	Error	Unable To Run External Command	

TABLE C-4. Client Plug-in Events

NUMBER	SEVERITY	EVENT	NOTES
3004	Error	Unable To Read External Command Output	
3005	Error	Operating System Call Error	
3006	Error	Operating System Call Error	
3007	Error	File Error	
3008	Error	Machine-Specific Key Error	
3009	Error	Unexpected Client Plug-in Shutdown	
3010	Error	Client Plug-in Database Error	
3600	Error	Get Windows System Directory Failed	Deprecated
3601	Warning	Read Local Data Error	Windows error.
3602	Warning	Windows Service Error	Windows error.
3603	Error	File Mapping Error	Windows error. File size error.
3700	Warning	Abnormal Restart Detected	Windows error.
3701	Info	System Last Boot Time Change	Windows error.

TABLE C-4. Client Plug-in Events

NUMBER	SEVERITY	EVENT	NOTES
Communication-Related Events			
4000	Warning	Invalid Protocol Header	Content length out of range.
4001	Warning	Invalid Protocol Header	Content length missing.
4002	Info	Command Session Initiated	
4003	Info	Configuration Session Initiated	
4004	Info	Command Received	
4011	Warning	Failure to Contact Server Plug-in	
4012	Warning	Heartbeat Failed	
Client Plug-in-Related Events			
5000	Info	Client Plug-in Started	
5001	Error	Thread Exception	
5002	Error	Operation Timed Out	
5003	Info	Client Plug-in Stopped	
5004	Warning	Clock Changed	
5005	Info	Client Plug-in Auditing Started	

TABLE C-4. Client Plug-in Events

NUMBER	SEVERITY	EVENT	NOTES
5006	Info	Client Plug-in Auditing Stopped	
5008	Warning	Filter Driver Connection Failed	
5009	Info	Filter Driver Connection Success	
5010	Warning	Filter Driver Informational Event	
Logging-Related Events			
6000	Info	Log Device Open Error	
6001	Info	Log File Open Error	
6002	Info	Log File Write Error	
6003	Info	Log Directory Creation Error	
6004	Info	Log File Query Error	
6005	Info	Log Directory Open Error	
6006	Info	Log File Delete Error	
6007	Info	Log File Rename Error	
6008	Info	Log Read Error	
6009	Warning	Log File Deleted Due To Insufficient Space	
6010	Warning	Events Were Suppressed	

TABLE C-4. Client Plug-in Events

NUMBER	SEVERITY	EVENT	NOTES
6011	Warning	Events Truncated	
6012	Error	Insufficient Disk Space	
Attack/Scan/Probe-Related Events			
7000	Warning	Computer OS Fingerprint Probe	
7001	Warning	Network or Port Scan	
7002	Warning	TCP Null Scan	
7003	Warning	TCP SYNFIN Scan	
7004	Warning	TCP Xmas Scan	

Index

U

W

X