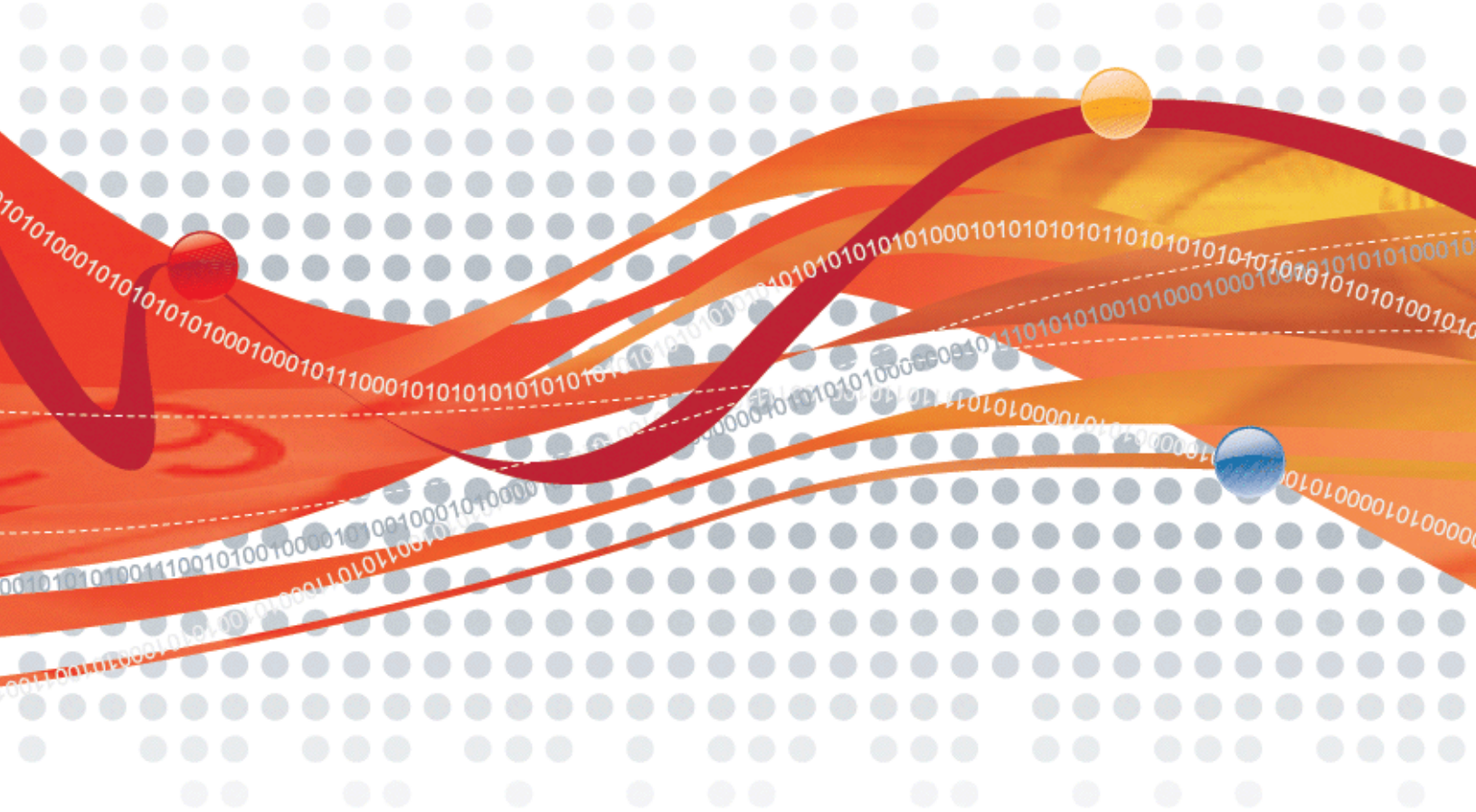
TREND MICRO™

Intrusion Defense Firewall 1.2

for OfficeScan Client/Server Edition

User's Guide



Endpoint Security

Document part number: OSEM83588/80317
Release date: January 2010

Table Of Contents

Introduction

Intrusion Defense Firewall 1.2

Trend Micro™ Intrusion Defense Firewall™ 1.2 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 a IDF Server Plug-in™ and multiple IDF Client Plug-ins™.

IDF Server Plug-in

IDF Server Plug-in ("the Server Plug-in") is a powerful, centralized Web-based management system that allows users to create and manage comprehensive security policies and track threats and preventive actions taken in response to them. All of this can be done in real-time, from the desktop.

Security Profiles

Security Profiles are policy templates that specify the security rules to be configured and enforced automatically for one or more Computers. These compact, manageable rule sets make it simple to provide comprehensive security without the need to manage thousands of rules. Default Security Profiles provide the necessary rules for a wide range of common Computer configurations, ensuring rapid deployment.

Dashboard

The customizable, Web-based UI makes it easy to quickly navigate and drill down to specific information. It provides:

- Extensive system, event and Computer reporting, with drill-down capabilities.
- Graphs of key metrics with trends, with drill-down.
- Detailed event logs, with drill-down, and log forwarding for event correlation with other systems.
- Ability to save multiple personalized dashboard layouts.

Built-in Security

Digital signatures are used to authenticate system components and verify the integrity of rules. Session encryption protects the confidentiality of information exchanged between components.

IDF Client Plug-in

The IDF Client Plug-in ("the Client Plug-in") is a high performance, small footprint, software component that sits directly on a Computer, and defends it by monitoring incoming and outgoing network traffic for protocol deviations or contents that might signal an attack. When necessary, the Client Plug-in intervenes and neutralizes the threat by either blocking or correcting traffic.

Firewall Rules

A sophisticated, bi-directional stateful firewall provides complete support for all network protocols, including TCP, UDP and ICMP. Firewall Rules are fully configurable to allow or deny traffic on a per-interface basis, and restrict communication to allowed IP or MAC addresses.

DPI (Deep Packet Inspection) Rules

Software vulnerabilities are shielded from attack through the use of deep-packet inspection, which examines application data to and from the Computer. DPI Rules allow, block, log, or edit data based on its content. DPI Rules protect vulnerabilities from known and unknown attacks by defining expected application data, and blocking malicious data based on its content.

Ongoing DPI Rule updates automatically provide the most current, comprehensive protection against known and unknown attacks.

Custom Rules

In addition to the rules provided by Trend Micro, clients and integration partners can create rules to support additional protocols or custom applications.

System Requirements

IDF Server Plug-in

- **Memory:** RAM 1GB (2GB recommended)
- **Disk Space:** 1.5GB (5GB recommended)
- **Operating System:** Microsoft Windows Server 2008™ (32- and 64-bit), Microsoft Windows Server 2003™ (SP2 or higher) (32- and 64-bit), Microsoft Storage Server 2003™ (SP2 or higher) (32- and 64-bit), Microsoft Cluster Server 2003™ (SP2 or higher) (32- and 64-bit), Microsoft Windows 2000 Server™ (SP4 or higher) (32-bit)
- **Web Browser:** Microsoft™ Internet Explorer™ 6+ (cookies enabled)
- **Pre-requisites:**
  - **Trend Micro Officescan Server™ Corporate Edition 8.0+**
  - **Trend Micro™ Officescan Plug-in Server Plug-in™** 1.0 Patch 2 (build 1.0.3151) or later
  - **Windows 2008:** Microsoft .NET Framework™ 2.0 or higher (Required for Microsoft SQL Server 2005 Express™ Installation)
  - **Windows 2003:** Microsoft .NET Framework 2.0 or higher (Required for SQL Server 2005 Express Installation)
  - **Windows 2000:** MDAC 2.81, Windows Installer™ 3.1 and Microsoft .NET Framework 2.0 or higher (Required for SQL Server 2005 Express Installation)
  - Adobe™ Acrobat Reader™ 5+ (Required to read deployment guide)

IDF Client Plug-in

- **Memory:** RAM 128MB
- **Disk Space:** 100MB (200MB recommended, primarily for logging)
- **Windows:** Windows 2000™ (32-bit), Windows XP™ (32- and 64-bit), Windows 2003™ (32- and 64-bit), Vista™ (32- and 64-bit), Windows 2008™ (32- and 64-bit), Windows 7™ (32 and 64 bit).

What's New in 1.2

Intrusion Defense Firewall 1.2

Location Awareness

Location Awareness lets users write Rules which can be automatically enabled or disabled depending on the Computer's environment. This is useful for mobile laptops which might require different firewall rules depending on whether they are on or off domain.

Isolated Interfaces

The Isolated Interfaces capability allows users to write rules which only allow one network interface to be active at any one time, thus preventing bridging attacks. Interfaces can be given priorities to set the order in which the Client Plug-in determines which one will be active. The Rules governing isolated interfaces can be associated with Location Awareness.

Navigation Pane

The main navigation pane in the Server Plug-in has a new design that is more robust, faster, and far easier to use.

- Each area of functionality loads independently meaning far improved load times for each window.
- The properties of individual **Computers** and **Security Profiles** are now displayed in a GUI that mirrors the main IDF Server Plug-in window.
- Rules can be assigned to all interfaces on a Computer or to a specific interface only.
- The new Status/Action oriented design means that whatever you want to do with your Computer is only a click or two away. For instance, the **Monitoring** section of the navigation menu has been removed, and you can now get events for each separate module (DPI, Firewall, etc.).
- **Alert Configuration** has been moved from the main navigation tree and can now be found on the **System > System Settings > System** tab.

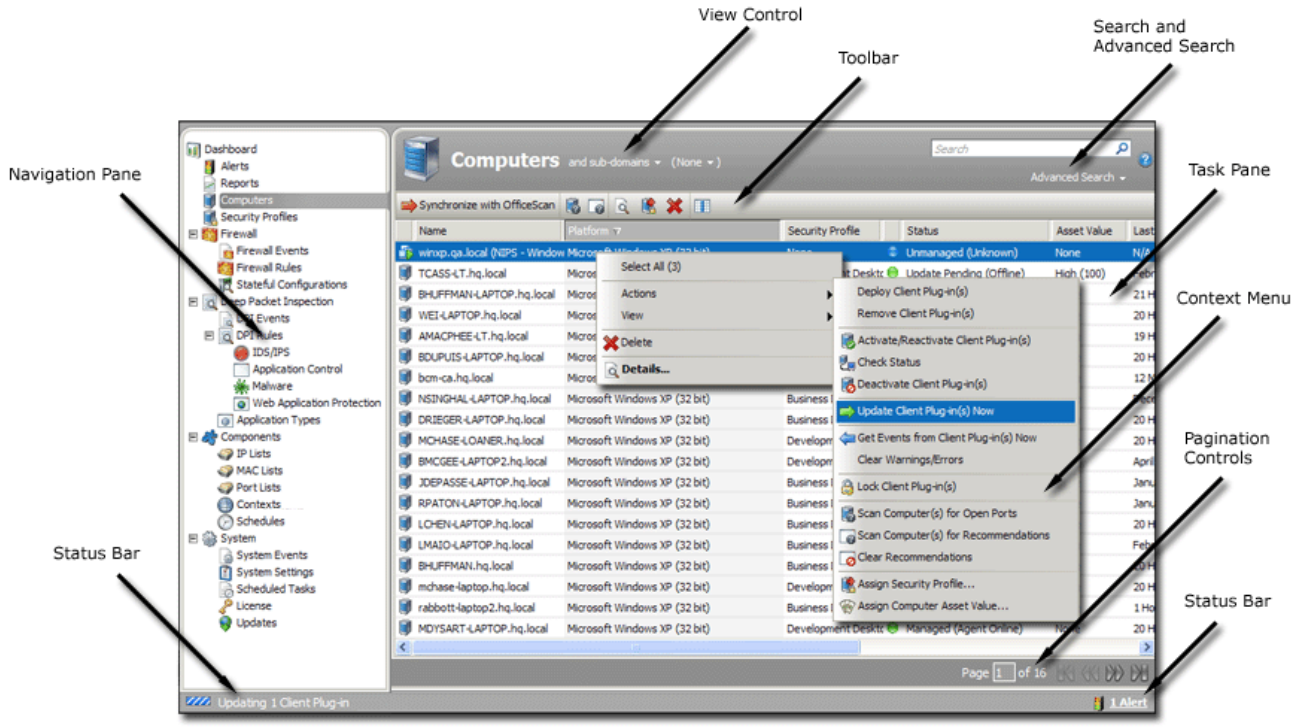
Terminology

- **Intrusion Prevention System (IPS)** has been renamed **Deep Packet Inspection (DPI)** . We have renamed the IPS/IDS functionality as the generic industry-defined term "Deep Packet Inspection" (DPI).
- **Contexts.** These new advanced Components are part of the Location Awareness feature. Contexts can be attached to Firewall Rules and DPI Rules, limiting the Rules so that they will only function in a certain context. This allows Firewall functionality to be enabled or disabled based on various properties of the Computer's environment.
- **License** is a new navigation pane function that enables you to view and change your Trend Micro license information. The update license functionality is no longer available on the **System > Updates** menu.

Server Plug-in Interface

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.



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 Column** 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 type 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 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

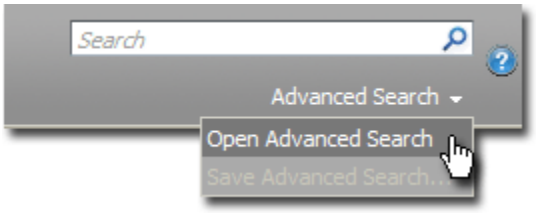
The toolbar holds buttons which carry out various actions specific to the screen you are working in. Most commonly, these will include buttons for the deletion, modification, and creation of list items. Each toolbar has a help button and a sign-out button. Many of the toolbar options are also available from the short-cut 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.

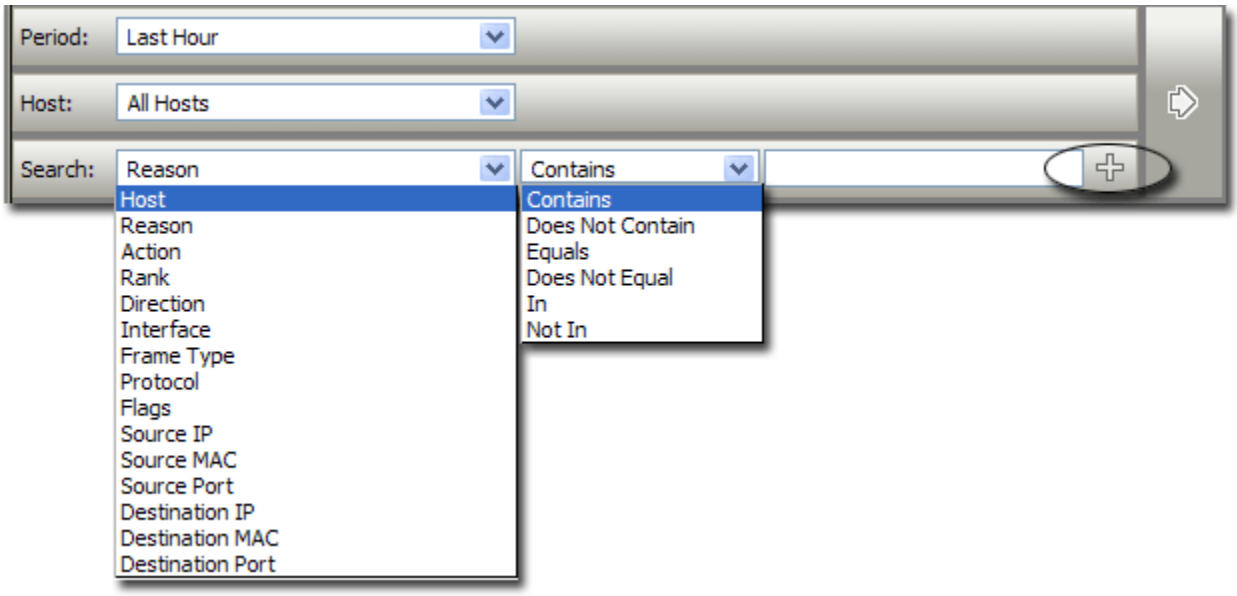
This will search the database for matches among the listed items (Firewall Events on the **Firewall** screen, System Events on the **System Events** screen, etc.) Note that all items will be searched not just the ones currently displayed. For instance, if you are viewing Firewall Events for all Computers 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".



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 Domains or Computer Security Profiles.



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 **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).

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.

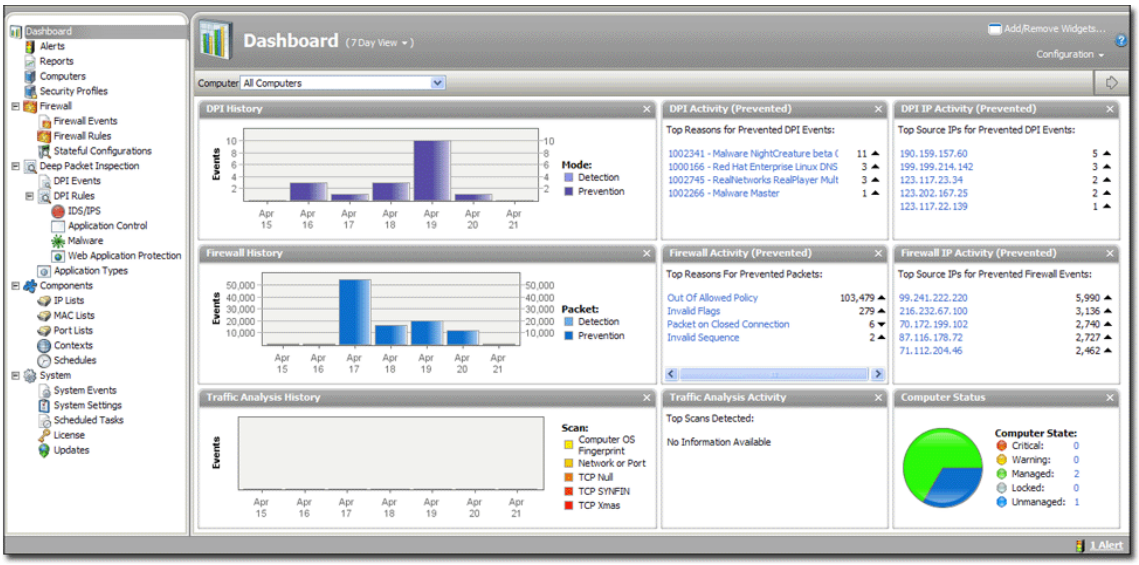
Shortcut Menus

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

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

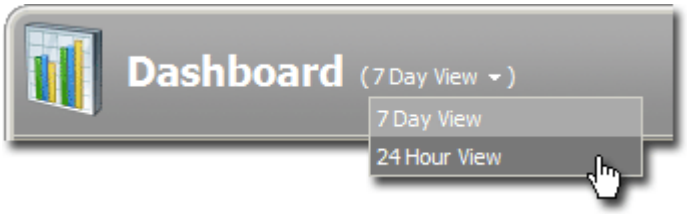
Dashboard

The Dashboard provides a quick at-a-glance view of the state of the IDF system. When logging in to the IDF Server Plug-in, the layout of the Dashboard is preserved from your last session.



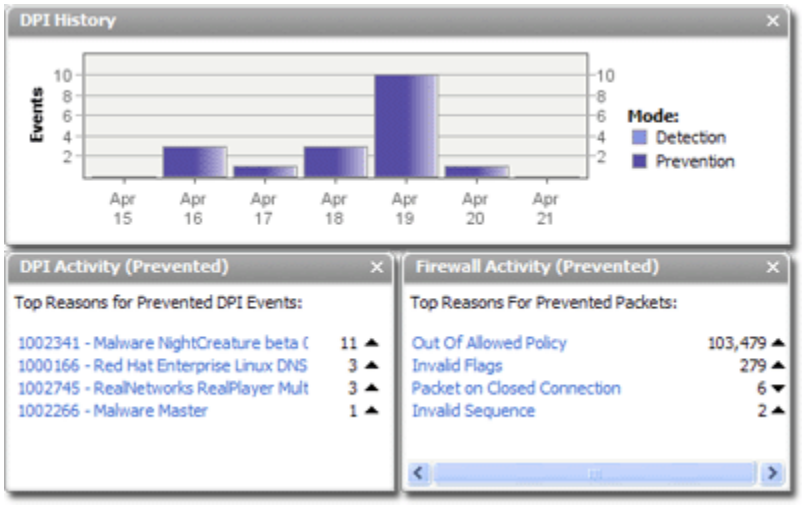
Date/Time Range

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.



"Widgets"

Information panels ("widgets") can be rearranged on the screen by dragging and dropping them to their new locations. Widgets can also be added to or removed from the Dashboard display.



Click **Add/Remove Widgets...** at the top right of the dashboard to view the list of available widgets.

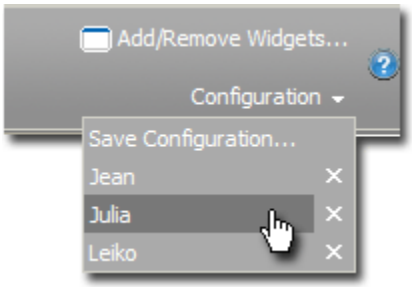
Many widgets contain links to let you "drill down" to the data. For example, clicking a column in the DPI History chart takes you to the **DPI Events** screen listing all the DPI Events that occurred on that day.

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

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.

Saving Dashboard Layouts

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



Alerts

The **Alerts** screen displays all active alerts. Alerts can be displayed in a Summary View (shown below) 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.

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...".

Use the Computers filtering bar to view only alerts for Computers in a particular Domain, with a particular Security Profile, etc.

Reports

IDF Server Plug-in produces reports in PDF, RTF, or XLS (MS Excel) formats. Most of the reports generated by the **Reports** screen have configurable parameters such as date range or reporting by Domain. Parameter options will be disabled for reports to which they don't apply.

Report

The various reports can be output to PDF, RTF, or XLS (MS Excel) format.

Time Filter

You can set the time filter for any period for which records exist. This is useful for security audits.

Computer Filter

Set the Computers whose data will be included in the report.

Encryption

Reports can be password protected.

Computers

The **Computers** screen allows you to manage and monitor the Computers on your network. This screen updates itself periodically.

Synchronize with OfficeScan

Synchronizes the list of Computers with those managed by OfficeScan. (The list is synchronized automatically 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 this button to force a synchronization with OfficeScan while the Server Plug-in is running.)

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.)

Scan Computers for Open Ports

Scan Computers performs a port 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.)

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.

Scan 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 the help for the **Computer Details** screen for more information.

Assign a Security Profile to a Computer

This opens a window with a drop-down list allowing you to assign a Security Profile to the Computer. The name of the Security Profile assigned to the Computer will appear in the **Security Profile** column in the Computers list.

Note that 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.

Search 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

Deploy Client Plug-in

Install a Client Plug-in on the OfficeScan client. The Client Plug-in will activate automatically.

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

Remove Client Plug-in

Remove the Client Plug-in from the OfficeScan client.

Activate/Reactivate the Client Plug-in on a Computer

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 "Online". 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.

Check the Status of a Computer

This command simply checks the status of a Computer without performing a scan or activation attempt.

Deactivate the Client Plug-in on a Computer

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 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.)

Update 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 that 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.

Get Events from Computer(s)

Override the normal event retrieval schedule (usually every heartbeat) and retrieve the Event logs from the Computer(a) now.

Clear Warnings/Errors

This command will clear any warnings or errors generated for a Computer whose Client Plug-in has been reset locally or has simply been removed from the network before a User has had a chance to deactivate or delete the Computer from the Computers List.

Lock a Client Plug-in

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.

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.

Unlock a Client Plug-in

Unlock a locked Computer. (See above.)

Cancel 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.

Clear 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 that this action will not un-assign any rules that were assigned because of past recommendations.

Assign 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**.

Examine Events Associated with a Computer

Examine system and administrative events (that is, non security-related events) associated with a particular Computer.

Examine a Computer's Event Logs

Examine the latest event logs uploaded from the Client Plug-in on this Computer.

Assign 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.

Computer Details

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

Computer Information Screen

General

- **Hostname:** 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 Domain to which the Computer belongs appears in the drop-down list. You can reassign the Computer to any other existing Domain.
- **Security Profile:** The Security Profile (if any) that has been assigned to this Computer.

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 on 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 with client plug-in):** Checking this 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.

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.

Status

- **Computer Status:**
  - When the Computer is unmanaged the status represents the state of the Client Plug-in with respect to activation. The status will display either "Discovered" or "New" followed by the Client Plug-in state in brackets ("No Client Plug-in", "Unknown", "Client Plug-in Reactivate Required", "Client Plug-in Activate Required", or "Client Plug-in Deactivate 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 ("Client Plug-in Online" or "Client Plug-in Offline").
  - When there are errors on the Computer (e.g., "Client Plug-in Offline", "Client Plug-in 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.
- **Client Plug-in:** Indicates whether the Server Plug-in can 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 Client Plug-in Now** button on the **Actions** tab.) When Server Plug-in-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.

Client Plug-in Activation

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 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 a 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.

Client Plug-in Update

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 Client Plug-in Now** button.

Client Plug-in Software

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.

Support

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.

Interfaces

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.

Alerts

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.

Firewall (Firewall Rules, Stateful Configurations)

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 that 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.

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.)

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.

Deep Packet Inspection (Events, Rules, Application Types)

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 **New SSL Computer 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 Assignment:** 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.

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.

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. On 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 ( )

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 ensure your Security Updates are current.

- Examine or modify the **Details** 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 ( )

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**.

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 Computer(s) 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 that the Security Profile will consist only of recommended elements on the Computer, regardless of what Rules are currently assigned to that Computer.

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)".

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.

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 wild-card based interface name match to auto map the interfaces to the appropriate interface type. Examples would be "Local Area Connection *", "eth*", and "Wireless *". An alert is triggered when an interface cannot be mapped automatically. You can map it manually from the **Interfaces** page on the **Computer Details** screen.

 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 that 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.

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 setting in the IDF Server Plug-in 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.

Firewall

The information box 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.

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 on 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 on the **System > System Settings** screen. The default setting is one week.

Firewall Event icons:

-  Single Event
-  Single Event with data
-  Folded Event
-  Folded Event with data

 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.

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 list data to a CSV file
- **Search** () for a particular event

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

- **Computer Details:** View the Details screen of the Computer that generated the log entry
- **Firewall 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 query on the destination IP

Columns for the Firewall 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:** 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. (For a listing of possible packet rejection reasons, see "Packet Rejection Reasons" in the Reference section of this help module.)
- **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", 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.

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.

View Event Properties

Double-clicking an event displays the **Properties** window for that entry which displays all the information about the event on one screen.

Filter the List and/or Search 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 Domains or Computer Security Profiles.

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).

Export...

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

Firewall Rules

Firewall Rules examine the control information that describes an individual packet. They either block or allow that packet based on rules that are defined on these pages. Firewall Rules are assigned directly to Computers or to Security Profiles which are in turn assigned to a Computer or collection of Computers.

Firewall Rule icons:

- Normal Firewall Rules
- Firewall Rules that operate according to a schedule

From the main 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)

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.

Firewall Rule Properties

General Information

- **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:
    1. 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" in the Reference section.
    2. It can **log only**. This means it will only make an entry in the logs and not interfere with the traffic.
    3. It can **force allow** defined traffic (it will allow traffic defined by this rule *without* excluding any other traffic.)
    4. It can **deny** traffic (it will deny traffic defined by this rule.)
    5. It can **allow** traffic (it will *exclusively* allow traffic defined by this rule.)

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**.

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.

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 that 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).

Packet Source

The following options 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 on 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.

Packet Destination

The following options 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.

Specific Flags

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.

Options

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 that 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.

Firewall Rules that are active only at scheduled times are displayed on 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 **Components > Contexts**.

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

Assigned To

This tab displays 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 on the **Security Profiles** screen and to Computers on the **Computers** screen.

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.).

Stateful Configuration icons:

- Normal Stateful Configurations

The **Stateful Configuration** screen lets you define multiple stateful inspection configurations which you can then include in your Security Profiles. From the toolbar or shortcut 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.

Stateful Configuration Properties

General Information

- **Name:** The name of the Stateful Configuration.
- **Description:** Type a description of the Stateful Configuration. This description will only appear here.

IP Packet Inspection

- **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.

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/offset:** 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.

TCP

TCP Packet Inspection

- **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]

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.

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.
- **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.

FTP Options

- **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.

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.

UDP

- **Enable UDP stateful inspection:** Check to enable stateful inspection of UDP traffic.

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.

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.

ICMP

- **Enable ICMP stateful inspection:** Check to enable stateful inspection of ICMP traffic.

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.)

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.

Assigned To

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

Deep Packet Inspection

Deep Packet Inspection

Turn DPI on or off and set the Inline DPI behavior to "Prevent" or "Detect".

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.

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

Recommendations

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 to the Computer and automatically unassign rules that are not required.

To turn the recommendation engine on or off, 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 on 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 on 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:

- **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

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.
- **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.
- **Direction:** The direction of the packet (incoming or outgoing)
- **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", 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.

View Event Properties

Double-clicking an event displays the **Properties** window for that entry.

Filter the List and/or Search 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 Domains or Computer Security Profiles.

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).

Export...

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

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.

DPI Rule icons:

-  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 shortcut 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 the **Configuration** tab. DPI Rules from Trend Micro or third party companies 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.

DPI Rule Properties

General Information

- **Name:** The name of the DPI Rule.
- **Description:** The description of the DPI Rule.
- **Minimum Driver Version:** The minimum version of the IDF Client Plug-in required to implement this DPI Rule.

Details

- **Application Type:** The Application Type this DPI Rule will be grouped under. You can select an existing type, or create a new one.

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. Note that if you check 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.

Events

- **Disable Logging:** Check to disable Event logging.
  - **Generate Event on Packet Drop:** Log the dropping/blocking of a packet.
  - **Generate Event on Packet Modify:** Log the modification of a packet (i.e. if you are replacing a suspicious string of bytes.)
  - **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.

Identification (Displayed for downloaded rules only)

- **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.

Vulnerability (Displayed for downloaded rules only)

Displays 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.)

Configuration (Displayed for downloaded rules only)

- **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.)

DPI Rules that have configuration options are displayed on 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 you've written yourself. (Please contact Trend Micro for information on writing your own DPI Rules.)

Options

Alert

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.

Schedule

Select whether the DPI Rule should only be active during a scheduled time.

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

Context

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 **Components > Contexts**.

Recommendation Options

Use this option to exclude this DPI Rule from Rule recommendations made after Recommendation Scans.

Assigned To

This tab displays the list of Computers and Security Profiles to which this DPI Rule is assigned.

Application Types

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.

Application Type icons:

-  Normal Application Types
-  Application Types that have configuration options

From the main screen you can:

1. Define a **New** ( New) Application Type
2. View or edit the **Properties** () of an existing Application Type
3. **Duplicate** (and then modify) existing Application Types ()
4. **Delete** () an Application Type

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

Application Type Properties

General Information

The name and description of the Application Type. "Minimum Driver Version" tells you what version of the IDF Client Plug-in is required to support this Application Type.

Connection

- **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.)

Assigned To

The **Assigned To** tab lists the DPI Rules associated with this Application Type.

Components

IP Lists

Reusable lists of IPs.

MAC Lists

Reusable lists of MAC addresses.

Port Lists

Reusable lists of ports.

Contexts

Contexts which can specify under what circumstances a Firewall or DPI Rule is in effect or not.

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** () port 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

General Information

The name and description of the IP list.

IPs

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.

Supported Formats

As well as individual addresses, you can type IP ranges and masked IPs. Use these examples to properly format your entries. (Note that you can insert comments into your IP list by preceding the text with a hash sign ("#").)

Assigned To

The **Assigned To** tab lists the 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** ( 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

General Information

The name and description of the list.

MAC(s)

Type the MAC addresses that are going to be on your list. Only put one of these per line.

Supported Formats

The MAC(s) list supports MAC addresses in both hyphen- and colon-separated formats. Use these examples to properly format your entries. (Note that you can insert comments into your MAC list by preceding the text with a pound sign ("#").)

Assigned To

The **Assigned To** tab lists the 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

General Information

The name and description of the list.

Port(s)

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)

Supported Formats

Individual ports and port ranges can be included on the list. Use these examples to properly format your entries. (Note that you can insert comments into your port list by preceding the text with a pound sign ("#").)

Assigned To

The **Assigned To** tab lists the rules making use of this port list. Clicking the names of the rules displays their **Properties** window.

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 on 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. Select the "Context applies when Domain Controller connection is: " option and choose from the following:

- **Local:** true only if the Computer can connect to its domain controller directly
- **Remote (VPN):** true if the Computer can only connect to its domain controller via VPN
- **Not Connected:** true if the Computer cannot connect to its domain controller by any means

By assessing the ability of the Computer to connect with its domain controller, 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 shortcut 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

General Information

The name and description of the Context Rule as well as the earliest version of the IDF Client Plug-in the rule is compatible with.

Options

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.

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 Client Plug-in checks Domain Controller connectivity every ten seconds.

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.)

Assigned To

The **Assigned To** tab displays a list of the rules making use of this Context.

Schedules

Schedules are used by various elements of the IDF system. They are used by the IDF Server Plug-in to determine when Client Plug-in software upgrades can be carried out, as well as to define when particular Firewall Rules are 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.

From the toolbar or the right-click shortcut 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** an 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

Schedule periods are defined by hour-long time blocks. Clicking a time block selects it, and shift-clicking de-selects it.

Assigned To

The **Assigned To** tab displays a list of the IDF system elements making use of this schedule.

System

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.

Scheduled Tasks

The Scheduled Tasks section provides the ability to configure recurring automated 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 check for new updates and software.

System Events

The System Event log is a record of system-related events (as opposed to security-related events). 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

View

Selecting an event and clicking **View** () displays the **Event Viewer Properties** window.

General Information

- **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.
- **Action Performed By:** Will show "Administrator" if the event was initiated by the Administrator.
- **IDF Server Plug-in:** The hostname of the IDF Server Plug-in Computer.

Description

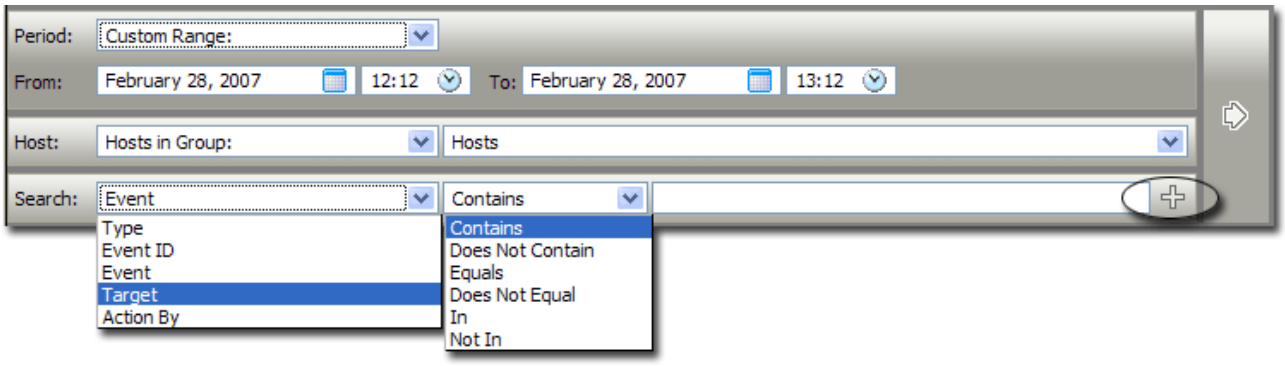
If appropriate, the specific details of what action was performed to trigger this entry in the system event log will be displayed here.

Filter the List and/or Search 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 Domains or Computer Security Profiles.

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



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).

Export

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.

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 system alerts, communications between Client Plug-ins and the Server Plug-in, heartbeat settings, etc.

Note that 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

Communication Direction

- **Bi-directional:** 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-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.


Before configuring a Client Plug-in for Client Plug-in initiated Communication, ensure that the Server Plug-in URL and heartbeat port can be reached by the Client Plug-in. If the Client Plug-in is unable to resolve the Server Plug-in URL or is unable to reach the IP and port, Client Plug-in initiated communications will fail for this Client Plug-in.


Note that 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 hostname **must** be in your local DNS for Client Plug-in initiated or bi-directional 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:

rule 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 enter Packet Source information for IP and/or MAC addresses to restrict traffic to the Computer.

Hostnames

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.)

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 whether Client Plug-in Initiated activations are allowed.

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

Usage: `dsa_control [/a <str>] [/g <str>] [/c <str>] [/r]`		**Notes**
`/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	

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.

Heartbeat

- **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.

Once a **Computer-Clock-Changed** alert is triggered, it must be dismissed manually.

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.) If you uncheck the **Automatically update all affected computers after changing any aspect of the IDF System** option, you will have to find affected Computers in the **Computers** screen, right-click them and choose "Update Client Plug-in(s) Now" from the context menu every time you make a change.

Note that 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.

Scheduler

- **Computer update scheduler period (in minutes):** How often the Client Plug-in on the Computer is updated with the latest settings from the Server Plug-in.
- **Computer retry period (in minutes):** How long should the system wait before again attempting to update a Computer if a previous attempt failed.
- **Number of automatic retry attempts:** Number of times the update will be attempted before the Server Plug-in stops trying to update the Client Plug-in. Whether or not this triggers an alert can be configured "Configure Alerts..." on the Alerts screen.

Local Overrides

This setting is for the use of Trend Micro Professional Services only. Do not change this setting.

Firewall and DPI

Network Engine Mode

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.

Firewall Events

You can set the maximum size of each individual log file and how many of the most recent files are kept. Firewall 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.

- **Maximum size of the event log files (on client plug-in):** (see above)
- **Number of event log files to retain (on client plug-in):** (see above)
- **Collect Firewall Events from Client Plug-in:** Retrieve the latest Firewall Events from the Client Plug-in at every Heartbeat.

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.

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.

The cache is always flushed whenever Events are sent to the IDF Server Plug-in.

- **Log 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.)

DPI Events

You can set the maximum size of each individual log file and how many of the most recent files are kept. DPI 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. DPI 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 DPI Rules in place.

- **Maximum size of the event log files (on client plug-in):** (see above)
- **Number of event log files to retain (on client plug-in):** (see above)
- **Collect DPI Events from Client Plug-in:** Retrieve the latest DPI logs from the Client Plug-in at every Heartbeat.
- **Do Not Record Events with Source IP of:** This option is useful if you want IDF to not make log entries for traffic from certain trusted Computers.

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.

The cache is always flushed whenever Events are sent to the IDF Server Plug-in

- **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.)

Advanced

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.
- **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.

 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 Trend Micro 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.

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 in the Reference section.

- **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.

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 Client Plug-in Debug Events. Note that 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.
- **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

Interface Isolation allows you to force a Computer to use only one interface at any one time. This feature was designed to enable you prevent attackers from bridging across two interfaces. To do so, set the "Enable Interface Isolation" option to type strings that will match the names of the interfaces on a Computer (in order of priority) and then set the "Limit to one active Interface per pattern" option.

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. If so, set the global settings to not use Isolated Interfaces and then override the setting on the Security Profile or the Computer . For more information on overriding settings, see Inheritance and Overrides in the Reference section.

Analysis

The **Analysis** screen allows users to enable and configure traffic analysis settings on all or selected Computers.

- **Detection Enabled:** Turn traffic analysis on or off.
- **Computers/Networks on which to perform traffic analysis:** 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 analyze 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.)

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. (See **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.

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:** 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 SYN, URG, and PSH flags set.

"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 variation that will be detected. If a computer however is acting as a router or bridge it could see traffic 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.

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.

Scan

Scanning for Open Ports

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 on the **Port Lists** screen in the **Components** section.)

Scanning for Recommendations

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

Alert Notification (from the Server Plug-in)

Type 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.)

Firewall and DPI Event Notification (from the Client Plug-ins)

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.

System Event Notification (from the IDF Server Plug-in)

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.

Forward System Events to a Remote Computer (via SNMP)

IDF also supports SNMP. The MIB file ("DeepSecurity.mib") is located in `\Trend Micro\IDF Server Plug-in\util`.

Execute Scripts for System Events

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.

Ranking

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.

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. (Firewall Rule 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.

Computer Asset Values

Computer Asset Values are not associated with any of their other properties like DPI Rules or Firewall Rules. Instead, Computer 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.)

System

SMTP

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. If your SMTP mail server requires outgoing authentication, type the username and password credentials. Once you've entered the necessary information, use the **Test SMTP Settings** to test the settings.

Prune

These settings define how long to store Event records and Counters, older Security Center Updates, and older versions of Client Plug-in software.

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** on 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 on 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.

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.

Export

The encoding used when you export data files from the IDF Server Plug-in.

WHOIS

The whois lookup to be used when logging DPI and Firewall Events.

Scheduled Tasks

The **Scheduled Tasks** screen lets you automate and schedule certain common tasks. From the main screen you can:

- Create **New** scheduled tasks ( New)
- Examine or modify the **Properties** of an existing scheduled task ()
- **Duplicate** (and then modify) existing scheduled tasks ()
- **Delete** a scheduled task ()
- **Run** () a selected scheduled task

Clicking **New** () displays the **New Scheduled Task** wizard which guides you through the simple steps of creating a new scheduled tasks. You will be prompted for different information depending on the type of task: a Computer list if you are automating a port scan, for example, or an email address if you are scheduling the generation of an **Outstanding Alert Summary** email.

Use the **Scheduled Tasks** screen to automate the following common activities:

Download and Apply New Security Updates

Regularly check for Security Updates and download and install them if any are available.

 Note that you can change the way automatically downloaded Security Updates are handled by going to **System > Updates**.

Download New Security Updates

Regularly check for Security Updates and download them without installing them.

Download New IDF Client Plug-ins

Automatically download IDF Client Plug-in software upgrades if they are available. (Downloaded Client Plug-in software is kept in a folder called "IDF Client Plug-ins" in the Server Plug-in's install directory.)

Scan Computers for Recommendations

Schedule periodic Recommendation Scans on one or more Computers.

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.

Backup

Perform regular database backups.

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 your support provider for more information.

License

The purpose of the license page is to check on the status of your current license as well as enter a new Activation Code.

When your license expires you have two potential remedies:

1. You can contact your Trend Micro representative and be issued a new Activation Code.
2. You can renew with your Trend Micro representative and then use the online update which will download the new details based on the Trend Micro activation servers.

Expiry and number of clients are connected into the Alerts so you will be notified when your license is about to expire or the number of clients has exceeded the limit of your license.

There is a different expiry and grace period depending on the license.

Updates

Security Updates

Security Updates are composed of IPS Filters, Firewall Rules, IP Lists, etc. created to protect Computers against the latest vulnerabilities. They are made available periodically by Trend Micro to be downloaded and incorporated into the Server Plug-in. Click the **Download** button to check if new updates are available. If they are, they will be downloaded and deployed to the Client Plug-ins immediately.

This process can be automated from the **System > Scheduled Tasks** screen. For more information on applying and automating Security Center Updates, see How To... Apply Security Center Updates.

Client Plug-in Updates

This panel lets you download and deploy the latest versions of the Intrusion Defense Firewall Client Plug-ins. Click the **Download** button check if new Client Plug-ins are available. If they are they will be downloaded and stored locally. When you are ready, click the **Deploy Latest** button to upgrade all managed Computers to the latest version of the Client Plug-in.

The panel also displays the latest versions of the Client Plug-ins and how many of your managed Computers are running the latest versions.

Server Diagnostics

Clicking **Generate Diagnostics Package...** displays the **Diagnostic Package Wizard** which will create a zip file containing Install/Uninstall and Debug Logs, System Information, Database Contents (last hour only for time-sensitive items), and a File Listing. This information can be given to your support provider to help troubleshoot any problems.

How To...

How To...

Customize the Dashboard

How to customize and save the layout of the Dashboard.

Secure IDF Server Plug-in

Some suggestions on securing the Computer on which IDF Server Plug-in is running.

Configure Server Plug-in-Client Plug-in Communications

A description of Server Plug-in-Client Plug-in communications in the IDF System and how to configure it.

Configure Logging

Some tips on reducing the space and resources taken up by logging.

Set Up Email Alerts

Configuring email alerts.

Configure Notifications

Configuring the Server Plug-in to work with third-party notification systems.

Configure Syslog Integration

How to send IDF's logs to a Syslog Server.

Configure Alerts

Configuring how the Server Plug-in behaves when particular alerts are triggered.

Configure Port Scan Settings

How to set which (if any) ports are scanned during the IDF Server Plug-in's periodic port scans of its managed Computers.

Apply Updates

Information about Applying Updates and how to keep up to date.

Filter SSL Data Streams

How to configure IDF to analyze SSL encrypted traffic.

Backup and Restore IDF

How to backup and restore your data.

Configure Alerts

There are just over thirty conditions that trigger Alerts in the IDF system. Generally Alerts exists to warn of system status anomalies like 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.)

Alerts can be viewed by going to the **Alert** screen and clicking "Configure Alerts..." at the top-right of the screen, or going to **System > System Settings > System** and clicking "View Alert Configuration".

The actions precipitated by each alert can be configured by opening the **Properties** window for the alert. Alerts can be turned on or off; their severity can be switched between Warning and Critical.

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

You also have the option to specify a default email address to which all email alerts will be sent. This option is found on the **System > System Settings > Notifications** screen.

Note that for the emails to be sent, you must configure the SMTP settings on the **System > System Settings > System** screen.

Configure Server Plug-in-Client Plug-in Communications

Who Initiates Communication

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**.


The following information is collected by the Server Plug-in during a heartbeat: the status of the drivers (on- or off-line), the Client Plug-in's status (including clock time), Client Plug-in logs since the last heartbeat, data to update counters, and a fingerprint of the Client Plug-in's 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 **Client Plug-in Communication** 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 was specified on 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 **Computer 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 was specified on its Security Profile's **Details** window or on 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 that 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 hostname **must** be in your local DNS for Client Plug-in initiated or bi-directional communication to work.

Customize the Dashboard

The Dashboard is the first screen that comes up after you log in to the IDF Server Plug-in. 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, regardless of whether another User has logged in the meantime and made changes to their layout.)

Configurable elements of the Dashboard display are the time period the data is taken from, which Computers' or Domains' data is displayed, which "widgets" are displayed, and the layout of those widgets on the screen.

Time Period

Choose between displaying data for the last seven days or 24 hours.

Computers and Domains

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

Select Dashboard Widgets

Click **Add/Remove Widgets...** to display the widget selection window and choose which widgets to display.

Changing the Layout

The selected widgets can be moved around the dashboard by dragging them by their title bar. Move the widget over an existing one and they will exchange places. (The widget that is about to be displaced will temporarily gray out.)

Save and Manage Dashboard Layouts

Click **Configuration...** to save, load, or delete a dashboard layout.

Set Up Email Alerts

IDF Server Plug-in can send emails 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.

Configuring your SMTP Settings

The SMTP configuration panel can be found in **System > System Settings > System**.

Type the address of your SMTP mail (with the port if required). Type 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. If your SMTP mail server requires outgoing authentication, type the username and password credentials. Once you've entered the necessary information, use the **Test SMTP Settings** to test the settings.

Configuring which Alerts should 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 which alerts trigger the sending of an email, go to the **System** tab on the **System > System Settings screen**. Click "View Alert Configuration" to display the list of all alerts. The checkmark next to the alert 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. Double-click an alert to view its **Alert Configuration** screen.

To have an alert trigger an email, it must be turned "On" and at least one of the "Send Email" checkboxes must be selected.

Specifying an email address

Type the email address to which Alert Notification will be sent on the **System > Settings > Notifications** screen.

Backup and Restore IDF

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

1. All Logs and Events
2. Security Profiles
3. IPS Filters
4. Firewall Rules
5. Stateful Configurations
6. All Components (IP Lists, MAC Lists, Port Lists, etc.)
7. Alert Configurations
8. System Settings
9. The configurations of the Client Plug-ins on all Computers

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"
```


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.

E.g. 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"
```

Configure Logging

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 60 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 on 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.

Configure 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-ins 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 Events (from the Client Plug-ins), and one for System events (from the Server Plug-in).

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\IDF Server Plug-in\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.

Configure Port Scan Settings

The IDF Server Plug-in can be instructed to scan a Computer for open ports by right-clicking the Computer and selecting **Actions > Scan Computer for Open ports**, or by clicking the **Scan for Open Ports** button on the **Firewall** screen of the Computer's **Details** window (where the results of the latest scan are displayed).

(Port scans can also be initiated by right-clicking an existing Computer on the **Computers** screen and choosing "Scan Computer for Open Ports". Another way to initiate port scans is to create a **Scheduled Task** to regularly carry out port scans on a list of Computers.)

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.

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.

Configure Syslog Integration

IDF supports SIEM integration through syslog. Syslog is a method of forwarding log information over an IP network, typically using UDP, to a Syslog server listening on port 514.

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, go to the **System > System Settings** screen and click the **Notifications** tab. In the panel called "System Event Notification",

1. place a check in the "Forward System Events to a remote Computer (via Syslog) " checkbox,
2. enter the hostname or the IP address of the Syslog computer,
3. enter which UDP port to use (usually 514),
4. select which Syslog facility to use (Local4 from the Red Hat example above),
5. select the log format (Trend Micro, or Common Event Format (CEF))

Common Event Format (CEF) is a format sponsored by Arcsight (www.arcsight.com). The specification can be found on 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 on the **Computers** screen and double-

click it to view its **Details** window. Got 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 :" radio button 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

The Client Plug-in sends two types of logs to Syslog: Firewall Event Logs, and DPI Event Logs. Firewall Event Logs are prefixed with "dsa_mpf:" and DPI Event Logs are prefixed with "dsa_mpld:". The content of the log is a space-separated string (comma-separated prior to version 4.5) containing additional information.

Note that 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

The Client Plug-in follows the format used by **netfilter/iptables** as closely as possible, and adds several Trend Micro specific fields. Fields are delimited by a single space character, and consist of a TOKEN or a TOKEN=value string. The value string will never contain space characters. In the case of items such as rule names or network interface names, space characters are converted to underscores.

Name	Description	Examples
Reason	The "REASON=" field contains either a built-in string or the string "PKT:" followed by the name of the Firewall Rule that caused the log. Space characters in the Firewall Rule name are converted to underscores.	REASON=Unsolicited_UDP REASON=PKT:Block_Incoming_NetBIOS_broadcasts
Interface Information	Interface name and Ethernet frame information. The IN=, OUT=, and MAC= fields are always present. If the packet is an incoming packet the interface name follows IN=, and the OUT= field contains nothing. The opposite is true for outgoing packets. The MAC= field consists of 14 two-digit hex characters. The first six are the destination MAC address, the next six are the source MAC address, and the last two are the Ethernet frame type.	IN=LAN_-_Gigabit OUT= MAC=FF:FF:FF:FF:FF:FF:00:80:C8:38:79:E3:08:00 IN= OUT=eth2 MAC=00:11:95:B9:A5:AD:00:11:95:B9:A5:B4:08:00
IP Information	For IP packets, the source and destination IPs in numeric form.	SRC=192.168.5.9 DST=192.168.5.255 SRC=192.168.5.8 DST=192.168.5.255
Packet Length	The LEN= field gives the length of the received packet.	LEN=216 LEN=92
Fragmentation	The "DF" field is present if the	DF

Information	IP Don't Fragment bit was set. The "MF" field is present if the IP More Fragments bit was set. The "FRAG=nnn" field contains the fragment offset value.	MF FRAG=22
Protocol	The "PROTO=" field contains the name of the protocol, or its numeric format (in decimal) if it's not one of the well known values.	PROTO=TCP PROTO=UDP PROTO=ICMP
Ports	The "SPT=" and "DPT=" fields contains source and destination ports, if applicable to the protocol type.	SPT=137 DPT=137 SPT=41794 DPT=3328
TCP Flags	For the TCP protocol, the URG, ACK, PSH, RST, SYN, FIN fields are present if the corresponding TCP header bit was set. The "RES=0xNN" field is always present and contains the value of the reserved TCP bits. The ECN flags "CWR" and "ECE" will show up in the two least significant bits of this field.	RES=0x00 ACK RES=0x00 SYN ACK
ICMP Flags	For the ICMP protocol, the "TYPE=N" field contains the ICMP type (in decimal) and the "CODE=N" field contains the ICMP code (in decimal).	TYPE=11 CODE=0 TYPE=8 CODE=0
IP Datagram Length	The "IPDGLEN=N" field contains the length of the IP datagram in decimal format.	IPDGLEN=0 IPDGLEN=60

DPI Event Log Format

As with the Firewall Rule syslog format, the Client Plug-in follows the format used by **netfilter/iptables** as closely as possible, and adds several Trend Micro specific fields.

Fields are delimited by a single space character, and consist of a TOKEN or a TOKEN=value string. The *value* string will never contain space characters. In the case of items such as rule names or network interface names, space characters are converted to underscores.

Name	Description	Examples
Reason	The "REASON=" field contains either a built-in string or the string "PLD:" followed by the name of the DPI Rule that caused the log. Space characters in the DPI Rule name are converted to underscores.	REASON=PLD:Log_HTTP_GET_commands REASON=URI_Path_Length_Too_Long
Direction	The direction of the data flow.	FWD REV

Interface Information	Interface name and Ethernet frame information. The IN=, OUT=, and MAC= fields are always present. Unlike the Firewall Event logs, the DPI Event logging doesn't log packets on an incoming/outgoing basis, but based on their connection flow direction (FWD or REV). In order to stick with netfilter/iptables interface logging conventions, the Client Plug-in looks at the DPI Rule definition. If the DPI Rule is an incoming rule the interface name follows IN=, and the OUT= field contains nothing. The opposite is true for outgoing DPI Rules. The MAC= field consists of 14 two-digit hex characters. The first six are the destination MAC address, the next six are the source MAC address, and the last two are the Ethernet frame type.	IN=LAN_-_Gigabit OUT= MAC=FF:FF:FF:FF:FF:FF:00:80:C8:38:79:E3:08:00 IN= OUT=eth2 MAC=00:11:95:B9:A5:AD:00:11:95:B9:A5:B4:08:00
IP Information	The source and destination IPs in numeric form.	SRC=192.168.5.9 DST=192.168.5.255 SRC=192.168.5.8 DST=192.168.5.255
Protocol	The "PROTO=" field contains the name of the protocol, or its numeric format (in decimal) if it's not one of the well known values.	PROTO=TCP PROTO=UDP PROTO=ICMP
Ports	The "SPT=" and "DPT=" fields contains source and destination ports, if applicable to the protocol type.	SPT=137 DPT=137 SPT=41794 DPT=3328
TCP Flags	For the TCP protocol, the URG, ACK, PSH, RST, SYN, FIN fields are present if the corresponding TCP header bit was set. The "RES=0xNN" field is always present and contains the value of the reserved TCP bits. The ECN flags "CWR" and "ECE" will show up in the two least significant bits of this field.	RES=0x00 ACK RES=0x00 SYN ACK
ICMP Flags	For the ICMP protocol, the "TYPE=N" field contains the ICMP type (in decimal) and the "CODE=N" field contains the ICMP code (in decimal).	TYPE=11 CODE=0 TYPE=8 CODE=0
IP Datagram Length	The "IPDGLEN=N" field contains the length of the IP datagram in decimal format.	IPDGLEN=0 IPDGLEN=60
Action	The "ACTION" field contains the action taken by the DPI Rule. It contains one of the strings "Block", "Reset", "Insert", "Delete", "Replace", "Log". If the rule or the DPI engine is operating in detect-only mode, the action value will be preceded by "IDS:".	ACTION=Log ACTION=IDS:Block

Status	The "STATUS" field contains the decimal format code for the DPI engine error. 0 is used for no error and values < 0 represent internal error codes.	STATUS=0 STATUS=-500
Position	The "POS" field contains the relative position of the event in the input buffer.	POS=9 POS=37
Stream Position	The "SPOS" field contains the absolute position of the event in the data stream, i.e., this is the Nth byte seen in that direction on this connection.	SPOS=128 SPOS=20
Note	The optional "NOTE" field contains a short binary or text note associated with the DPI Rule. For edits this gives the amount of data deleted, inserted or replaced and up to 16 bytes of it. For a drop or log action this is the argument to drop/log (up to 16 bytes). 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.	NOTE=Drop_data

Flags	The "FLAGS" field contains various flags combined together in a single decimal value. The bits that make up the value are:
	`dataTruncated: 1 means data could not be logged`
	`logOverflow: 2 logs overflowed after this log`
	`suppressed: 4 logs threshold suppression occurred after this entry`
	`haveData: 8 contains packet data (data is not included in syslog output)`
	`refData: 16 references previously logged data`
		FLAGS=0
		FLAGS=9

System Event Log Format

System Events are displayed in Syslog with a Date, Time, Priority, Hostname, and a Message. The contents of the Message column depend on whether the IDF Server Plug-in has been configured to send the data using Trend Micro's format (IDF Server) or Common Event Format (CEF). CEF is a standard sponsored by Arcsight (www.arcsight.com). The following table describes the Trend Micro syslog format. For information on CEF, please visit Arcsight's Web site to download the specification.

Name	Description	Examples
Time/Date and IDF Server Node	The time and date the event occurred and the Server Plug-in node on which it occurred.	Jun 8 11:00:08 mckinley-lab IDF Server Jun 8 11:00:38 mckinley-lab CEF
EVENTNUMBER	Numeric ID of the Event.	701 (The list of System Events elsewhere in this reference section includes the Event number.)
TITLE	Title of the Event.	User signed in. Alert ended. DPI Rule updated.
TARGET	The target (if applicable) of the Event.	This can be a username, a hostname, a DPI Rule, etc. depending on the nature of the event.
ACTIONBY	Which entity initiated the Event.	This will be either "System" or the username of a User.
DESCRIPTION	A textual description of the details of the Event.	Alert: Client Plug-in Offline Severity: Critical User signed in from 10.0.1.20 06-08-2007 10:56:17 Local0.Info 127.0.0.1 Jun 8 10:56:17 jean-laptop IDF Server: EVENTNUMBER=710 TITLE=Client Plug-in Events Retrieved TARGET=jean-laptop ACTIONBY=System DESCRIPTION=Client Plug-in Event(s): Client Plug-in Time: June 8, 2007 10:48:52 Type: Info Event ID: 2000 Client Plug-in Event: Security Configuration Updated Description: Security configuration updated. Client Plug-in Time: June 8, 2007 10:48:51 Type: Info Event ID: 5005 Client Plug-in Event: Client Plug-in Auditing Started Description: Client Plug-in auditing started. Client Plug-in Time: June 8, 2007 10:48:51 Type: Info Event ID: 5000 Client Plug-in Event: Client Plug-in Started Description: Client Plug-in started. The client plug-in's version number is 5.0.0.1845. The client plug-in is using its own private copy of OpenSSL 0.9.8d 28 Sep 2006. Client Plug-in Time: June 8, 2007 10:30:14 Type: Info Event ID: 5003 Client Plug-in Event: Client Plug-in Stopped Description: Client Plug-in stopped. Client Plug-in Time: June 8, 2007 10:30:14 Type: Info Event ID: 5006 Client Plug-in Event: Client Plug-in Auditing Stopped Description: Client Plug-in auditing stopped. Client Plug-in Time: June 8, 2007 10:27:03 Type: Info Event ID: 5005 Client Plug-in Event: Client Plug-in Auditing Started Description: Client Plug-in

Apply 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.)

Go to **System > Updates**. This screen will display the date and time of the last check for updates, the version number of the currently applied update, and the version number of the latest available update.

To manually check for, download, and apply the latest Security Updates:

1. Click the **Download** button to check for and retrieve the latest update.
2. Once the update is downloaded, click the **View 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 that you can revert to a previous Security Update by selecting it and clicking **Revert** in the menu bar.

To automatically check for and download the latest Update:

5. Navigate to the **System > Scheduled Tasks** screen
6. Click **New** on the tool bar to open the **New Scheduled Task** Wizard
7. Select "Download New Security Updates" from the drop-down menu
8. Follow the steps in the wizard to select how often and at what time to carry out this task

Updates will be automatically downloaded, but you will still have to apply them using the procedure described above.

To automatically check for, download, and apply the latest Security Updates:

1. Navigate to the **System > Scheduled Tasks** screen
2. Click **New** on the tool bar to open the **Scheduled Tasks** Wizard
3. Select "Download and Apply New Security Updates" from the drop-down menu
4. Follow the steps in the wizard to select how often and at what time to carry out this task

The Server Plug-in will download and apply updates as they become available.

Backup and Restore IDF

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

1. All Logs and Events
2. Security Profiles
3. IPS Filters
4. Firewall Rules
5. Stateful Configurations
6. All Components (IP Lists, MAC Lists, Port Lists, etc.)
7. Alert Configurations
8. System Settings
9. The configurations of the Client Plug-ins on all Computers

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"
```


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.

E.g. 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"
```

Uninstall IDF

Neither the IDF Server Plug-in nor the IDF Client Plug-in can be uninstalled using the Control Panel Add or Remove Programs applet.

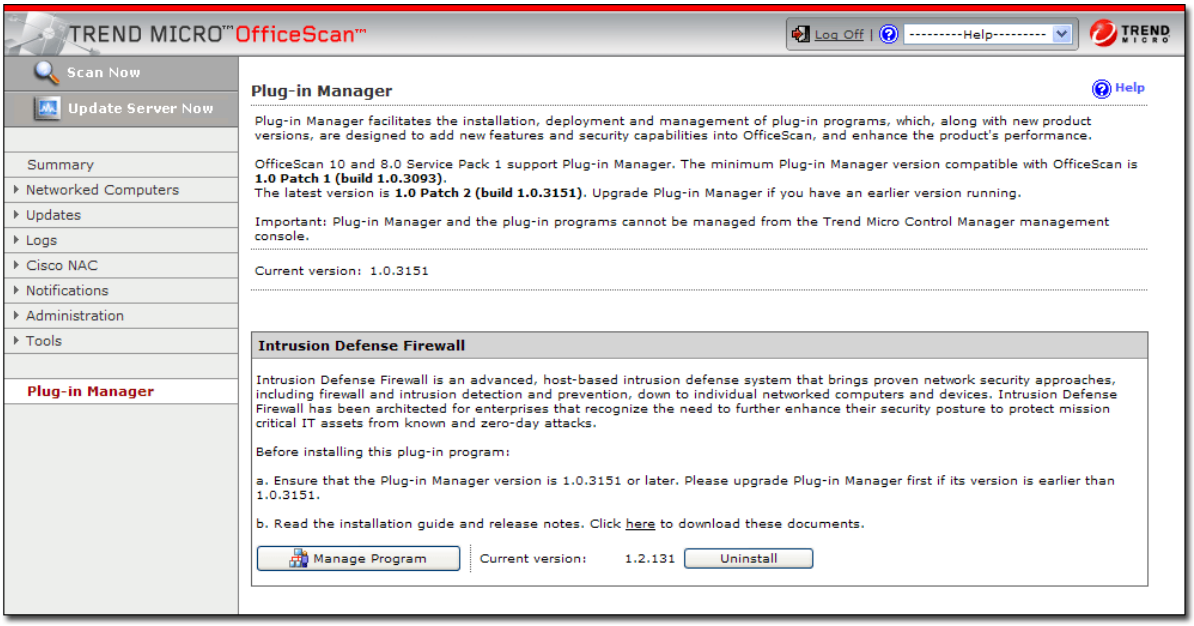
Client Plug-in

1. Using the IDF Server Plug-in, go to the **Computers** screen.
2. Right-click the Computer from which you want to remove the Client Plug-in.
3. Select Actions > Remove Client Plug-in.

If you cannot use the Server Plug-in to communicate with the Client Plug-in, see Manually Uninstall a Client Plug-in in the "How To..." section.

Server Plug-in

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



Upgrade 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.

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.)

Manually Deactivate a 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.

On the client machine:

1. 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 that the Computer is now no longer being protected by the Intrusion Defense Firewall filters and rules.)

Manually Uninstall a Client Plug-in from a Computer

On the client machine:

1. 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
```

Migrate 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.

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.

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

1. Backup 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.

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$87251922972564e6bb3e2da9e688cd4ceb42b9bf
b17a942c3c8ad99ff05938c81
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
```

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.

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.

Migrate 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.

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 How To... Backup and Restore Intrusion Defense Firewall) 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 How To... Backup and Restore Intrusion Defense Firewall.
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 How To... Backup and Restore Intrusion Defense Firewall.
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.

Migrate 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 How To... Backup and Restore Intrusion Defense Firewall).

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.

Optimize 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 limitation of 4GB

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 “Migrate to a Larger Database” in the **How To..** section of the online help for instructions.) Please 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. The on-line help includes information on creating scheduled backups. See "Export or Backup Data" in the **How To...** section of the online help.

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->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 we notice they 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)
```

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".

Migrate IDF data from the bundled SQL Server Express onto another database

A set of migration steps have been established (see "Migrate to a Larger Database" in the **How To...** section of the online help). Please contact your support provider team for additional assistance.

Use the Stand-alone Client Plug-in Installer

The IDF Stand-alone Client Plug-in Installer package is a self-extracting .exe 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 stand-alone 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 Stand-alone Client Plug-in Installer:

1. Extract idfclient.exe from the stand-alone zip package.
2. Run `idfclient.exe` on the target computer. (The exe is a self-extracting zip file that will extract the necessary binaries and scripts to a temporary location and execute them.) It will log to `%WINDIR%\idf_standalone.log`
3. Verify the client is listed on the **Computers** screen and that its status is "Managed".

Because the stand-alone installer will briefly interrupt the client's network connection, the installer *must* be run locally on the host computer.

Reference

Protecting a Mobile Laptop Computer

In this guide, we will use the Server Plug-in to protect a mobile laptop. This will involve the following steps:

1. Activate the Client Plug-in on the laptop computer.
2. Create a new Security Profile for a Windows laptop
    a. Create a new Security Profile
    b. Assign Firewall and Stateful Configuration Rules with Location Awareness Conditions
    c. Assign Deep Packet Inspection (DPI) Rules
3. Apply Security Profiles to the Computer
4. Monitor Activity using the Server Plug-in

We will assume that you have already installed the Server Plug-in on the Computer from which you intend to manage the IDF Client Plug-ins throughout your network. We will also assume that **you have installed (but not activated) IDF Client Plug-ins on the mobile laptops you wish to protect**. If you have not done so, consult the installation instructions for the steps to get to this stage.

Activate the Client Plug-in on a Computer

Client Plug-ins need to be activated by the Server Plug-in before rules can be assigned to them. The activation process includes the exchange of unique "fingerprints" between the Client Plug-in and the Server Plug-in. This ensures that only this IDF Server Plug-in (or one of its nodes) can send instructions to the Client Plug-in.

To manually activate a Client Plug-in on a Computer, right-click one or more selected Computers and select **Actions > Activate/Reactivate Client Plug-in(s)**.

Create a Security Profile

Now that the Client Plug-in is activated, we can assign some rules to protect the Computer. Although you can assign rules directly to a Computer, it's more useful to create a Security Profile which contains these rules and which can then be assigned to multiple Computers.

Creating the Security Profile will involve the following steps:

1. Creating and naming the new Security Profile
2. Defining Multiple Interface Types
3. Setting the Firewall to Inline Mode
4. Assigning Firewall Rules with Location Awareness
5. Assigning Deep Packet Inspection (DPI) Rules
6. Assigning the Security Profile to the Computer

Creating and Naming the New Security Profile

To create a new Security Profile:

1. Click **Security Profiles** in the Server Plug-in's navigation pane, and then click "New" to display the **New Security Profile** wizard.
2. Name the new Security Profile "My New Laptop Security Profile". Click **Next.**
3. The next screen asks if you would like to base the Security Profile on an existing Computer's current configuration. If you were to select "Yes", you would be asked to pick an existing

managed Computer and the wizard would take all the configuration information from that Computer and create a new Security Profile based on it. This can be useful if, for instance, you have fine-tuned the security configuration of an existing Computer over a period of time and now wish to create a Security Profile based on it so that you can apply it to other functionally identical Computers. For now, select "No" and click **Next**.

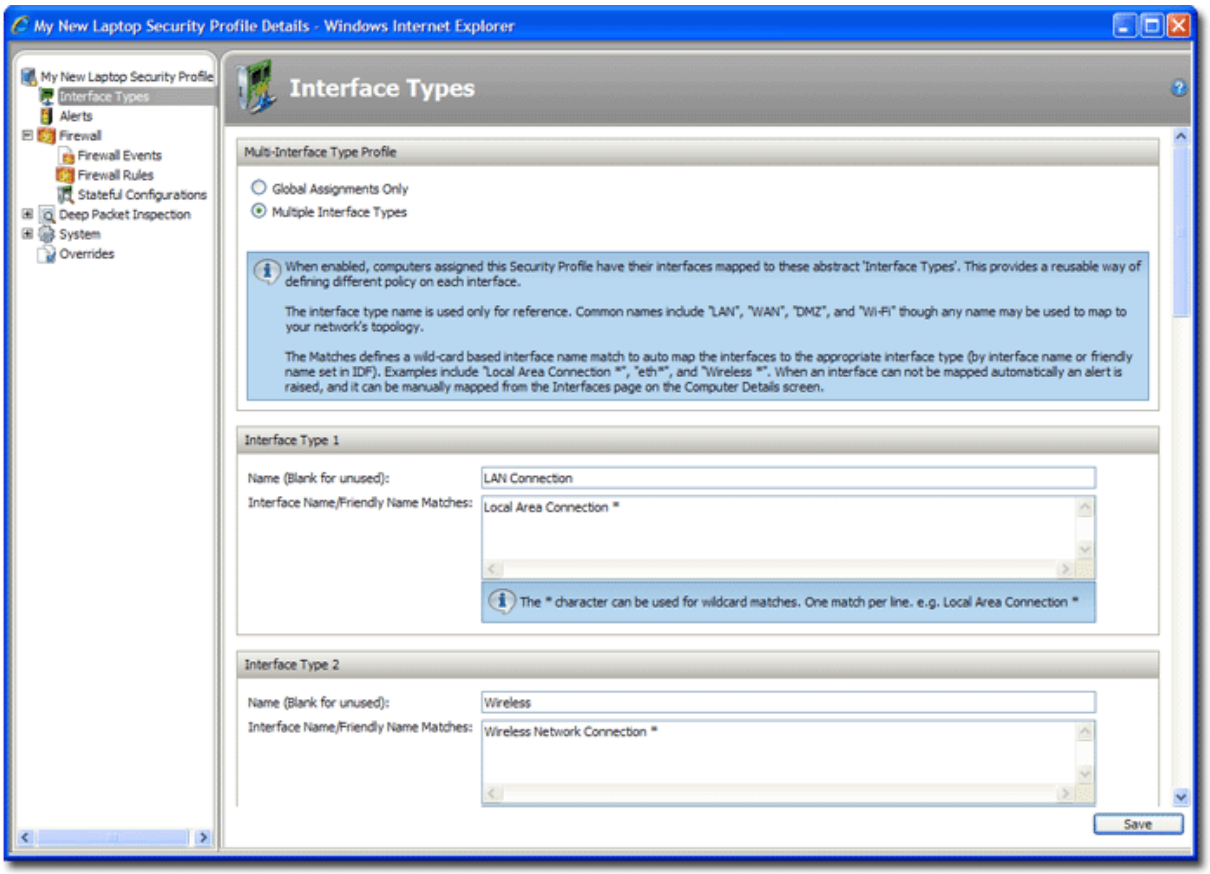
4. The final screen confirms that the new Security Profile has been created. Set the **Open Security Profile Details on 'Close'** option and click **Close**.
5. Because you set the **Open Security Profile Details on 'Close'** option, the new Security Profile's **Details** screen appears.

Defining Multiple Interface Types

Let's assume that the laptops to which this Security Profile will be assigned are equipped with two network interfaces (a local area connection and a wireless connection) and that we intend to tune the security configuration to take into account which interface is being used. We must first define the two interface types for the Security Profile.

To define multiple interface types:

1. Click **Interface Types** in the navigation pane of the new Security Profile's **Details** window.
2. Select the **Multiple Interface Types** option.
3. Type names for the interfaces and strings (with optional wildcards) which the Client Plug-in will use to match interface names on the laptop Computer: "LAN Connection" and "Local Area Connection *", and "Wireless" and "Wireless Network Connection *" in the first two Interface Type areas.
4. Click **Save** at the bottom right of the screen.

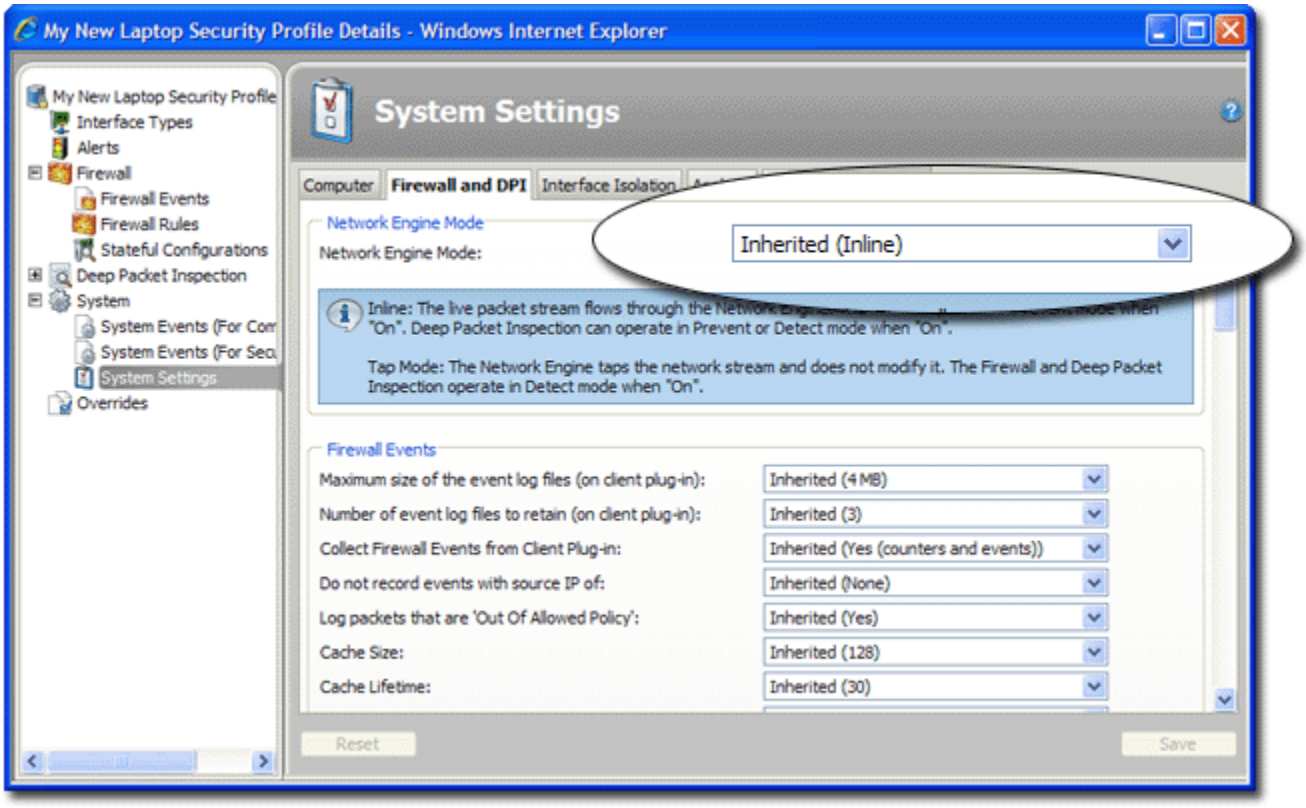


Setting the Firewall to Inline Mode

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.

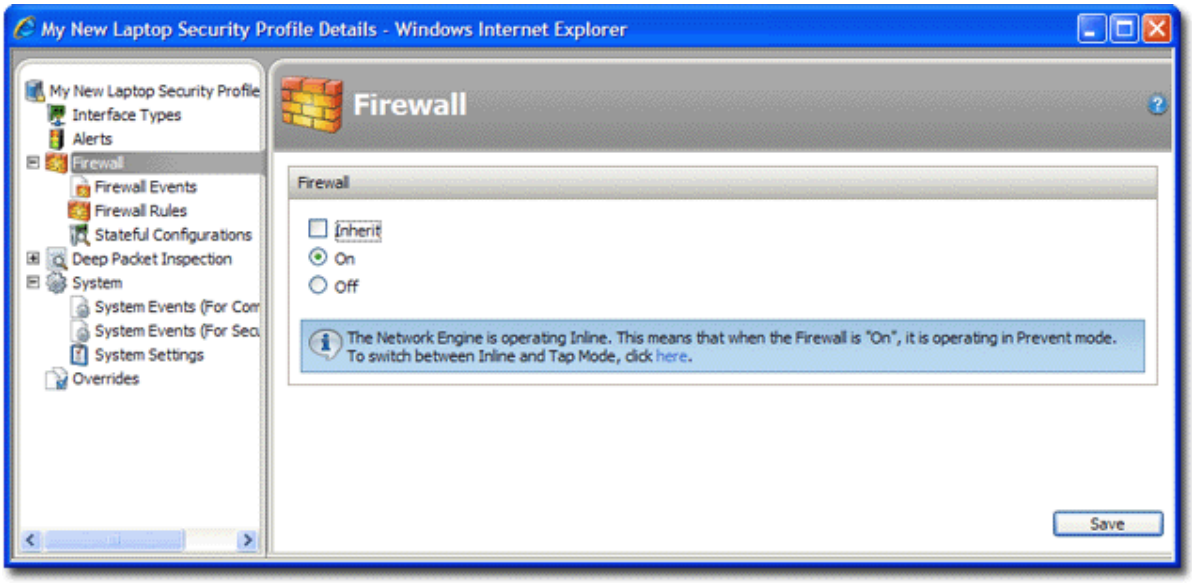
For now, we will configure our Security Profile to direct the engine to operate Inline. **To set the Firewall engine to Inline Mode:**

1. Still in the My New Laptop Security Profile **Details** screen, go to **System > System Settings** and click on the **Firewall and DPI** tab.
2. Set the Network Engine Mode to "Inline". (By default, the setting should already be set to "Inherited (Inline)" since the global default mode (configured in the main IDF Server Plug-in system settings) is "Inline" and a new Security Profile inherits global settings.)
3. Click **Save** at the bottom right of the screen.



Assigning Firewall Rules with Location Awareness

Click **Firewall** in the navigation pane, de-select the **Inherit** checkbox and select **On** beneath it.

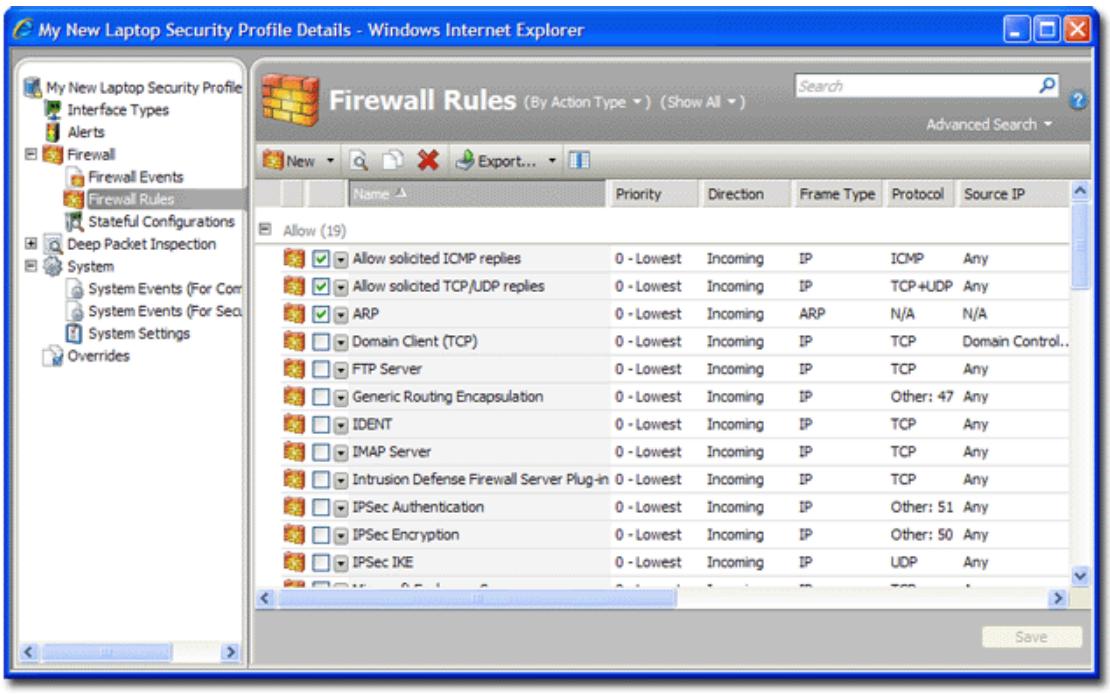


The **Inherit** checkbox determines whether or not these settings will be inherited from global settings defined in the Server Plug-in. For information on Inheritance, see "Inheritance and Overrides" in the Reference section.

Now we will assign some Firewall Rules and Stateful Configuration rules to this Security Profile.

To assign Firewall Rules and Stateful Configuration rules to this Security Profile:

1. Click "Firewall Rules" to display the list of available predefined Firewall Rules. (You can create your own Firewall Rules, but for this exercise we will select from the list of existing ones.) Select the following set of Firewall Rules to allow basic communication:
    - Allow Solicited ICMP replies
    - Allow solicited TCP/UDP replies
    - Domain Client (UDP)
    - ARP
    - Wireless Authentication
    - Windows File Sharing (This is a force-allow rule to permit incoming Windows File Sharing traffic.)

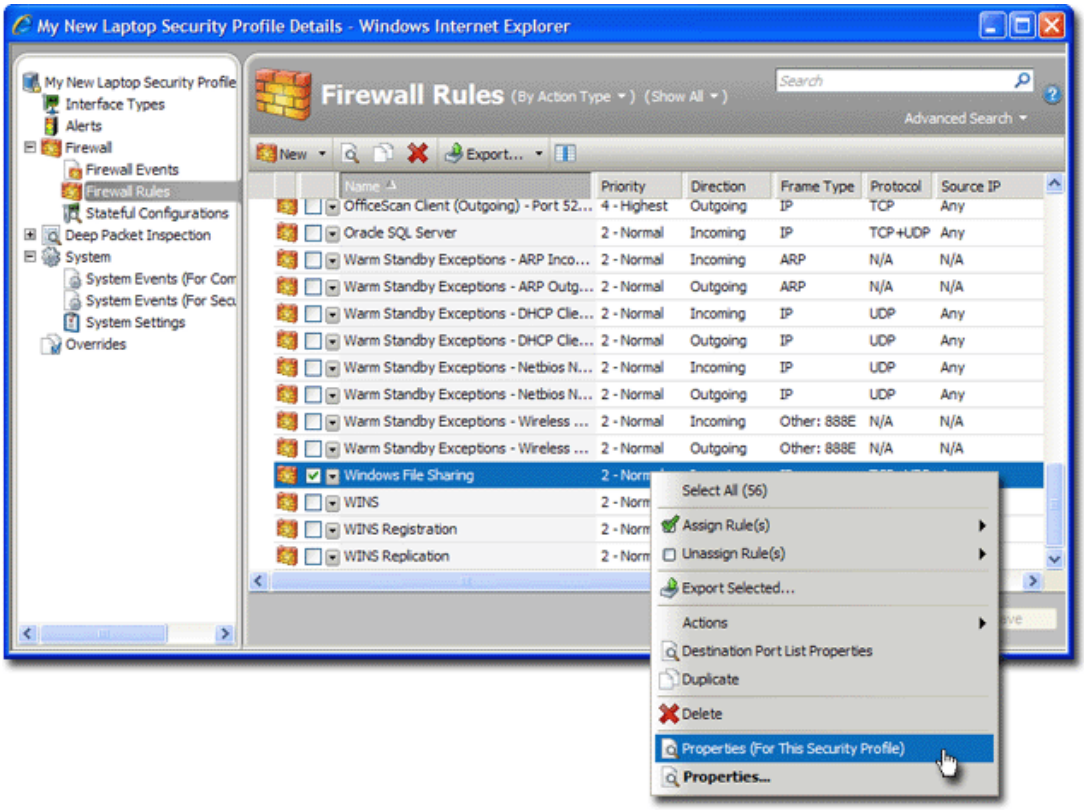


Notice the gray down-arrow next to the Firewall Rule checkboxes. These appear if you have defined multiple interfaces in the previous step. They allow you to specify whether the Firewall Rule will apply globally to all interfaces on the Computer or just to interfaces that you specify. Leave these at the default (global) setting for now.

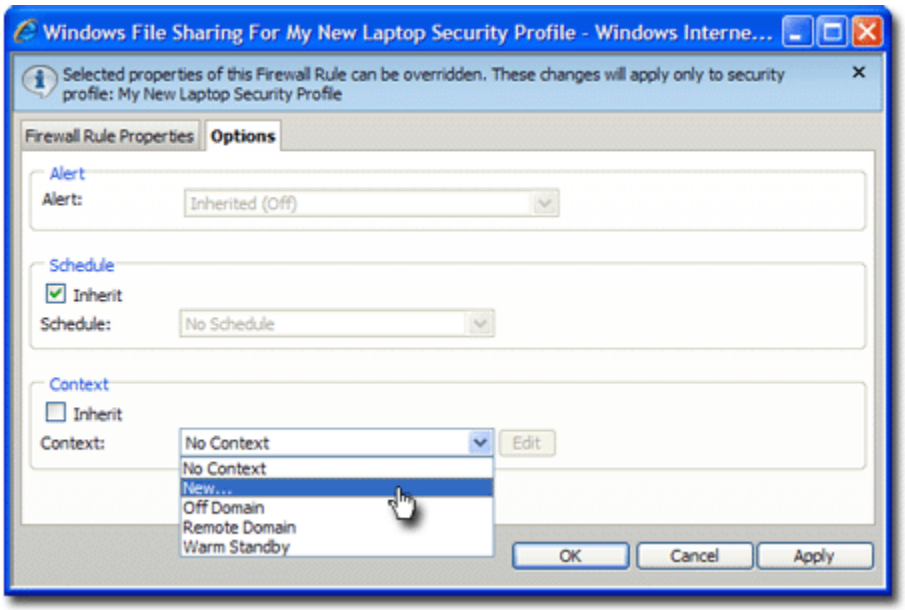
2. Click the **Save** button.

   We assigned a Firewall Rule that permitted Windows File Sharing. Windows File Sharing is a very useful feature in Windows but it has had some security issues. It would better to restrict this ability to when the laptop is in a secure office environment and forbid it when the laptop is out of the office. We will apply Location Awareness to the Firewall Rule when used with this Security Profile to implement this policy.

3. In the new Security Profile's **Details** screen, right-click the Windows File Sharing Firewall Rule and select **Properties (for this Security Profile)**. This will display the **Properties** window for the Firewall Rule but the changes we make to it will only apply to the Firewall Rule when it is applied as part this new Security Profile:

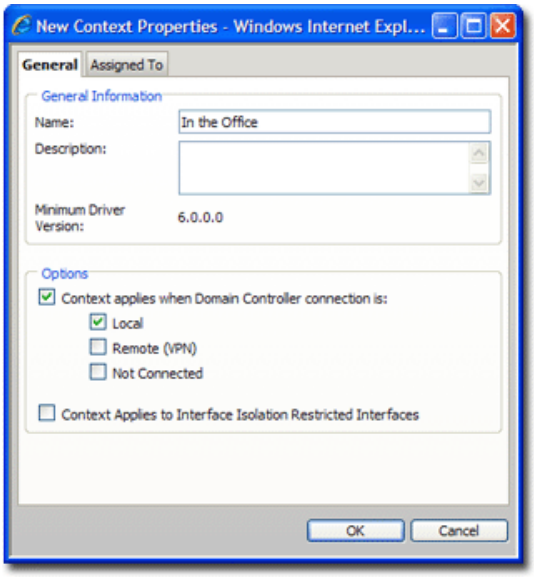


4. In the **Properties** window, click the **Options** tab. In the **Context** area, select "New..." from the drop-down list to display the **New Context** Properties window. We will create a Context that will only allow the Firewall Rule to be active when the laptop has local access to its Domain Controller. (That is, when the laptop is in the office.)

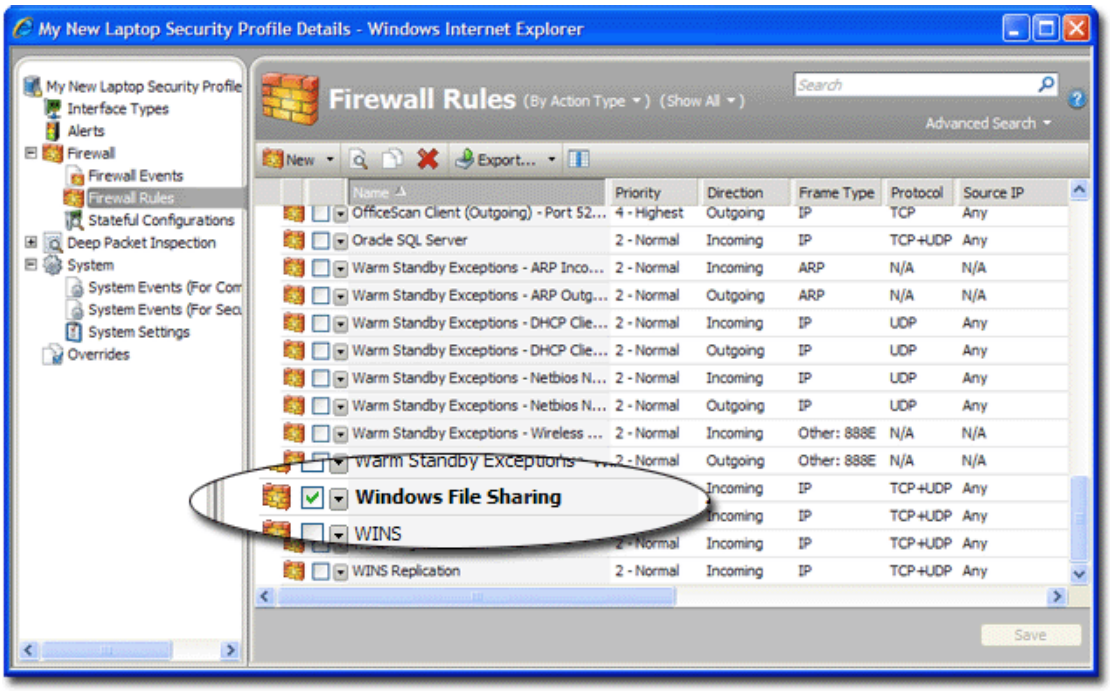


5. Name the new Rule Context "In the Office". In the **Options** area, set the "Context applies when Domain Controller connection is:" option and select "Local" below it. Then click **Ok**.

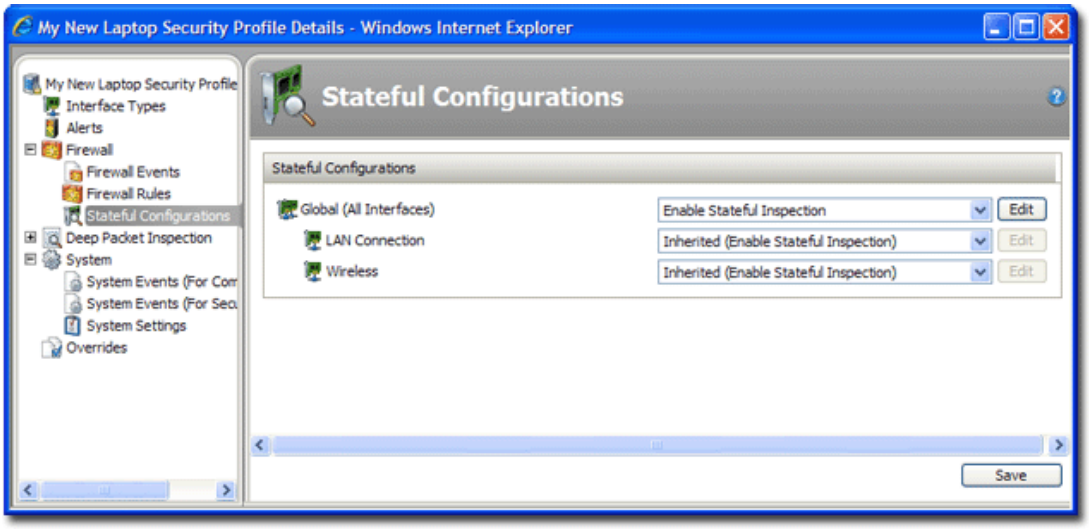
> If the Domain Controller can be contacted directly (via ICMP), the connection is "Local". If it can be contacted via VPN only, then the connection is "Remote".



6. Click **OK** to close the new Rule Context **Properties** window and click **OK** in the Windows File Sharing Firewall Rule **Properties** window.
7. Now the Windows File Sharing Firewall Rule will only be in effect when the laptop has direct access to its Windows Domain Controller. The Windows File Sharing Firewall Rule is now displayed in bold letters in the Security Profile **Details** screen. This indicates that the Firewall Rule has had its properties edited for this Security Profile only.



8. The final step in the Firewall section is to enable Stateful inspection. Click **Stateful Configurations** under Firewall in the navigation pane. Under **Global (All Interfaces)** select **Enable Stateful Inspection**.



9. Click **Save** to finish.

Note that Location Awareness is also available for DPI Rules.

Assign Deep Packet Inspection (DPI) Rules

To assign Deep Packet Inspection (DPI) rules to the Security Profile:

1. Still in the "My New Laptop Security Profile" **Details** window, click **Deep Packet Inspection** in the navigation pane. In the **Deep Packet Inspection** area, clear the **Inherit** check box, and select **On** beneath it. DPI can be set to either Prevent or Detect mode when the Network Engine is operating in Inline Mode (as opposed to Tap Mode). Detect Mode is useful if you are trying out a new set of DPI Rules and do not want to risk dropping traffic before you are sure the new rules are working properly. In Detect Mode, traffic that would normally be dropped will generate events but will be allowed to pass. Set Deep Packet Inspection to **On**.

Note the **Recommendations** area. The IDF Client Plug-in can be instructed to run a Recommendation Scan. (In the Server Plug-in's **Computers** list, right-click a Computer and select **Actions > Scan Computer(s) for Recommendations.**) The Recommendation engine will scan the Computer for applications and make DPI Rule recommendations based on what it finds. The results of the Recommendation Scan can be viewed in the Computer's **Details** window by clicking **Deep Packet Inspection > DPI Rules** and selecting "Show Recommended" from the **Show** drop-down list.

For now, leave the "Recommendations" option set to "Inherited (No)".

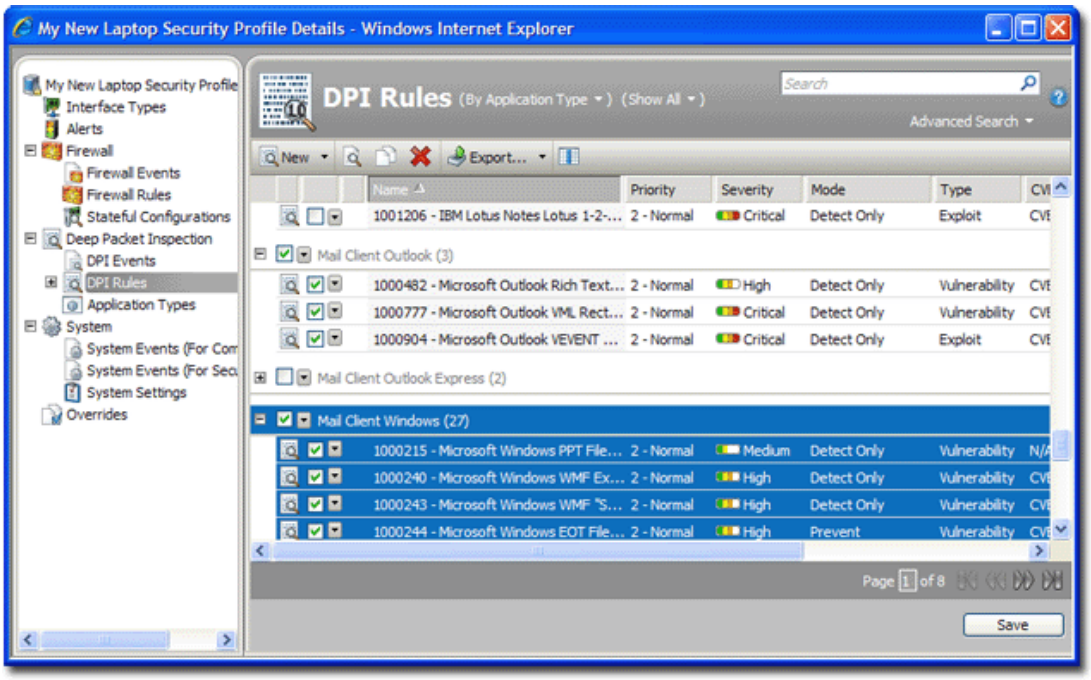
2. DPI Rules are organized by Application Type. Application Types are a useful way of grouping DPI Rules; they have only three properties: communication direction, protocol, and ports. For our new laptop Security Profile, we will assign the following Application Types:
   - Mail Client Outlook
   - Mail Client Windows
   - Microsoft Office
   - Web Client Common
   - Web Client Internet Explorer
   - Web Client Mozilla Firefox

- Windows Services RPC Client
- Windows Services RPC Server

Click DPI Rules under Deep Packet Inspection in the navigation pane. Sort the DPI Rules "By Application Type" and then put a check next to the Application Types listed above. (There are many Application Types and DPI Rules, so you will have to have to use the pagination controls at the bottom right of the screen to get to them all, or use the search features at the top right of the screen.)

Some DPI Rules are dependent on others. If you assign a rule that requires another rule to also be assigned (which has not yet been assigned) a popup window will appear letting you assign the required rule.

When assigning any kinds of Rules to a Computer, do not let yourself be tempted to be "extra secure" and assign all available rules to your Computer. The Rules are designed for a variety of operating systems, applications, vulnerabilities and may not be applicable to the Computer you want to protect. The traffic filtering engine would just be wasting CPU time looking for patterns that will never appear. Be selective when securing your Computers!



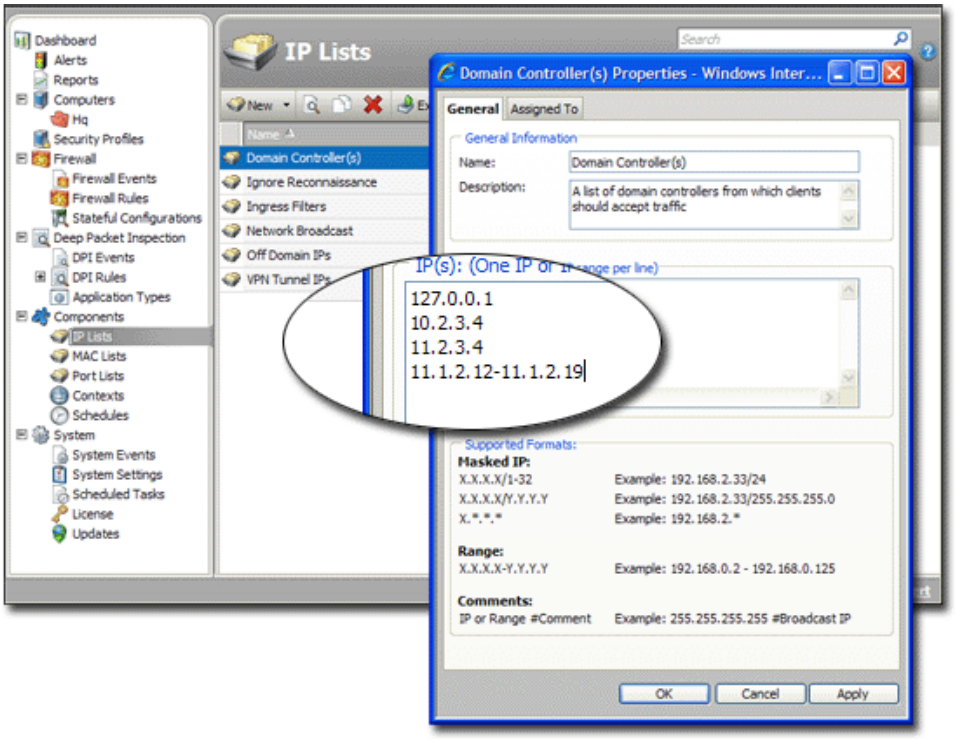
3. Click **Save** to assign the Application Types to the Security Profile.
4. Click **Save** to apply the rules to the Security Profile.

We are now finished editing the new Security Profile. You can now close the My New Security Profile **Details** screen.

Edit the Domain Controller(s) IP List

Finally, since the new Security Profile includes three Firewall Rules that use the "Domain Controller(s)" IP List, we will have to edit that IP List to include the IP addresses of the local Windows Domain Controller.

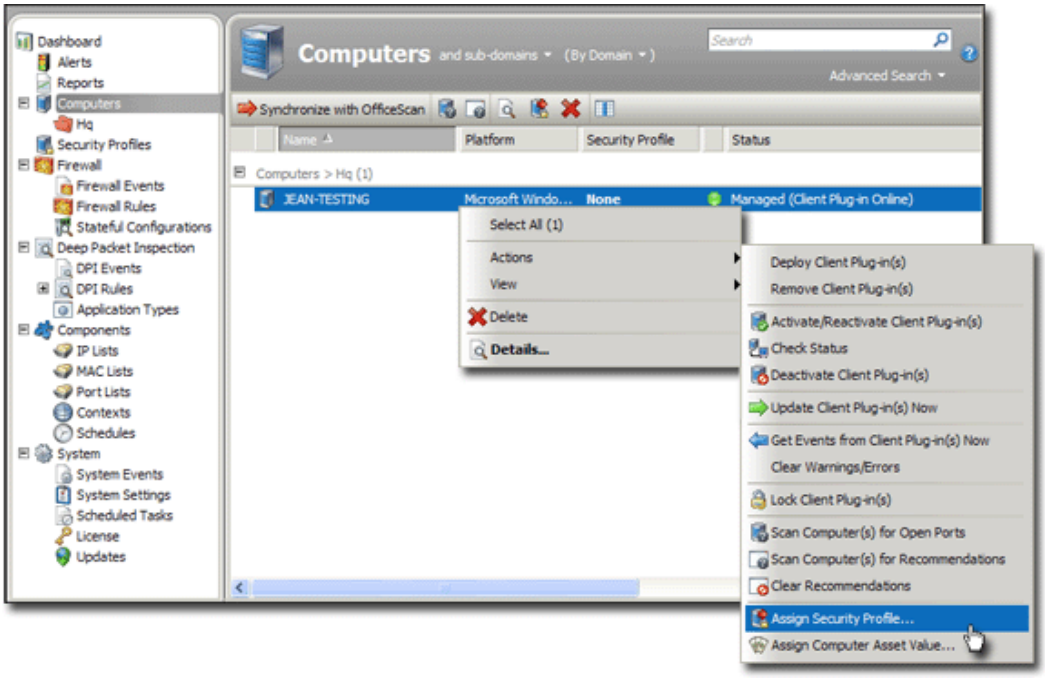
In the main window of the Server Plug-in, go to the **Components > IP Lists**, double-click the **Domain Controller(s)** IP List to see its **Properties** window, and type the IP(s) of your domain controller(s).



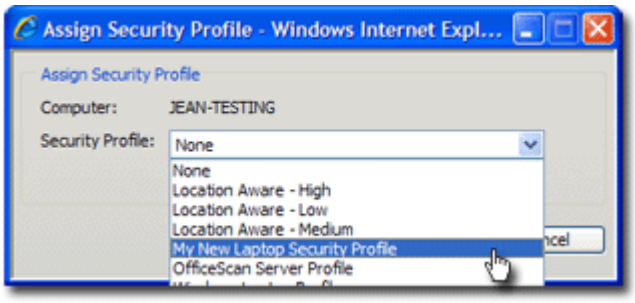
Click **OK** when you're done.

Apply the Security Profile to a Computer

Now we can apply the Security Profile to the Computer. Go to the **Computers** screen. Right-click the Computer to which you will assign the Security Profile and select "Assign Security Profile...".



Choose "My New Laptop Security Profile" from the drop-down list in the **Assign Security Profile** dialog box and click **OK**:



After clicking **OK**, the Server Plug-in will send the Security Profile to the Client Plug-in. The **Computer Status** column and the Server Plug-in's status bar will display messages that the Client Plug-in is being updated.

Once the Client Plug-in on the Computer has been updated, the status column will read "Managed (Client Plug-in Online)".

Configure SMTP Settings

Configuring the IDF Server Plug-in's SMTP settings allows email alerts to be sent out to users.

To configure SMTP settings:

1. Go to **System > System Settings** and click the **System** tab.
2. Type the appropriate information and click the **Test SMTP Settings** to confirm IDF Server Plug-in can communicate with the mail server.
3. Now click the **Notifications** tab. On the **Notifications** screen, type the default email address to which you want notifications sent.

Whether a particular Alert generates emailed notifications can be configured on that Alert's **Properties** window (**System > System Settings > System > View Alert Configuration...**).

Click the **Save** button at the bottom of the screen to save your settings.

Monitor Activity Using the IDF Server Plug-in

The Dashboard

After the Computer has been assigned a Security Profile and has been running for a while, you will want to review the activity on that Computer. The first place to go to review activity is the Dashboard. The Dashboard has many information panels ("widgets") that display different types of information pertaining to the state of the IDF Server Plug-in and the Computers that it is managing.

On the Dashboard toolbar, Click **Add/Remove Widgets.** to view the list of available widgets.

In this Guide, we will add the following widgets from the **Firewall** section:

- Firewall Activity (Prevented)

- Firewall IP Activity (Prevented)
- Firewall History (2x1)

Select the checkbox beside each of the three widgets, and click **OK**. The widgets will appear on the dashboard. (It may take a bit of time to generate the data.)

- The **Firewall Activity (Prevented)** widget displays a list of the most common reasons for packets to be denied (that is, blocked from reaching a Computer by the Client Plug-in on that Computer) along with the number of packets that were denied. Items in this list will be either types of Packet Rejections or Firewall Rules. Each "reason" is a link to the corresponding logs for that denied packet.
- The **Firewall IP Activity (Prevented)** widget displays a list of the most common source IPs of denied packets. Similar to the **Firewall Activity (Prevented)** widget, each source IP is a link to the corresponding logs.
- The **Firewall History (2x1)** widget displays a bar graph indicating how many packets were blocked (prevented) or only logged (detected) in the last 24 hour period or seven day period (depending on the view selected). Clicking a bar will display the corresponding logs for the period represented by the bar.

Note the trend indicators next to the numeric values in the **Firewall Activity (Prevented)** and **Firewall IP Activity (Prevented)** widgets. An upward or downward pointing triangle indicates an overall increase or decrease over the specified time period, and a flat line indicates no significant change.

Logs of Firewall and DPI Events

Now drill-down to the logs corresponding to the top reason for Denied Packets: in the **Firewall Activity (Prevented)** widget, click the first reason for denied packets (in the picture above, the top reason is "Out of Allowed Policy"). This will take you to the **Firewall Events** screen.

The **Firewall Events** screen will display all Firewall Events where the **Reason** column entry corresponds to the first reason from the Firewall **Activity (Prevented)** widget ("Out of Allowed Policy"). The logs are filtered to display only those events that occurred during the view period of the Dashboard (Last 24 hours or last seven days). Further information about the **Firewall Events** and **DPI Events** page can be found in the help pages for those screens.

For the meaning of the different packet rejection reasons, see Firewall Events and DPI Events.

Reports

Often, a higher-level view of the log data is desired, where the information is summarized, and presented in a more easily understood format. The **Reports** fill this role, allowing you to display detailed summaries on Computers, Firewall and DPI Event Logs, Events, Alerts, etc. On the **Reports** screen, you can select various options for the report to be generated. These options are further discussed in the Reports help section.

We will generate a **Firewall Report**, which displays a record of Firewall Rule and Stateful Configuration activity over a configurable date range. Select **Firewall Report** from the Report drop-down. Click **Generate** to launch the report in a new window.

By reviewing reports, by logging into the system and consulting the dashboard, by performing detailed investigations by drilling-down to specific logs, and by configuring alerts to notify you of critical events, you can remain apprised of the health and status of your network.

About Firewall Rules

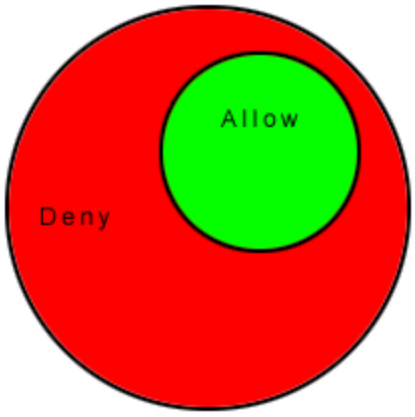
IDF Firewall Rules have both a rule action and a rule priority. Used in conjunction, these two properties allow you to create very flexible and powerful rule-sets. Unlike rule-sets used by other firewalls, which may require that the rules be defined in the order in which they should be run, IDF Firewall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

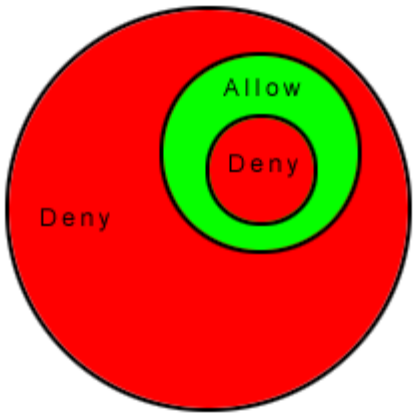
Each rule can have one of four actions.

1. **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).
2. **Force Allow:** if a packet matches a **force allow** rule it is passed regardless of any other rules (at the same priority level).
3. **Deny:** if a packet matches a **deny** rule it is dropped.
4. **Allow:** if a packet matches an **allow** rule, it is passed. Any traffic not matching one of the **allow** rules is denied.
5. **Log Only:** if a packet matches a **log only** rule it is passed and the event is logged.

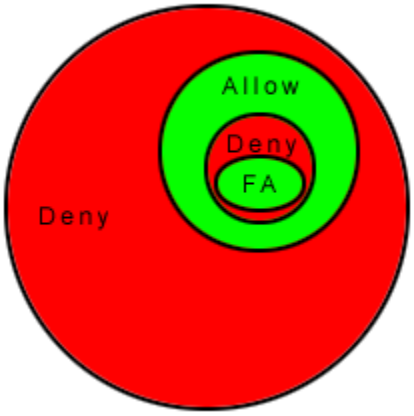
Adding an ALLOW rule will deny everything else:



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



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



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 a User 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.

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
- Force Allow
- Deny
- Allow
- Log Only

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.

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.

Example

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 in 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 in 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.

 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.

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 which types of Events are ignored in four of the more complex Advanced Logging Policy modes:

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
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
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 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

Client Plug-in Events

Client Plug-in Events are displayed within a System Event on the **System Events** screen. For example, double-clicking the "Client Plug-in Events Retrieved" System Event will display a window listing all the Client Plug-in Events that were retrieved.

Number	Event
1000	Unable To Open Engine
1001	Engine Command Failed
1002	Engine List Objects Error
1003	Remove Object Failed
2000	Security Configuration Updated
2003	Save Security Configuration Failed
2004	Invalid Interface Assignment
2006	Invalid Action
2007	Invalid Packet Direction
2008	Invalid Rule Priority
2017	Invalid Schedule Length
2018	Invalid Schedule String
2019	Unrecognized IP Format
2020	Object Not Found
2021	Object Not Found
2022	Invalid Rule Assignment
2085	DPI Rule Error
2086	Unsupported IP Match Type
2087	Unsupported MAC Match Type
2088	Invalid SSL Credential
2089	Missing SSL Credential
3000	Invalid MAC Address
3001	Get Event Data Failed
3002	Too Many Interfaces
3003	Unable To Run External Command
3004	Unable To Read External Command Output
3005	Operating System Call Error
3006	Operating System Call Error
3007	File Error
3008	Machine-Specific Key Error
3300	Get Event Data Failed
3302	Get Security Configuration Failed
3303	File Mapping Error
3601	Read Local Data Error

3602	Windows Service Error
3603	File Mapping Error
4000	Invalid Protocol Header
4001	Invalid Protocol Header
4002	Command Session Initiated
4003	Configuration Session Initiated
4004	Command Received
4011	Heartbeat Failed
5000	Client Plug-in Started
5001	Thread Exception
5002	Operation Timed Out
5003	Client Plug-in Stopped
5004	Clock Changed
5005	Client Plug-in Auditing Started
5006	Client Plug-in Auditing Stopped
6000	Log Device Open Error
6001	Log File Open Error
6002	Log File Write Error
6003	Log Directory Creation Error
6004	Log File Query Error
6005	Log Directory Open Error
6006	Log File Delete Error
6007	Log File Rename Error
6008	Log Read Error
6009	Log File Deleted Due To Insufficient Space
7000	Computer OS Fingerprint Probe
7001	Network or Port Scan
7002	TCP Null Scan
7003	TCP FIN Scan
7004	TCP Xmas Scan

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:

1. Packets matching Bypass will not be processed by DPI Rules
2. Unlike Force Allow, Bypass will not automatically allow the responses on a TCP connection when Stateful Configuration is on (See below for more information)
3. 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)

Important: 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:

1. **Priority**: Highest
2. **Frame Type**: IP
3. **Protocol**: TCP, UDP, or other IP protocol. (Do not use the "Any" option.)
4. **Source and Destination IP and MAC**: all "Any"
5. 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".
6. 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".
7. **Schedule**: None.

Logging

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

Creating and Applying New Firewall Rules

Firewall Rules are composed of four basic elements:

- **Rule 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:
    1. "bypass"
    2. "force allow"
    3. "deny"
    4. "allow"
    5. "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.
- **Control Information:** all the information that describes the packet (frame type, protocol, source and destination IPs, source and destination ports, flags, etc.)

To create a new Firewall Rule:

1. Go to the **Firewall Rules** screen and click **New** on the toolbar.
2. Type a name and description for your new Firewall Rule.
3. Select a rule action, priority, and packet direction from the drop-down lists.
4. Define the criteria that this rule will look for in the packets' control information. (Note that as well as inclusive criteria, you can define exclusive criteria by checking the "Not" checkbox at the right of each option.)
5. Click the **Options** tab and select whether you want the rule to only be active during certain scheduled periods. Specify whether you want this rule to trigger an alert when it is triggered.
6. Click **OK** to close the **New Firewall Rule** Window.

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:

1. Go to the **Security Profiles** screen and double-click the Security Profile to which you want to assign a new rule. This will open the Profile's **Details** window.
2. Click the **Firewall Rules** tab.
3. Find your new Firewall Rule in the list and put a check in its checkbox.
4. Click **OK**.

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

Optionally, you can assign a new Firewall Rule directly to a Computer:

1. Go to the **Computers** screen and double click the Computer to which you want to assign the new rule.
2. Click the **Firewall Rules** tab.
3. Find your new Firewall Rule in the list.
4. Put a check in its checkbox and click the **OK** button.

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

Note that 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.

Creating Custom DPI Rules

Trend Micro's DPI Rules are written in a proprietary language. Please contact your support provider for information on training opportunities.

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.
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.
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.
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.

Encrypting IDF Server to DB Communication

Communication between the IDF Server Plug-in and the database is not encrypted by default. This is for performance reasons and because the channel between the Server Plug-in and the database may already be secure (either they are running on the same Computer or they are connected by crossover cable, a private network segment, or tunneling via IPSec).

However, if the communication channel between the IDF Server Plug-in and the database is not secure, you should encrypt the communications between them. Do this by editing the `dsm.properties` file located in `\IDF Server Plug-in\webclient\webapps\ROOT\WEB-INF\`

MS SQL Server

Add the following line to `dsm.properties`:

```
database.SqlServer.ssl=require
```

Save and close the file. Stop and restart the Server Plug-in service.

Oracle Database

Add the following lines to `dsm.properties`:

```
database.Oracle.oracle.net.encryption_types_client=(3DES168)
database.Oracle.oracle.net.encryption_client=REQUIRED
database.Oracle.oracle.net.crypto_checksum_types_client=(MD5)
database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
```

Save and close the file. Stop and restart the IDF Server Plug-in service.

Note that Oracle Database must be configured to accept encrypted communication. Consult your Oracle Database documentation for instructions.

Running a Client Plug-in on the Database Server

Encryption should be enabled if you are using a Client Plug-in to protect the database. When you carry out a Security Update, the IDF Server Plug-in stores new DPI Rules in the database. The rule names themselves will almost certainly generate false positives as they get parsed by the Client Plug-in if the data is not encrypted.

Firewall Events

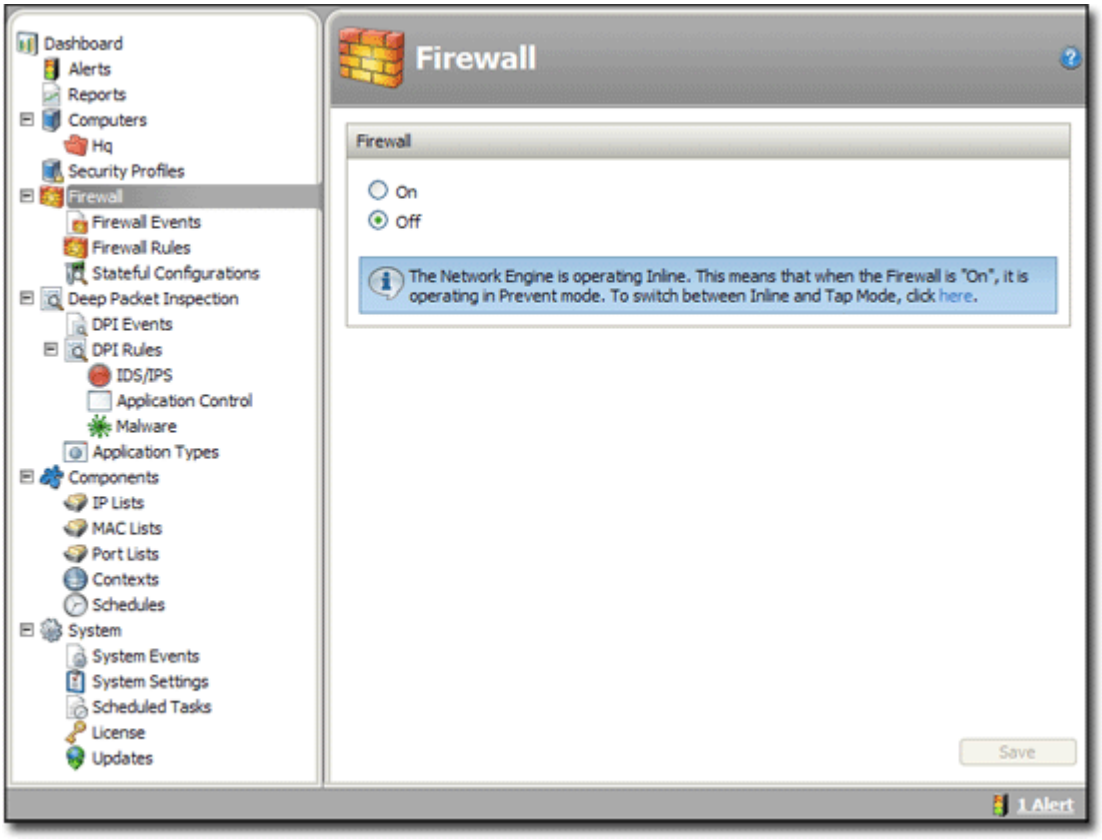
Event	Notes
CE Flags	The CWR or ECE flags were set and the stateful configuration specifies that these packets should be denied.
Dropped Retransmit	Dropped Retransmit.
First Fragment Too Small	A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).
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.
Invalid Flags	A packet with nonsensical flag combinations was encountered.
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.
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.

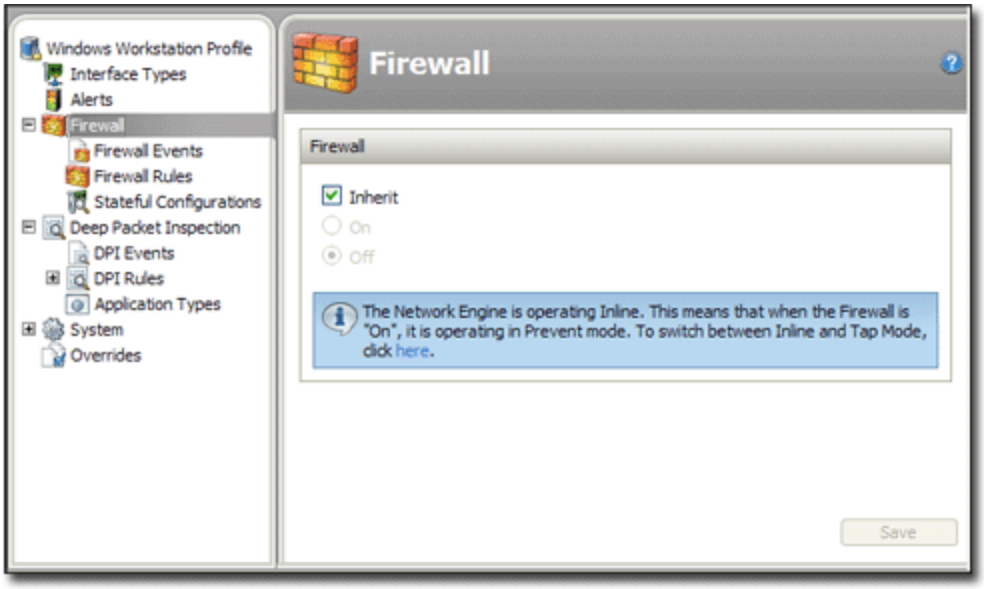
Inheritance and Overrides

Settings

Global settings can be overridden by settings at the Security Profile or Computer level. For example, the IDF 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.



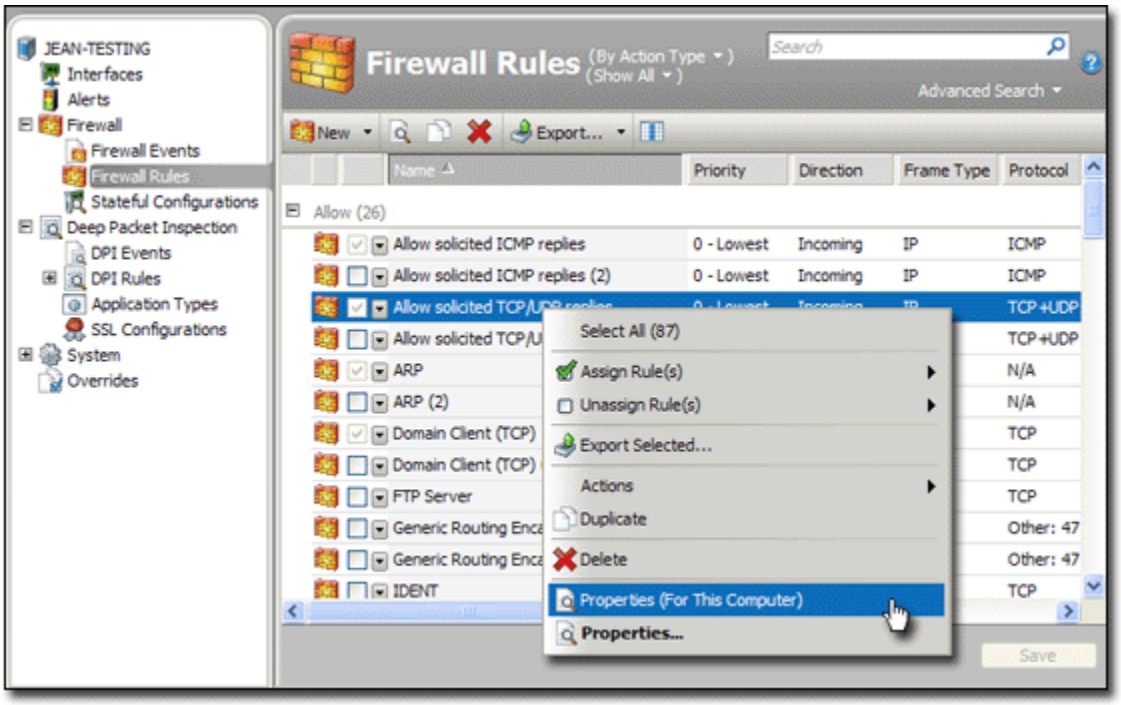
By default, lower levels in the hierarchy inherit their settings from the level above them. Therefore, if you turn off the Firewall at the Global level, it will be turned off in all Security Profiles and Computers that are set to "Inherit".



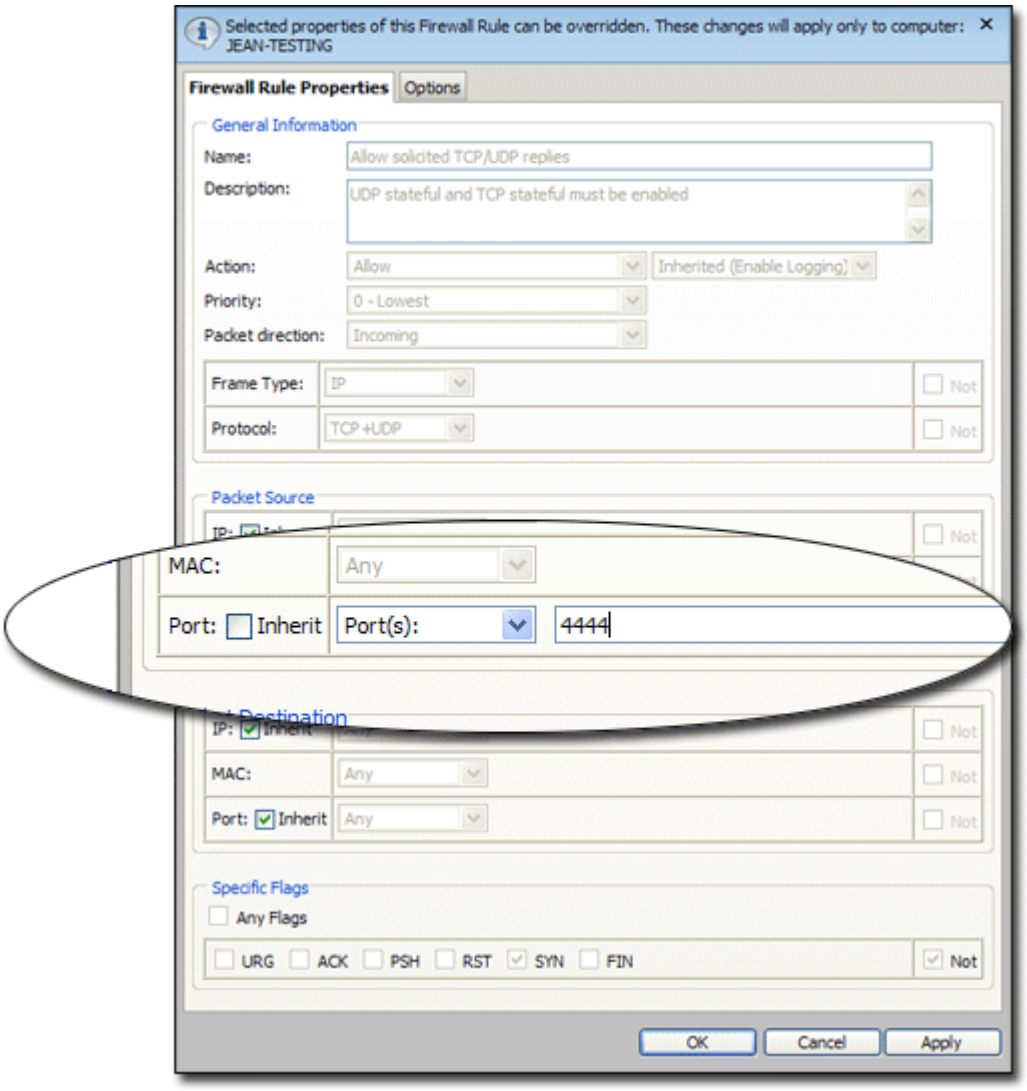
Other Properties

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)".



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.



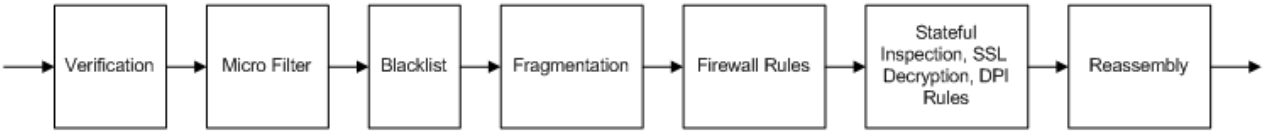
This operation can also be performed at the Security Profile level if the Firewall Rule is part of a Security Profile. You would open the Security Profile's **Details** window and make the same changes. (You could then override those again on a particular Computer.)

Seeing the Overrides on a Computer or Security Profile at a glance

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.

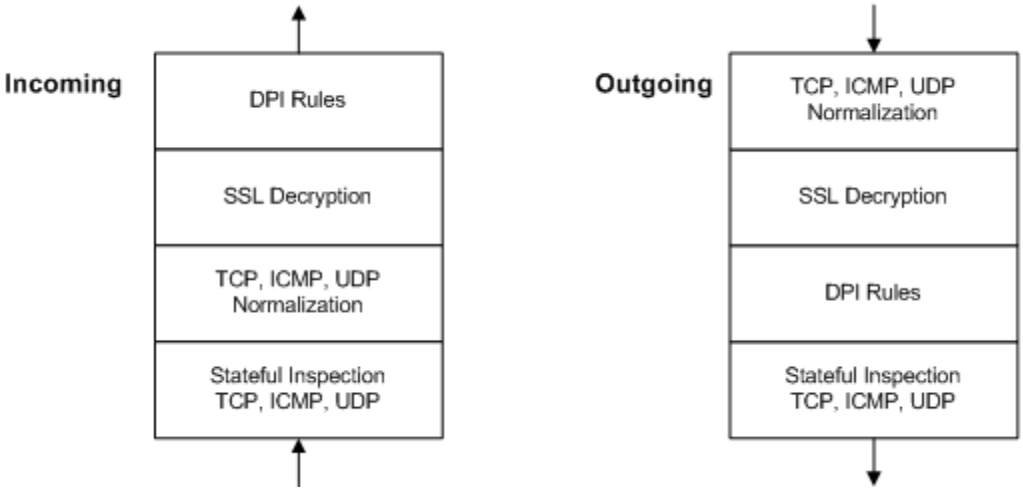
Packet Processing Sequence

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



- **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:



Required Ports

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
- Connected To: DSA
- 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 remotely
- Protocol: TCP
- Initiated By: Web Browser
- Connected To: IDF Server
- Proxy: No
- Configuration: This port is configured during the IDF Server installation process

Port: 4120 (default)

- Use: Client Plug-in to Server Plug-in communication
- Protocol: TCP
- Initiated By: DSA
- Connected To: IDF Server
- Proxy: No
- Configuration: This port is configured during the IDF Server installation process

Port: 514 (default)

- Use: Syslog
- Protocol: UDP
- Initiated By: DSA
- Connected To: Syslog facility
- Proxy: No
- Configuration: This port can be configured in the IDF Server Settings section

Port: 25 (default)

- Use: E-mail Alerts
- Protocol: TCP
- Initiated By: IDF Server
- Connected To: Specified SMTP server
- Proxy: No
- Configuration: This port can be configured in the IDF Server Settings section

Port: Randomly selected

- Use: DNS lookup for hostnames
- Protocol: TCP
- Initiated by: IDF Server
- Connected to: DNS server
- Proxy: No
- Configuration: The port is randomly selected when the IDF Server Computer needs to lookup a hostname.

Firewall Rule Sequence

Packets arriving at a Computer running a IDF 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)
    1. **Bypass**
    2. **Log Only** (Note that **Log Only** rules can only be assigned a priority of **4 (highest)**)
    3. **Force Allow**
    4. **Deny**
2. Firewall Rules with priority 3 (high)
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
3. Firewall Rules with priority 2 (normal)
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
4. Firewall Rules with priority 1 (low)
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
5. Firewall Rules with priority 0 (lowest)
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
    4. **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.

System Events

Number	Event
0	Unknown Error
100	IDF Server Plug-in Started
101	License Changed
102	Trend Micro IDF Customer Account Changed
103	Check For Updates Failed
104	Automatic Client Plug-ins Download Failed
105	Scheduled Security Update Download and Apply Failed
106	Scheduled Security Update Downloaded and Applied
107	Security Update Downloaded and Applied
108	Script Executed
109	Script Execution Failed
110	System Events Exported
111	Firewall Events Exported
112	DPI Events Exported
113	Scheduled Security Update Download Failed
114	Scheduled Security Update Downloaded
115	Security Update Downloaded
116	Security Update Applied
117	IDF Server Plug-in Shutdown
118	IDF Server Plug-in Offline
119	IDF Server Plug-in Back Online
120	Heartbeat Server Failed
121	Scheduler Failed
122	Server Plug-in Message Thread Failed
123	IDF Server Plug-in Forced Shutdown
130	Credentials Generated
131	Credential Generation Failed
150	System Settings Saved
151	Client Plug-in Software Added
152	Client Plug-in Software Deleted
153	Client Plug-in Software Updated
154	Client Plug-in Software Exported
155	Client Plug-in Platforms Changed
160	Authentication Failed
161	Security Update Exported
180	Alert Type Updated
190	Alert Started

191	Alert Changed
192	Alert Ended
197	Alert Emails Sent
198	Alert Emails Failed
199	Alert Processing Failed
250	Computer Created
251	Computer Deleted
252	Computer Updated
253	Security Profile Assigned to Computer
254	Computer Moved
255	Client Plug-in Activate Requested
256	Client Plug-in Update Now Requested
257	Client Plug-in Locked
258	Client Plug-in Unlocked
259	Client Plug-in Deactivate Requested
260	Scan for Open Ports
261	Scan for Open Ports Failed
262	Scan for Open Ports Requested
263	Scan for Open Ports Canceled
264	Client Plug-in Software Upgrade Requested
265	Client Plug-in Software Upgrade Cancelled
266	Computer Warnings/Errors Cleared
267	Check Status Requested
268	Get Events Now Requested
270	Computer Creation Failed
275	Duplicate Computer
280	Computers Exported
281	Computers Imported
286	Computer Log Exported
290	Domain Added
291	Domain Removed
292	Domain Updated
293	Computer Interface Renamed
294	Computer Bridge Renamed
295	Computer Interface Deleted
296	Computer Interface IP Deleted
297	Scan for Recommendations Requested
298	Recommendations Cleared
299	Asset Value Assigned to Computer
300	Scan for Recommendations
301	Client Plug-in Software Deployment Requested

302	Client Plug-in Software Removal Requested
303	Computer Renamed
310	Directory Added
311	Directory Removed
312	Directory Updated
320	Directory Synchronization
321	Directory Synchronization Finished
322	Directory Synchronization Failed
323	Directory Synchronization Requested
324	Directory Synchronization Cancelled
325	User Synchronization
326	User Synchronization Finished
327	User Synchronization Failed
328	User Synchronization Requested
329	User Synchronization Cancelled
330	SSL Computer Configuration Created
331	SSL Computer Configuration Deleted
332	SSL Computer Configuration Updated
350	Security Profile Created
351	Security Profile Deleted
352	Security Profile Updated
353	Security Profiles Exported
354	Security Profiles Imported
410	Firewall Rule Created
411	Firewall Rule Deleted
412	Firewall Rule Updated
413	Firewall Rule Exported
414	Firewall Rule Imported
420	Stateful Configuration Created
421	Stateful Configuration Deleted
422	Stateful Configuration Updated
423	Stateful Configuration Exported
424	Stateful Configuration Imported
460	Application Type Created
461	Application Type Deleted
462	Application Type Updated
463	Application Type Exported
464	Application Type Imported
470	DPI Rule Created
471	DPI Rule Deleted
472	DPI Rule Updated

473	DPI Rule Exported
474	DPI Rule Imported
510	IP List Created
511	IP List Deleted
512	IP List Updated
513	IP List Exported
514	IP List Imported
520	Port List Created
521	Port List Deleted
522	Port List Updated
523	Port List Exported
524	Port List Imported
530	MAC List Created
531	MAC List Deleted
532	MAC List Updated
533	MAC List Exported
534	MAC List Imported
550	Schedule Created
551	Schedule Deleted
552	Schedule Updated
553	Schedule Exported
554	Schedule Imported
560	Scheduled Task Created
561	Scheduled Task Deleted
562	Scheduled Task Updated
563	Scheduled Task Manually Executed
564	Scheduled Task Started
565	Backup Finished
566	Backup Failed
567	Sending Outstanding Alert Summary
568	Failed To Send Outstanding Alert Summary
569	Email Failed
570	Sending Report
571	Failed To Send Report
572	Invalid Report Jar
573	Computer Asset Value Created
574	Computer Asset Value Deleted
575	Computer Asset Value Updated
600	User Signed In
601	User Signed Out
602	User Timed Out

603	User Locked Out
604	User Unlocked
608	User Session Validation Failed
609	User Made Invalid Request
610	User Session Validated
611	User Viewed Firewall Event
613	User Viewed DPI Event
615	User Viewed System Event
650	User Created
651	User Deleted
652	User Updated
653	User Password Set
660	User Role Created
661	User Role Deleted
662	User Role Updated
663	User Roles Imported
664	User Roles Exported
670	Contact Created
671	Contact Deleted
672	Contact Updated
700	Client Plug-in Installed
701	Client Plug-in Install Failed
702	Client Plug-in Credentials Generated
703	Client Plug-in Credential Generation Failed
704	Client Plug-in Activated
705	Client Plug-in Activate Failed
706	Client Plug-in Software Upgraded
707	Client Plug-in Software Upgrade Failed
708	Client Plug-in Deactivated
709	Client Plug-in Deactivate Failed
710	Client Plug-in Events Retrieved
711	Client Plug-in Software Deployed
712	Client Plug-in Software Deployment Failed
713	Client Plug-in Software Removed
714	Client Plug-in Software Removal Failed
720	Client Plug-in Updated
721	Client Plug-in Update Failed
722	Get Interfaces Failed
723	Get Interfaces Failure Resolved
724	Insufficient Disk Space
725	Logs Suppressed

726	Get Client Plug-in Events Failed
727	Get Client Plug-in Events Failure Resolved
728	Get Firewall/DPI Events Failed
729	Get Firewall/DPI Events Failure Resolved
730	Client Plug-in Offline
731	Client Plug-in Back Online
732	Firewall Rule Engine Offline
733	Firewall Rule Engine Back Online
734	Computer Clock Change
735	Client Plug-in Misconfiguration Detected
736	Check Status Failure Resolved
737	Check Status Failed
738	DPI Engine Offline
739	DPI Engine Back Online
740	Client Plug-in Error
741	Abnormal Restart Detected
750	Last Automatic Retry
760	Driver Version Compatibility Resolved
761	Client Plug-in Upgrade Recommended
762	Client Plug-in Upgrade Required
763	Incompatible Driver Version
764	Client Plug-in Upgrade Recommended (Incompatible DPI Rules(s))
765	Computer Reboot Required
766	Firewall Detect Mode Configuration Incompatibility
767	Firewall Detect Mode Version Incompatibility
768	Firewall Detect Mode Incompatibility Resolved
770	Client Plug-in Heartbeat Rejected
771	Contact by Unrecognized Client
780	Scan for Recommendations Failure Resolved
781	Scan for Recommendations Failure
790	Client Plug-in Initiated Activation Requested
791	Client Plug-in Initiated Activation Failure
800	Alert Dismissed
801	Computer Error Dismissed
850	Reconnaissance Detected: Computer OS Fingerprint Probe
851	Reconnaissance Detected: Network or Port Scan
852	Reconnaissance Detected: TCP Null Scan
853	Reconnaissance Detected: TCP SYNFIN Scan
854	Reconnaissance Detected: TCP Xmas Scan
900	IDF Server Plug-in Audit Started
901	IDF Server Plug-in Audit Shutdown

902	IDF Server Plug-in Installed
910	Diagnostic Package Generated
911	Diagnostic Package Exported
912	Diagnostic Package Uploaded
970	Command Line Utility Started
978	Command Line Utility Failed
979	Command Line Utility Shutdown
980	System Information Exported
990	Server Plug-in Node Added
991	Server Plug-in Node Decommissioned
992	Server Plug-in Node Updated
998	System Event Notification Error
999	Internal Software Error

Privacy Policy

Trend Micro, Inc. is committed to protecting your privacy. Please read the Trend Micro Privacy Policy available at www.trendmicro.com.