TREND MICRO™

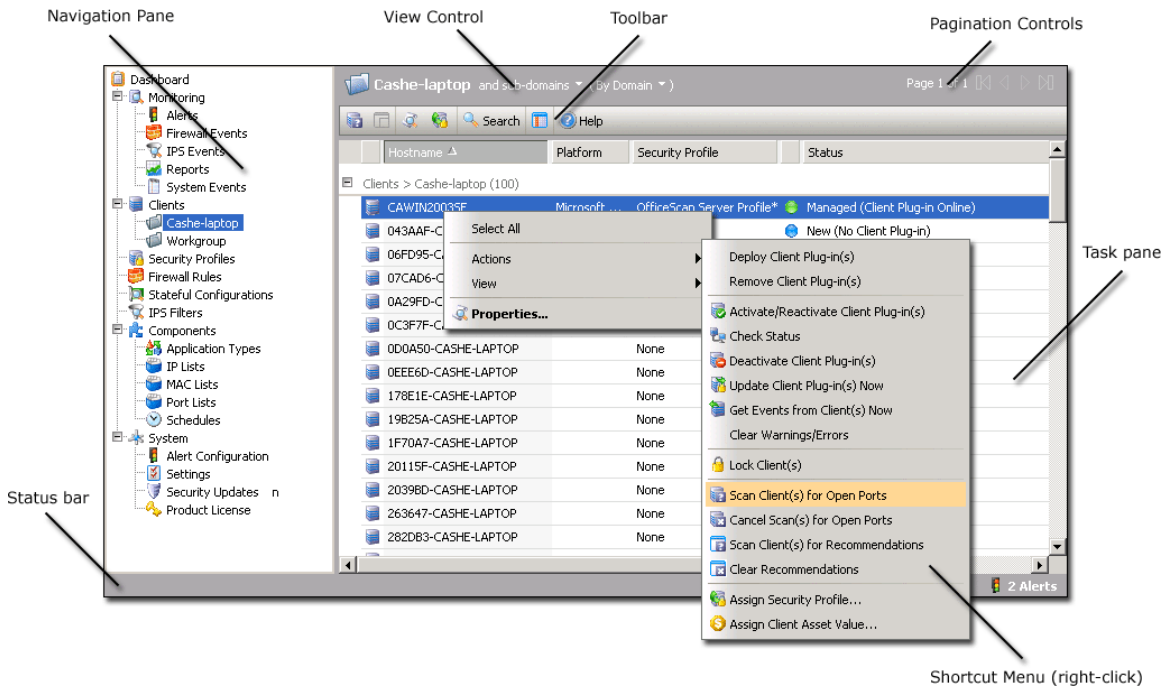
Intrusion Defense Firewall 1.0 for OfficeScan Client/Server Edition Administrator's Guide

Endpoint Security

Document part number: OSEM83465/71122
Release date: Nov 2007

Table Of Contents

Overview of the Server Plug-in Interface



Navigation Pane

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

- **Dashboard:** an at-a-glance overview of the status of the Server Plug-in.
- **Monitoring:**
  - **Alerts:** a summary of current critical and warning alerts concerning system or security events.
  - **Firewall Events:** logs of security-related Firewall activity
  - **IPS Events:** logs of security-related IPS activity
  - **Reports:** a report generator to produce summaries of system status and summaries of activities.
  - **System Events:** a summary of system-related events.
- **Computers:** a list of Computers synchronized from OfficeScan with status information for each.
- **Security Profiles:** a list of defined security profiles
- **Firewall Rules:** where you define and manage Firewall Rules
- **Stateful Configurations:** where you define and manage Stateful Configurations
- **IPS Filters:** where you define and manage IPS Filters
- **Components:** a list of common components used by various elements of the Intrusion Defense Firewall
- **System:** where you can find administrative tools to manage the operation of the Server Plug-in

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 on the "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.

View Control

Where appropriate, the view control gives you options for displaying listed items.

Toolbar

The toolbar holds buttons that 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 shortcut menu.

Status Bar

The status bar displays information relating to the current state of your Server Plug-in. 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 port-scanning operations, Client Plug-in activations, or Client Plug-in updates.

Shortcut Menus

Many of the Server Plug-in's screens have context-sensitive menus. Right-clicking on a Security Profile, for example, gives you a shortcut menu with access to most of the options in the toolbar for that screen. Right-clicking on a group of Computers brings up a shortcut menu with options to manage the current domain or create a new one.

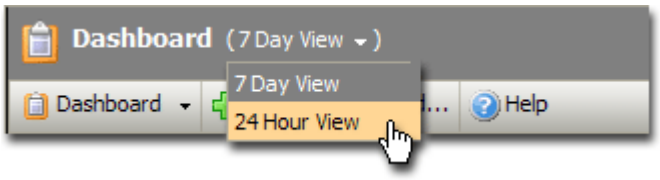
Screen-by-Screen Guide to the Intrusion Defense Firewall Server Plug-in Interface

Dashboard

The Dashboard provides a quick at-a-glance view of the state of the Intrusion Defense Firewall. When you start the Server Plug-in, the Server Plug-in preserves the layout of the Dashboard from your last session.

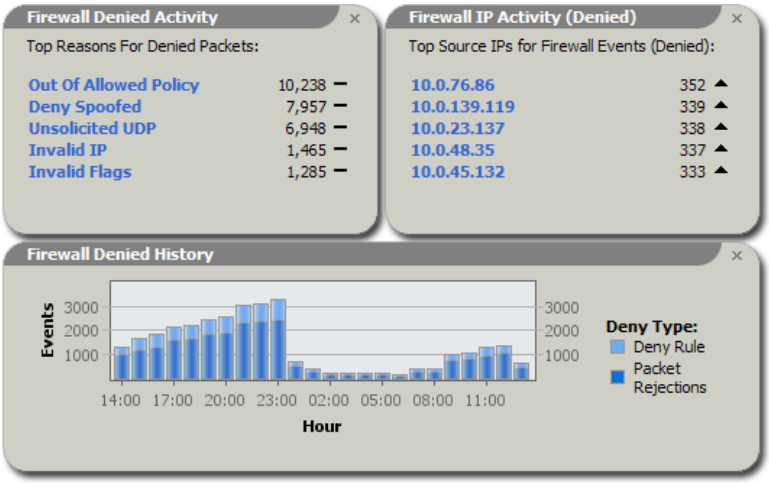
Date/Time Range

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 To Dashboard...** on the toolbar to view the list of available widgets.

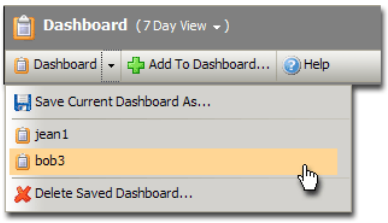
Many widgets contain links to let you "drill down" to the data. For example, clicking on a column in the Events graph brings up a screen listing all the system events that occurred on that day.

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 period, and a flat line indicates no significant change.

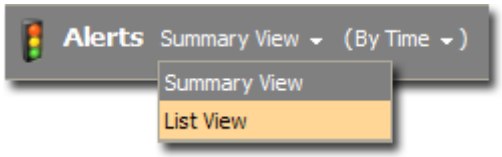
Saving Dashboard Layouts

Individual Dashboard layouts can be saved, loaded, and deleted using the **Dashboard** drop-down menu in the toolbar:



Alerts

The **Alerts** screen displays all active alerts. Alerts can be displayed in a Summary View, which will group 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 on "Show Details") displays all the objects (Computers, filters, etc.) to which the alert applies. (Clicking on the object will bring up its Properties screen.)

In Summary View if the list of objects is longer than five, an ellipsis ("...") appears after the fifth one. Clicking on 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 check box next to the target of the alert and clicking on the "**Dismiss**" link. (In List View, right-click on the alert to see the list of options in the context menu.)

Alerts can be of two types: System and Security. System Alerts (Computer Offline, Clock Change on Computer, etc.) are configured in the **System > Alert Configuration** screen. Security Alerts are triggered by Firewall Rules and IPS Filters.

All Alerts have default severity ratings (critical, or warning). These ratings can be changed on the **System > Alert Configuration** screen.

Use the "Computer" filtering bar to view only Alerts for Computers in a particular domain, with a particular Security Profile, etc.

Firewall Events

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

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

From the main screen, you can:

1. **View** () the properties of a particular event.
2. **Search**() for a particular event, or
3. **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events.
4. **Export**() the event list data to a CSV file.

Additionally, right-clicking on a log entry gives you the following options:

- **Computer Properties:** View the properties of the Computer that generated the log entry.
- **Firewall Rule Properties:** View all the properties of a particular log entry on its **Properties** screen.
- **Whois Source IP:** Perform a whois on the source IP.

> "WHOIS" is a TCP-based protocol used for determining the owner of a domain name or an IP address on the Internet.

- **Whois Destination IP:** Perform a whois on the destination IP.

Columns for the Firewall Event logs 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.
- **Action:** The action taken by the Firewall Rule or Stateful Configuration. Possible actions are: Deny, and Log Only.
- **Rank:** The Ranking system provides a way to quantify the importance of IPS and Firewall Events. By assigning "asset values" to Computers, and assigning "severity values" to IPS Filters 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 IPS 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 brings up the **Properties** screen for that entry which displays all the information about the event on one screen.

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 Computer domains or Computer Security Profiles.

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

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.

IPS Events

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

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

From the main screen, you can:

1. **View**( ) the properties of a particular event.
2. **Search**( ) for a particular event, or
3. **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events.
4. **Export**( ) the event log data to a CSV file.

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

- **Computer Properties:** View the properties of the Computer that generated the log entry.
- **IPS Filter Properties:** View the all the properties of a particular log entry on open **Properties** screen.
- **Whois Source IP:** Perform a whois on the source IP.
- **Whois Destination IP:** Perform a whois on the destination IP.

Columns for the IPS Filter logs display:

- **Time:** Time the event took place on the Computer.
- **Computer:** The Computer on which this event was logged.
- **IPS Filter:** The name of the IPS Filter.
- **Action:** What action the IPS Filter took (Allow, Deny, Force Allow, Log Only, or Detect Only (if the filter is in **Detect Only** mode)).
- **Rank:** The Ranking system provides a way to quantify the importance of IPS and Firewall Events. By assigning "asset values" to Computers, and assigning "severity values" to IPS Filters 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 IPS 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 brings up the **Properties** screen for that entry.

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 Computer domains or Computer Security Profiles.

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

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.

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:

1. **View**() the details (properties) of a system event
2. **Search**() for a particular system event, or
3. **Export**() currently displayed system events to a CSV file

View

Selecting an event and clicking on **View (** ) brings up the **Event Viewer Properties** screen. The **Event Viewer** has two panels.

1. General Information

- **Time:** The time according to the system clock on the Computer.
- **Type:** The type of event that occurred. Event types 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 on the object's identification will bring up the object's properties sheet.

2. 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 Computer Domains or Computer Security Profiles.

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

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

You can export displayed events (all pages) to a CSV file. You have the option of displaying the displayed list or the selected items.

Reports

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

Alert Report

The Alert Report displays graphs of alert activity during the period you specified, and a table listing the twenty most commonly raised alerts over the period.

Attack Report

The Attack Report displays activities relating directly to security. The Summary table displays a summary of traffic analysis activity and breaks it down according to attack prevention/detection techniques and filter types. It also distinguishes between defenses that are in Intrusion Prevention mode (blocking malicious traffic), and Intrusion Detection mode (logging malicious traffic but not blocking any -- usually implemented during testing phases.)

Subsequent tables display the most commonly triggered filters.

Firewall Report

The Firewall Report displays a record of Firewall Rule and Stateful Configuration activity over the specified date range.

Note that if you disable logging for a particular filter, that filter's activity will stop being incremented in this report.

Forensic Computer Audit Report

The Forensic Computer Audit Report displays the configuration of a Client Plug-in on a Computer at a particular time and for how long that configuration has been in effect.

Computer Report

The Computer Report displays a summary about each Computer listed in the **Computers** screen. You can filter the reports by Computer, by Domain, or by Security Profile. The report displays a chart and a table of how many Computers are in a particular state, followed by a summary for each Computer.

IPS Report

The IPS Report displays a record of IPS Filter activity over the specified period.

Note that if you disable logging for a particular filter, that filter's activity will stop being incremented in this report.

Computers

The **Computers** screen lets you to manage and monitor the Computers on your network. This screen regularly updates itself to ensure that displayed information does not become out of date. Use this screen to organize your Computers into domains and manage the Security Profiles that you have applied to them. From the **Computers** screen you can:

- **Scan** ( ) Computers for open ports
- Scan Computers for **Recommendations** ( )
- View or edit the **Properties** ( ) of a Computer
- Assign ( ) a **Security Profile** to a Computer
- **Delete** ( ) a Computer from the Computers list
- Search ( ) for a Computer

Right-clicking on a Computer brings up a shortcut menu from which you can carry out most of the above tasks, as well as:

- **Deploy** Client Plug-in(s)
- **Remove** Client Plug-in(s)
- **Activate/Reactivate** ( ) the Client Plug-in on a Computer

> After being installed on a Computer, a Client Plug-in must be "activated" by the Server Plug-in. During this process, the Server Plug-in sends a "fingerprint" to the Client Plug-in. From that point on, the Client Plug-in will only accept instructions from an Server Plug-in with that unique fingerprint.

- **Check the Status** ( ) of the Client Plug-in
- **Deactivate** ( ) the Client Plug-in on a Computer
- **Update** ( ) the Client Plug-in on a Computer
- **Get Events** ( ) from a Client Plug-in
- **Clear Warnings or Errors** on the Computer
- **Lock** ( ) a Client Plug-in
- **Unlock** ( ) a Client Plug-in
- **Cancel any currently executing port scans** ( )
- **Clear Recommendations for this Computer** ( )
- **Assign an Asset Value to this Computer** ( )
- Examine System **Events** associated with this Computer
- Examine the **Firewall and IPS Event Logs** associated with this Computer

Additionally, right-clicking on the Computer's icon (Computers) or a Domain icon (Workgroup) in the navigation pane brings up a shortcut menu with the following additional options that apply to domains of Computers:

- **Assign** ( ) a Security Profile to all the Computers in the current domain
- **Assign an Asset Value** ( ) to this to all Computers in this domain
- View or edit the **Properties** ( ) of a Domain

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. You can change this range in the **System > Settings** section under the **scan** tab.)

The Server Plug-in always scans port 4118 regardless of port range settings. It is the port on the Computer to which Server Plug-in-initiated communications are sent. If you set communication direction to "Client Plug-in-initiated" on a Computer (**Computer Properties > Advanced > Computer > Communication Direction**), port 4118 is closed.

Scan Computers for Recommendations

Scan for Recommendations causes the Client Plug-in to scan the Computer for common applications and then make filtering recommendations based on what is detected. Recommendations that have not been automatically applied will raise an Alert. The results of a recommendation scan can also be seen on the Computer's **Properties** screen on the **IPS Filters** tab: if the IPS filters are sorted by Application Type, recommended Application Types will have a green flag displayed next to their name. Recommendation Scan settings can be configured on Security Profiles and on individual Computers themselves.

View Computer Properties

The **Computer Properties** screen has five tabs: **Computer Properties**, **Firewall Rules**, **Stateful Configurations**, **IPS Filters**, and **Actions**.

Computer Properties

The **Computer Properties** tab has four panels, an **SSL** button, and an **Advanced** button.

1. General Information

- **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 operating system will appear here.
- **Computer Domain:** The domain to which the Computer belongs.
- **Security Profile:** The Security Profile (if any) that you have assigned to this Computer.
- **Asset Value:** The Server Plug-in uses a ranking system to quantify the importance of IPS and Firewall Events. IPS Filters, Firewall Rules, and Assets (Computers) are assigned a numerical value. When an IPS Filter or Firewall Rule is triggered on a Computer, those values are multiplied together. This produces a score that you can use to sort Events by importance. (Event ranking can be seen on the **Monitoring > Firewall Events** and **Monitoring > IPS Events** screens.) Use this **Asset Value** drop-down list to assign a value to this Computer. (To configure Ranking settings, go to **System > Settings > Ranking**.)
- **Lock Computer:** Ticking this check box blocks all communications between the Client Plug-in and the Server Plug-in. The Computer's Security Profile is still active (all filters and rules are still applied to all traffic), but should any alerts be generated, they will not be sent to the Server Plug-in. (The remove Client-Plug-in operation is exempt.)

You may wish to lock a Computer if you are going to perform some maintenance on it and do not want a series of alerts to appear in the Server Plug-in.

2. 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-client 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.)
- **Computer Events Button**: Displays System Events associated with this Computer.

3. Firewall (Firewall Rules, Stateful Configurations)

Choose whether you want Firewall protection enabled or disabled. Selecting "Inherited" means that the Security Profile applied to this Computer will determine whether the Firewall is enabled or disabled. The Computer will inherit the setting from the Security Profile. (Disabling the Firewall for a particular Security Profile will disable the Firewall on all Computers whose Firewall Control setting is set to "Inherited".)

4. Intrusion Prevention (IPS Filters)

Like the Firewall, Intrusion Prevention can be turned on or off on a particular Computer using these settings. Selecting "Inherit" means that whether Intrusion Prevention on this Computer is on or off depends on what the Security Profile assigned to this Computer is set to. "Prevent (IPS)" means the Intrusion Prevention is on. "Detect (IDS) " means that Intrusion Prevention is in log-only mode. Traffic will be monitored, any IPS Filters and rules that are triggered will be logged (if they are set to log), alerts will be sent if configured to do so, but no traffic will be blocked. "Off" means that no IPS Filtering will take place at all.
Perform ongoing Scans for Recommendations: You can choose to have the Client Plug-in periodically scan the Computer and then make recommendations. The frequency of these recommendation scans can be set globally for all Computers from **System > Settings > Scan.**

Automatically assign recommended filters to Computers during Scans for Recommendations: Select this check box to apply recommended filters to the Computer. If this check box is not selected, an alert will be raised (unless the alerts for Recommendation Scans have been turned off.).

5. SSL

The Client Plug-in supports IPS Filtering of SSL traffic. The SSL dialog allows you to create SSL Configurations for a given certificate-port pair on one or more interfaces. You can import Certificates in **PKCS 12** or **PEM** format. Windows Computers have the option of using **Windows CryptoAPI** directly.

Clicking the **SSL...** button brings up the **SSL Computer Configurations** screen which lists existing SSL configurations and allows you to create new ones.

Double-click an existing configuration to bring up its **Properties** screen with an **Assignment** tab and a **Credentials** tab.

Assignment

- **General Information:** The name and description of the SSL configuration, and whether it is enabled on this Computer.
- **Interface Assignments:** The interfaces this configuration is being applied to
- **Port Selection:** The 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.

For information on setting up SSL filtering, see **How To... Filter SSL Data Streams**

6. Advanced Settings

Throughout the Server Plug-in's interface, many configurations settings can be set globally but then overridden further down a hierarchical chain. For example, Heartbeat Frequency can be set globally in **System > Settings > Computers > Heartbeat**, but then can be overridden in a particular Security Profile in **Security Profile > Properties > Computer > Heartbeat**, and yet again even further down the chain at the individual Computer level (**Computers > Properties > Computer Properties > Advanced > Computer > Heartbeat**). At any level below the global level, the default setting is to inherit from the level above. In these cases, the user interface will display the word "Inherited" followed by what the inherited setting is.

Computer

- **Communication Direction: Direction of Server Plug-in to Client Plug-in communications:** At the default setting (**bi-directional**), the Client Plug-in will initiate the heartbeat but will still listen on the Client Plug-in port for Server Plug-in connections and the Server Plug-in is free to contact the Client Plug-in in order to perform operations as required. **Server Plug-in-initiated** means that the Server Plug-in will initiate all communications. Communication will occur when the Server Plug-in performs scheduled updates, performs heartbeat operations (below), and when you choose the **Activate/Reactivate** or **Update Now** options from the Server Plug-in interface. If you want to completely close off the Computer to communications initiated by any remote source, you may 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**.
- **Heartbeat:** 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.
- **Computer Access Schedule:** The periods during which the Server Plug-in can apply automated/queued updates to the Client Plug-in. Heartbeats will still occur. This setting is mainly to prevent updates from being applied or recommendation scans to be run during a server's busiest time. Updates can still be applied manually at any time by right-clicking on the Computer and selecting "Update Client Plug-in(s) Now". This setting can be inherited from the Security Profile that was assigned to this Computer or you can select another predefined schedule from the drop-down list.
- **Troubleshooting:** Choose whether to inherit the logging-override settings from the Security Profile assigned to this Computer ("Inherited"), to not override logging settings ("Do Not Override"), to log all triggered Firewall Rules ("Full Firewall Event Logging"), to log all triggered IPS Filters ("Full IPS Event Logging"), or to log all triggered filters ("Full Logging").

Whether logging takes place is configured at three different levels: the filters themselves, Security Profiles that include particular filters, and Computers to which the Security Profiles/filters are assigned. Logging levels are inherited in that order. The option to override logging levels exists mainly for debugging purposes. When initially applying a set of filters to a Computer, you may want to log all

filtering activity on that one Computer alone without having to change the logging settings for each individual filter that is being applied to this Computer. Using the override option lets you log all filtering on an individual Computer without turning it on on all other Computers at the same time.

Firewall

- **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. Firewall 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 Firewall Rules in place.
    - **Collect Firewall Events from Client Plug-in:** Periodically retrieve the latest Firewall logs from the Client Plug-in.

Logs are records of individual events. **Counters** are a record of the number of times individual events have occurred. Logs are used to populate the "Events" screens (Firewall Events, IPS Events, System Events). 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 log collection. Logs can potentially take up a lot of disk space and you might not want to store the data twice.

    - **Do not record logs with source IP of:** This option is useful if you want Intrusion Defense Firewall to not make log entries for traffic from certain trusted Computers.
    - **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.)
- **Advanced Firewall Events:** For information on Advanced Firewall Events, see **System > Settings > Firewall.**

IPS

- **IPS Events:** You can set the maximum size of each individual log file and how many of the most recent files to keep. IPS 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. IPS 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 IPS Filters in place.
    - **Collect IPS Events from Client Plug-in:** Periodically retrieve the latest IPS logs from the Client Plug-in.
    - **Do not record Logs with source IP of:** This option is useful if you do not want Intrusion Defense Firewall to log traffic from certain trusted Computers.
    - **Allow IPS Filters to capture data for the first hit of each filter:** Keep the data from the packet that triggered a log entry. (You can view the packet's data with the log entry. Each filter will only capture data once every five minutes per filter to avoid unduly large log files.)
- **Advanced IPS Events:** For information on Advanced IPS Events, see **System > Settings > IPS.**

Analysis

For information on Traffic Analysis, see **System > Settings > Analysis.**

Scan

- **Scanning for Open Ports:** Select a port list to use when the 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 filtering recommendations based on what is detected. This setting sets the interval between scans on Computers that have been configured to allow them. (You can configure Client Plug-ins to allow scans from their Computer's **Properties** screens.)

Notifications

- **Use Inherited Settings:** Use this option to inherit settings from the next level up.
- **Do Not Forward Logs:** No forwarding of logs from this Client Plug-in
- **Forward Logs To:** Override settings and send logs to a particular Syslog server.

Firewall Rules

The **Firewall Rules** tab displays the Firewall Rules assigned to this Computer's interface(s).

Notice that all the defined interface types in the left pane are nested under a "Global" parent. Trend Micro recommends assigning all filters that will be common to all interfaces to this Global interface type. Only filters that are specifically designed for particular interface types should actually be assigned at the interface type level. If by some oversight a newly installed interface is not assigned a Type, it will nevertheless have some default protection.

The Client Plug-in will detect and display all interfaces on the Computer. When a previously listed interface is no longer detected (for example, if it has been removed from the Computer), it will still be listed here but grayed out. This is because the Server Plug-in assumes the situation will not be permanent and it will not discard any settings. If you know that the grayed out interface will not be returned to the Computer, you can remove it manually from the list using the right-click menu.

If you are using virtual interfaces on the Computer then the physical interface must have a static IP address. The Client Plug-in will not recognize the virtual interfaces if the physical interface is set to use DHCP.

Note that if you are using virtual interfaces the **Firewall Rules** tab will display each of the individual IP addresses. The Server Plug-in will allow you apply Firewall Rules to the individual IP addresses, but you should keep in mind that they are on the same physical interface. Therefore if you apply an allow rule to one IP it effectively applies a deny rule to all traffic on all other IP addresses on the same interface. When using virtual interfaces you should apply Firewall Rules to the physical interface only and not to individual IP addresses.

Firewall Rules are listed next to check boxes. A checked box that has been grayed out means that this Firewall Rule is being applied to traffic on this Computer because the Security Profile assigned to the Computer includes the filter. Rules that are checked and *not* grayed out have been assigned to this Computer directly and not because they are included in a Security Profile.

Editing the Properties of a Firewall Rule from the Computer Properties Screen

You can examine and edit the properties of a Firewall Rule from the Computer Properties screen. Changes you make to the Firewall Rule can either be applied to the rule as it is applied to this Computer only, or they can be applied to all Computers that make use of this rule now or in the future. To make changes to the rule locally on this Computer only, right-click on the rule and select "Firewall Rule Properties (This Computer Only)" and make your changes. To make changes to the Firewall Rule globally on all Computers, right-click on the rule and select "Firewall Rule Properties" (or simply double-click on the rule).

Note that only the specific element of the Firewall Rule on this Computer will be changed. If later on you change a different element of the Firewall Rule without specifying "This Computer Only", that change will be applied to all Computers making use of this rule.

This ability to change an element's properties locally or globally applies to Firewall Rules, IPS Filters, and Application Types.

Stateful Configuration

The **Stateful Configuration** tab displays the Stateful Configuration assigned to this Computer's interface(s).

Notice that all the defined interface types in the left pane are nested under a "Global" parent. Trend Micro recommends assigning all filters that will be common to all interfaces to this Global interface type. Only filters that are specifically designed for particular interface types should actually be assigned at the interface type level. If by some oversight a newly installed interface is not assigned a Type, it will nevertheless have some default protection.

The Client Plug-in will detect and display all interfaces on the Computer. When a previously listed interface is no longer detected (for example, if it has been removed from the Computer), it will still be listed here but grayed out. This is because the Server Plug-in assumes the situation will not be permanent and it will not discard any settings. If you know that the grayed out interface will not be returned to the Computer, you can remove it manually from the list using the right-click menu.

Use this screen to select which Stateful Configuration will be applied to the interface(s) on this Computer. As the radio buttons suggest, only one Stateful Configuration can be applied to an interface at any given time. You can create and edit Stateful Configurations from this screen as well as from the **Stateful Configurations** screen.

Note that any changes you make to a Stateful Configuration from this screen will affect all Computers making use of the same configuration.

IPS Filters

The **IPS Filters** tab displays the IPS Filters assigned to this Computer's interface(s).

Notice that all the defined interface types in the left pane are nested under a "Global" parent. Trend Micro recommends assigning all filters that will be common to all interfaces to this Global interface type. Only filters that are specifically designed for particular interface types should actually be assigned at the interface type level. If by some oversight a newly installed interface is not assigned a Type, it will nevertheless have some default protection.

The Client Plug-in will detect and display all interfaces on the Computer. When a previously listed interface is no longer detected (for example, if it has been removed from the Computer), it will still be listed here but grayed out. This is because the Server Plug-in assumes the situation will not be permanent and it will not discard any settings. If you know that the grayed out interface will not be returned to the Computer, you can remove it manually from the list using the right-click menu.

IPS Filters are listed next to check boxes. A checked box that has been grayed out means that this IPS Filter is being applied to traffic on this Computer because the Security Profile assigned to the Computer includes the filter. Filters that are checked and *not* grayed out have been assigned to this Computer directly and not because they are included in a Security Profile.

Green flags ( ) indicate that the Application Type (and its associated IPS Filters) have been recommended for this Computer because of a Recommendation Scan. A partial green flag ( ) next to the name of the Application Type indicates that not all the IPS Filters associated with the Application Type are recommended for the Computer.

Editing the Properties of an IPS Filter from the Computer Properties Screen

You can examine and edit the properties of an IPS Filter from the Computer Properties screen. Changes you make to the IPS Filter can either be applied to the filter as it is applied to this Computer only, or they can be applied to all Computers that make use of this filter now or in the future. To make changes to the filter locally on this Computer only, right-click on the filter and select "IPS Filter Properties (This Computer Only)" and make your changes. To make changes to the IPS Filter globally on all Computers, right-click on the filter and select "IPS Filter" (or simply double-click on the filter).

Note that only the specific element of the IPS Filter on this Computer will be changed. If later on you change a different element of the IPS Filter without specifying "This Computer Only", that change will be applied to all Computers making use of this rule

This ability to change an element's properties locally or globally applies to Firewall Rules, IPS Filters, and Application Types.

Note that you can modify the port list associated with a particular application type for individual Computers as well. Right-click on the Computer(s) or the Application Type and select "Application Type Properties (for this Computer)" and make your changes.

Actions

The **Actions** tab has five panels:

1. Client Plug-in Activation

The Client Plug-in's fingerprint is used to uniquely identify the Computer to the Server Plug-in. It is a digest of the Client Plug-in's public certificate. If a Client Plug-in's public certificate is not in the Server Plug-in's database of certificates, the Server Plug-in can not verify the Client Plug-in's identity in server-client communications and so the Client Plug-in must be reactivated. Click the **Reactivate** button to do so.

2. Client Plug-in Update

- **Last Update Required:** The last time the Client Plug-in on this Computer was scheduled to receive an update. (If the last update was successful, only "Last Update Required" will be displayed. If the last update failed, the time and date of the last update attempt will be displayed next to "Last Update Required".)
- **Last Successful Update:** The last time the Client Plug-in on this Computer was successfully updated.

Press the **Update Client Plug-in Now** button to immediately apply any changes you have made to the Client Plug-in on this Computer (or to force the Server Plug-in to retry a Client Plug-in update if a previous update attempt failed). If you wish to cancel any pending/scheduled updates, press the "Cancel Update" button.

You can configure the server-client communication settings on the **Computer Communication** tab in the **System > Settings** section.

3. Client Plug-in Software

Use this panel to deploy or remove the Client Plug-in from this Computer. If a Client Plug-in is already installed on this Computer, its driver version number will be displayed here.

4. Computer Scan

Intrusion Defense Firewall performs two types of scan: a regular Port Scan, and a Recommendation Scan. The Port Scan will scan the range of ports defined on the **Scan** tab on the **System > Settings** screen in the **System** section. The Recommendation Scan examines the Computer for common applications and then makes filtering recommendations based on what is detected. Global Recommendation Scan settings are also configured on the **Scan** tab on the **System > Settings** screen in the **System** section.

5. Firewall/IPS Events

Displays the date and time of the last Firewall and IPS log retrievals from the Client Plug-in into the Server Plug-in. You can retrieve the latest logs ("Get Logs Now") and view them ("View Logs").

Assign a Security Profile to a Computer

To Assign a Security Profile to one or more selected Computers, either:

- Right-click and select **Actions > Assign Security Profile...**, or
- Click the **Assign Security Profile...** button () on the toolbar.

This opens a window with a drop-down list allowing you to assign a Security Profile to the Computer(s). 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), an asterisk will appear next to the name of the Security Profile indicating that the default settings have been changed.

Delete a Computer

To delete one or more selected Computers, either:

- Right-click and select **Delete**, or
- Click the **Delete** button () on the toolbar.

If you delete a Computer, you will delete all Client Plug-in configuration information pertaining to that Computer along with it.

Search for a Computer

The **Search** button lets you search for a particular Computer among already listed Computers.

Deploy Client Plug-in(s)

Deploy the Client Plug-in to the Computer. (Note that the Computer is not protected until you assign a Security Profile to the Client Plug-in.)

Remove Client Plug-in(s)

Uninstall the Client Plug-in from the Computer. (Note that removing the Client Plug-in will leave the Computer unprotected by Intrusion Defense Firewall and vulnerable to malicious intrusion.)

Activate/Reactivate the Client Plug-in on a Computer

When a Computer is unmanaged (that is, the Client Plug-in is not activated) the Client Plug-in must be activated to move it 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 manually deactivate the Client Plug-in from the Computer. See "How To... Manually Deactivate a Client Plug-in on a Computer " for more information.)
- **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 locally deactivated on the Computer from the command line. (See "How To... Manually Deactivate a Client Plug-in on a Computer " for more information.)
- **Unknown:** The Computer is in an unrecognized state.

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 on 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 OfficeScan 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 (see "How To... Manually Deactivate a Client Plug-in on a Computer " for more information) or from the Server Plug-in currently managing the Client Plug-in. (A Computer does not have to be reachable in order to be deactivated. If an unreachable deactivated Computer becomes reachable again, it will simply appear as a "New (Unknown)" Computer in the Computers List.)

Update the Client Plug-in on a Computer

Updating the Client Plug-in on a Computer pushes 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 (deactivated) locally or has simply been removed from the OfficeScan network before an administrator has had a chance to deactivate or delete the Computer from the Computers List.

Lock a Computer

You can lock a Computer if you are going to perform some maintenance on it and do not want to raise 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 raise 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 unaware 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", the Client Plug-in may generate an event that it will report when it finally contacts the Server Plug-in again.

Unlock a Computer

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 Filter recommendations resulting from a Recommendation Scan on this Computer. This will also remove the Computer from those listed in an Alert produced because of a Recommendation Scan.

Note that this action will not un-assign any rules or filters 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 filter to allow you to rank Firewall and IPS Filter Events. To configure Ranking, go to **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 Firewall or IPS Event Logs

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

View or edit the Properties of a Domain

The properties of Domains include their name and description.

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 assigned 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.

Security Profiles

Security Profiles allow common configurations of Firewall Rules, Stateful Configurations, and IPS Filters, (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 filters and rules that do not exist in the older version. Always make sure your Security Updates are current.

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

Clicking on **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 Properties** screen. Clicking on **Properties**( ) brings up the **Security Profile Properties** screen with five tabs (**Security Profile Properties**, **Firewall Rules**, **Stateful Configuration**, **IPS Filters**, and **Assigned To**).

Security Profile Properties

The **Security Profiles Properties** tab contains four panels and an **Advanced Settings** button.

1. General Information

- **Name:** The name of the profile.
- **Description:** A description of the Security Profile.

Do not hesitate to fully describe the purpose of the profile here. It will be easier for you or another administrator to determine what your intentions were for this profile by reading a detailed description than by examining all the properties and settings of a profile named "Second Profile" and described as "profile number 2".

2. Interface Assignments

If you have a Computer 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 click **Customize**. The **Customize Interface Assignments Properties** screen will appear.

Specify the number of interfaces you want this Security Profile to control and give a name to each. When the Security Profile is assigned to a Computer, it will detect existing interfaces and try to match their names to what you enter in the **Interface Name Matches** text box. Use the wildcard character ("*") to make sure all interfaces are recognized. (For example, "Local Area Connection 1", "Local Area Connection 2", and "Local

Area Connection 3" would all be detected with an entry such as "Local Area*".) Make sure multiple entries are on separate lines.

If interfaces are detected on the Computer but they do not match any of these entries, the Server Plug-in will raise an alert to notify you.

3. Firewall (Firewall Rules, Stateful Configurations)

Choose whether the Firewall should be on or off. This feature provides you with a master on/off switch for Firewall Rules and stateful inspection activity for this Security Profile. You may wish to temporarily switch off Firewall Rules for testing and troubleshooting purposes.

Note that if you apply a Security Profile with Firewall turned off 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.

4. Intrusion Prevention (IPS Filters)

Use these options to enable or disable IPS actions for this Security Profile. In **Prevent (IPS)** mode, all elements of the IPS are enabled and this Security Profile is operating as an **Intrusion Prevention System (IPS)**. In **Detect (IDS)** mode, IPS Filtering still takes place, but all events are only logged; no traffic is blocked or modified. The Security Profile operates as an **Intrusion Detection System (IDS)**. You can use this feature to introduce a new Security Profile to a set of Computers and watch how it performs before switching to Prevent (IPS) mode. Setting Intrusion Prevention to **Off** mode turns off filtering altogether. You may wish to use this feature if you are performing diagnostics, tests, or maintenance on Computers using this Security Profile.

Perform ongoing Scans for Recommendations: You can choose to have the Client Plug-in periodically scan the Computer and then make recommendations. The frequency of these recommendation scans can be set globally for all Computers from **System > Settings > Scan.**

Automatically assign recommended filters to Hosts during Scans for Recommendations: Selecting this check box will cause the recommended filters to be applied to the Computer. If this check box is not selected, an alert will be raised (unless the alerts for Recommendation Scans have been turned off).

5. Advanced Settings

Throughout the Server Plug-in interface, many configurations settings can be set globally but then overridden further down a hierarchical chain. For example, Heartbeat Frequency can be set globally in **System > Settings > Computers > Heartbeat**, but then can be overridden in a particular Security Profile in **Security Profile > Properties > Computer > Heartbeat**, and yet again even further down the chain at the individual Computer level (**Computers > Properties > Computer Properties > Advanced > Computer > Heartbeat**). At any level below the global level, the default setting is to inherit from the level above. In these cases, the user interface will display the word "Inherited" followed by what the inherited setting is.

Computer

- **Communication Direction: Direction of Server Plug-in to Client Plug-in communications:** At the default setting (**bi-directional**), the Client Plug-in will initiate the heartbeat but will still listen on the Client Plug-in port for Server Plug-in connections and the Server Plug-in is free to contact the Client Plug-in in order to perform operations as required. **Server Plug-in-initiated** means that the Server Plug-in will initiate all communications. Communication will occur when the Server Plug-in performs scheduled updates, performs heartbeat operations (below), and when you choose the **Activate/Reactivate** or **Update Now** options from the Server Plug-in interface. If you want to completely close off the Computer to communications initiated by any remote source, you may 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**.

- **Heartbeat:** 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.
- **Computer Access Schedule:** The periods during which the Server Plug-in can apply automated/queued updates to the Client Plug-in. Heartbeats will still occur. This setting is mainly to prevent updates from being applied or recommendation scans to be run during a server's busiest time. Updates can still be applied manually at any time by right-clicking on the Computer and selecting "Update Client Plug-in(s) Now". This setting can either be inherited from the Security Profile that was assigned to this Computer or you can select another predefined schedule from the drop-down list.
- **Troubleshooting:** Choose whether to inherit the logging-override settings from the Security Profile assigned to this Computer ("Inherited"), to not override logging settings ("Do Not Override"), to log all triggered Firewall Rules ("Full Firewall Event Logging"), to log all triggered IPS Filters ("Full IPS Event Logging"), or to log all triggered filters ("Full Logging").


Whether logging takes place is configured at three different levels: the filters themselves, Security Profiles that include particular filters, and Computers to which the Security Profiles/filters are assigned. Logging levels are inherited in that order. The option to override logging levels exists mainly for debugging purposes. When initially applying a set of filters to a Computer, you may want to log all filtering activity on that one Computer alone without having to change the logging settings for each individual filter that is being applied to this Computer. Using the override option lets you log all filtering on an individual Computer without turning it on all other Computers at the same time.

Firewall

- **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. Firewall 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 Firewall Rules in place.
    - **Collect Firewall Events from Client Plug-in:** Periodically retrieve the latest Firewall logs from the Client Plug-in.
    - **Do Not Record Logs with Source IP of:** This option is useful if you do not want Intrusion Defense Firewall to log traffic from certain trusted Computers.
    - **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.)
- **Advanced Firewall Events:** For information on Advanced Firewall Events, see **System > Settings > Firewall.**

IPS

- **IPS Events:** You can set the maximum size of each individual log file and how many of the most recent files are kept. IPS 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. IPS 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 IPS Filters in place.
    - **Collect IPS Events from Client Plug-in:** Periodically retrieve the latest IPS logs from the Client Plug-in.
    - **Do Not Record Logs with Source IP of:** This option is useful if you do not want Intrusion Defense Firewall to log traffic from certain trusted Computers.
    - **Allow IPS Filters to capture data for the first hit of each filter:** Keep the data from the packet that triggered a log entry. (The packet's data can be viewed with the log entry. Each filter will only capture data once every five minutes to avoid unduly large log files.)
- **Advanced IPS Events:** For information on Advanced IPS Events, see **System > Settings > IPS.**

Analysis

For information on Traffic Analysis, see **System > Settings > Analysis.**

Scan

- **Scanning for Open Ports:** Select a port list to be used when the 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 filtering recommendations based on what is detected. This setting sets the interval between scans on Computers that have been configured to allow them. (Use a Computer's **Properties** screen to configure a Client Plug-in to allow scans.)

Notifications

- **Use Inherited Settings:** Use this option to inherit settings from the next level up.
- **Do Not Forward Logs:** No forwarding of logs from this Client Plug-in
- **Forward Logs To:** Override settings and send logs to a particular Syslog server.

Firewall Rules

The **Firewall Rules** tab contains a list of all Firewall Rules with check boxes indicating which Firewall Rules are assigned to this Security Profile. Use this screen to add or remove Firewall Rules to or from this Security Profile. You can create and modify Firewall Rules from this tab as well as from the **Firewall Rules** screen.

Editing the Properties of a Firewall Rule from the Security Profiles Properties Screen

You can examine and edit the properties of a Firewall Rule from the Security Profile Properties screen. Changes you make to the Firewall Rule can either be applied to the rule as it is applied to this Security Profile only, or they can be applied to all Computers that make use of this filter now or in the future. To make changes to the rule locally for this Security Profile only, right-click on the rule and select "Firewall Rule Properties (For This Profile)" and make your changes. To make changes to the Firewall Rule globally, right-click on the rule and select "Firewall Rule Properties" (or simply double-click on the rule). Note that only the specific element of the Firewall Rule in this Security Profile will be changed if you make a "local" edit. If later on you change a different element of the "master copy" of the Firewall Rule, that change will still be pushed down to this local copy of the rule.

 This ability to change an element's properties locally or globally applies to Firewall Rules, IPS Filters, and Application Types.

 Notice that all the defined interface types in the left pane are nested under a "Global" parent. Trend Micro recommends assigning all filters that will be common to all interfaces to this Global interface type. Only filters that are specifically designed for particular interface types should actually be assigned at the interface type level. If by some oversight a newly installed interface is not assigned a Type, it will nevertheless have some default protection.

 Also note that filters assigned at the Global level are applied before filters at the interface-type level. For instance, if you applied a filter at the Global level that allowed only TCP traffic and applied another filter at a particular interface-type level that allowed UDP traffic, the second filter would have no effect since all UDP traffic would have been dropped by the Global filter.

Stateful Configuration

The **Stateful Configuration** tab contains the list of defined Stateful Configurations. You can create and modify Stateful Configurations from this screen as well as from the **Stateful Configurations** screen.

IPS Filters

The **IPS Filters** tab contains the list of IPS Filters that get applied with this Security Profile. You can create and modify IPS Filters from this screen as well as from the **IPS Filters** screen.

Editing the Properties of an IPS Filter from the Security Profile Properties Screen

You can examine and edit the properties of an IPS Filter from the Security Profile Properties screen. Changes you make to the IPS Filter can either be applied to the filter as it is applied to this Security Profile only, or they can be applied to all Security Profiles that make use of this filter now or in the future. To make changes to the filter locally in this Security Profile only, right-click on the filter and select "IPS Filter Properties (For this Profile)" and make your changes. To make changes to the IPS Filter globally, right-click on the filter and select "IPS Filter" (or simply double-click on the filter). Note that only the specific element of the IPS Filter in this Security Profile will be changed. If later on you change a different element of the "master copy" of the IPS Filter, that change will still be pushed down to this copy of the Filter.

This ability to change an element's properties locally or globally applies to Firewall Rules, IPS Filters, and Application Types.

Note that the port list associated with a particular application type can be modified for individual Computers as well. Right-click on the Computer(s) or the Application Type and select "Application Type Properties (for this Computer)" and make your changes.

Assigned To

The **Assigned To** tab contains a list of the Computers to which this profile is currently assigned.

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 a Domain of Computers.

Firewall Rule icons:

-  Normal Firewall Rules
-  Firewall Rules that operate according to a schedule
-  Firewall Rules that have been assigned because they are part of a Security Profile (Only appears on the **Firewall Rules** tab of an individual Computer's **Properties** screen.)

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 ()
- **Search** () for a particular 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 assigned to one or more Computers or part of a Security Profile cannot be deleted from the Server Plug-in.

Firewall Rule Properties

Clicking on New( New) or Properties() brings up the **Firewall Rules Properties** screen with three tabs (**Firewall Rule Properties**, **Options**, and **Assigned To**).

1. General Information

- **Name:** The name of the Firewall Rule.
- **Description:** A detailed description of the Firewall Rule.
- **Filter Action:** Your Firewall Rule can behave in five 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 IPS 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.
    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 filter *without* excluding any other traffic.)
    4. It can **deny** traffic (it will deny traffic defined by this filter.)
    5. It can **allow** traffic (it will *exclusively* allow traffic defined by this filter.)

Only one filter action is applied to any particular packet, and filters (of the same priority) are applied in the order listed above.

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

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

- **Packet Direction:** Select whether this filter will be applied to **incoming** or **outgoing** traffic.
- **Frame Type:** Select or specify the frame type your filter will be looking for. Use the check box 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 filter will be looking for. Use the check box 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).

2. 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.

3. 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.

4. 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

Select whether or not this Firewall Rule should raise 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.

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

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

Assigned To

This tab displays a list of Security Profiles which include this filter as well as any Computers to which this filter 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

Intrusion Defense Firewall'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 that 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 ()
- **Search** () for a particular Stateful Configuration (if you have that many)
- **Export** () one or more Stateful Configurations 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 on **New**( New) or **Properties**() brings up the **Stateful Configuration Properties** screen with five tabs (**Stateful Configuration Properties**, **TCP**, **UDP**, **ICMP**, and **Assigned To**).

Stateful Configuration Properties

The **Properties** tab contains two panels.

1. General Information

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

2. IP Packet Inspection

- **Deny all incoming fragmented packets:** If you enable this option, 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

The **TCP** tab contains two panels:

1. 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 from 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 Computer that initiated the connection.
- **Enable Ack Storm protection when the number of already acknowledged packets exceeds:** Set the number duplicate ACK packets to accept before either rejecting the packet or closing the connection.

2. 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 Computer.
- **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 Computer.

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

UDP

The **UDP** tab contains one panel:

1. UDP Packet Inspection

- **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 filter 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

The **ICMP** tab contains one panel:

1. ICMP Packet Inspection

- **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 filter will create or update its ICMP "stateful" table and will then only allow an ICMP response if it occurs within 60 seconds of the request. (ICMP pair types supported: Type 0 and 8, 13 and 14, 15 and 16, 17 and 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 particular stateful inspection configuration.

IPS Filters

Whereas Firewall Rules and Stateful Configurations examine a packet's control information (data that describes the packet), IPS Filters examine the actual content of the packet (and sequences of packets). Based on rules defined within the IPS Filter, 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.

IPS Filter icons:

- Normal IPS Filters
- IPS Filters that operate according to a schedule
- IPS Filters that have been assigned because they are part of a Security Profile (Only appears on the **IPS Filters** tab of an individual Computer's **Properties** screen.)
- IPS Filters that have configuration options.
- IPS Filters that *require* configuration.

The **IPS Filters** screen lets you create and manage IPS Filters. From the toolbar or the right-click shortcut menu, you can:

- Create **New** IPS Filters from scratch (New)
- **Import** ( ) IPS Filters from an XML file
- Examine or modify the **Properties** of an existing IPS Filter ( )
- **Duplicate** (and then modify) existing IPS Filters ( )
- **Delete** an IPS Filter ( )
- **Search** ( ) for a particular IPS Filter
- **Export** ( ) one or more IPS Filters 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)
- Create or modify **Application Types** ( )

Clicking on **New** (New) or **Properties** ( ) brings up the **IPS Filter Properties** screen with five tabs (**IPS Filter Properties**, **Vulnerability**, **Configuration/Rules**, **Options**, and **Assigned To**).

Note the **Configuration/Rules** tab. IPS Filters from Trend Micro or third party companies are not directly editable through the Server Plug-in. Instead, if the IPS Filter requires (or allows) configuration, those configuration options will be available on the **Configuration** tab. Custom IPS Filters that you write yourself will be editable, in which case the **Rules** tab will be visible.

IPS Filter Properties

The **IPS Filter Properties** tab has four panels:

General Information

- **Name:** The name of the IPS Filter.
- **Description:** The description of the IPS Filter.

Details

- **Application Type:** The Application Type this IPS Filter 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 IPS Filter. Higher priority filters are applied before lower priority filters.
- **Severity:** Setting the severity of a filter has no effect on how the filter is implemented or applied. The option to specify a severity level exists so that you can sort the display of your IPS Filters by this criterion by clicking on the **Severity** column when looking at your filters in a list.
- **Detect Only:** Use this check box when testing new filters. By checking this box, the filter 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" check box in the next panel (below), the filter's activity will not be logged regardless of whether "Detect Only" is checked or not.

Logging

- **Disable Event Log:** 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:** Check to include the packet data in the log entry.

Identification (Displayed for downloaded filters only)

- **Type:** Can be either Smart (one or more known and unknown (zero day) vulnerabilities), Exploit (an exact exploit, usually signature based), or Vulnerability (a specific vulnerability for which one or more exploits may exist).
- **Issued:** The date the Filter was released (not downloaded).
- **Identifier:** The filter's unique identifier tag.

Vulnerability (Displayed for downloaded filters only)

Displays information about this particular vulnerability.

Configuration (Displayed for downloaded filters only)

- **Configuration Options:** If the downloaded filter 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 filter without setting a required option, an alert will be raised telling you which filter on which Computer(s) requires configuration. (This also applies to any filters that are downloaded and automatically applied by way of a Security Update.)

IPS Filters that have configuration options are displayed on the **IPS Filters** screen with a small check mark over their icon ( ).

- **View Rules:** Click the **View Rules** button to see the code that defines the rules included in this filter. (Not always available.)

Rules (Displayed for custom filters only)

This tab will be visible for filters that you've written yourself. (Please contact Trend Micro for information on writing your own filters.)

Options

Select whether or not this IPS Filter should raise an alert when it is triggered. If you only wish this filter to be active during specific periods, assign a schedule from the drop-down list.

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

Assigned To

This tab displays the list of Computers to which this IPS Filter has been assigned.

Application Types

Application Types are a useful way of grouping IPS Filters. They are used to organize IPS Filters with a common purpose into groups. This simplifies the process of selecting a set of IPS Filters to assign to a Computer. For example, consider a set of IPS Filters required to protect HTTP traffic to an Oracle Report Server. By grouping IPS Filters into Application Types it is easy to select filters in the "Web Server Common" and "Web Server Oracle Report Server" sets while excluding, for example, the set of filters that would be specific to IIS Servers.

Application Type icons:

-  Normal Application Types
-  Application Types that have configuration options

From the main screen, you can:

1. Define a **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
5. **Search** () for an Application Type

Clicking on **New**( New) or **Properties**() brings up the Application Type **Properties** screen with three tabs (**Application Type Properties**, **Configuration**, and **Assigned To**).

> Note that the configuration tab appears on Application Types created by Trend Micro. If the Application Types require configuration, an explanation will appear on the tab.

Application Type Properties

The **Application Type Properties** tab contains two panels:

1. General Information

The name and description of the Application Type.

2. 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 IPS Filters 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 IPS Filters associated with this Application Type.

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)
- Examine or modify the **Properties** of an existing IP List ()
- **Duplicate** (and then modify) existing IP Lists ()
- **Delete** an IP List ()
- **Search** () for a particular 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 on New ( New) or Properties () brings up the IP List **Properties** screen with two tabs (**IP List Properties**, and **Assigned To**)

IP List Properties

The **IP List Properties** tab contains three panels:

1. General Information

The name and description of the IP list.

2. IPs

Type the IP addresses, masked IP addresses, and IP address ranges that are going to be on your list. Be sure to only put one of these per line.

3. Supported Formats

As well as individual addresses, you can enter 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 pound sign ("#").)

Assigned To

The **Assigned To** tab lists the Firewall Rules making use of this IP List.

Clicking on the names of the Firewall Rules brings up the **Properties** screen for those elements.

MAC Lists

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

From the main screen, you can:

- Create **New** MAC lists from scratch ( New)
- **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 ()
- **Search** () for a particular 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 on New ( New) or Properties () brings up the MAC List **Properties** screen with two tabs (**MAC List Properties**, and **Assigned To**).

MAC List Properties

The **MAC List Properties** tab contains three panels:

1. General Information

The name and description of the list.

2. MAC(s)

Type the MAC addresses that are going to be on your list. Put only one per line.

3. 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 Firewall Rules making use of this MAC list.

Clicking on the names of the Firewall Rules brings up their **Properties** screen.

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 ()
- **Search** () for a particular 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 on **New** ( New) or **Properties** () brings up the Port List **Properties** screen with two tabs (**Port List Properties**, and **Assigned To**)

Port List Properties

The **Port List Properties** tab contains three panels:

1. General Information

The name and description of the list.

2. Port(s)

Enter the ports that are going to be on your list. Be sure to only put one of these per line.

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

3. 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 Firewall Rules making use of this port list.

Clicking on the names of the Firewall Rules brings up their **Properties** screen.

Schedules

Schedules are used by various elements of the Intrusion Defense Firewall. For example, they are used by the Server Plug-in to determine when updates can be carried out, as well as to define when particular Firewall Rules are in effect.

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 ( )
- **Search** ( ) for a particular 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 on New (New) or Properties ( ) brings up the Schedule Properties screen with two tabs (**Schedule Properties**, and **Assigned To**).

Schedule Properties

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

Assigned To

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

Alert Configuration

1. **Administrator Locked Out:** (Does not apply to this version of Intrusion Defense Firewall.)
2. **Administrator Password Expires Soon:** (Does not apply to this version of Intrusion Defense Firewall.)
3. **Application Type Recommendation:** the Server Plug-in has determined that a Computer on your network should be assigned an Application Type. This could be because a Client Plug-in was installed on a new Computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the Application Type to the Computer, open the 'Computer Properties' dialog box, click on the 'IPS Filters' tab, and assign the Application Type.

As of version 1.0, a single less verbose Recommendation Alert (called simply "**Recommendation**") is included. It is intended to replace the following three recommendation alerts: **Application Type Recommendation, IPS Filter Recommendation,** and **IPS Filter Removal Recommendation**. The three older alerts are turned off by default, but can be turned on if you want information that is more granular in your alerts. If you do turn them on, you should turn off the newer **Recommendation** alert to avoid redundancy.

4. **Client Plug-in Offline:** The Server Plug-in raises this Alert when the Client Plug-in has missed a specified number of heartbeats. You can configure this number on the **Computer Communications** tab in the **System > Settings** screen. This alert will be cleared automatically the next time the Server Plug-in successfully communicates with the Client Plug-in (either through a heartbeat or through a manually initiated operation (like clicking the **Update Client Plug-in Now** button on the **Actions** tab in the **Computer Properties** screen.)
5. **Clock Change Detected:** The Client Plug-in reports the time on the Computer at every heartbeat. The Server Plug-in uses this information to determine if the Computer clock has changed since the last heartbeat. The permitted clock drift is configurable on the **Computer Communication** tab in the **System > Settings** screen. This alert must be dismissed manually since an administrator may want to investigate any unexpected changes to the system clock on a Computer.
6. **Computer Configuration Required:** This alert is raised if you define a Security Profile that has multiple interface types and then apply it to a Computer that has one or more interfaces that do not match the ones defined in the Security Profile. This alert can generally be avoided by specifying "match strings" when defining multiple interface types. For example, if you anticipate finding a wifi and a LAN connection on your Computers, use the wildcard character ("*") and set the matches (on Windows machines) to "Local Area Connection*****" and "Wireless Connection*****".
7. **Computer Reboot Required:** On rare occasions, the Computer on which has Client Plug-in has just been installed, upgraded, or uninstalled must be rebooted. If so, this alert will be raised.
8. **Duplicate Computer Detected:** It is possible that you may inadvertently add a Computer to the system twice. Computers can be identified by hostname or by IP, and they can be added manually through the **New Computer** wizard or automatically via Discovery. The administrator may then try to activate the Client Plug-in twice, once for each entry in the Computers list. This alert is raised if the Server Plug-in detects that this has occurred. You must remove one of the duplicate Computers and, if necessary, reactivate the other Computer.
9. **Firewall Engine Offline:** This alert is raised whenever the Client Plug-in reports that a Firewall Rule engine on a Computer is offline. It is automatically cleared when the Client Plug-in reports that the engine is back online.
10. **Firewall Rule Alert:** This alert is raised when a particular Firewall Rule is triggered on a particular Computer or on a group of Computers to which a particular Security Profile has been applied. (To configure a Computer or a Security Profile to raise an alert when a particular Firewall Rule is triggered, go to the **Alerts** tab on the **Firewall Rule Properties** screen. From there you can configure the system to raise an alert when the Firewall Rule is triggered on particular Computers or on Computers to which a particular Security Profile has been assigned.)

Note that you can configure a Firewall Rule to raise an alert on a particular Computer *even if the Firewall Rule has not been assigned to the Computer at this time.* This way, if ever the filter *does* get assigned to the Computer, an alert will be raised if the filter is triggered.

11. **Heartbeat server failed:** The heartbeat server failed to start properly. This may be due to a port conflict. Client Plug-ins will not be able to contact the Server Plug-in until this problem is resolved. To resolve this problem ensure that another service is not using the port reserved for use by the

heartbeat server and restart Server Plug-in services. If you are not using the heartbeat service, you can turn off this alert.

12. **Incompatible Client Driver Version:** This alert is raised when the Server Plug-in detects a version of the Client Plug-in software that is more recent than it (and therefore incompatible). Upgrading the Server Plug-in to the latest version is recommended to resolve this incompatibility.
13. **Insufficient Disk Space:** The Client Plug-in has reported that is was forced to delete an old log file to free up disk space for a new log file. Please immediately free up disk space to prevent loss of IPS, Firewall and Client Plug-in Events.
14. **Intrusion Defense Firewall Server Plug-in License has Expired or Will Expire Soon:** The Intrusion Defense Firewall Server Plug-in license has expired, or will expire in the near future. You can remove this alert by changing your Activation Code or updating to a new license in the **System > Product License** screen.
15. **IPS Engine Offline:** This alert is raised whenever the Client Plug-in reports that an IPS Filter engine on a Computer is offline. It is automatically cleared when the Client Plug-in reports that the engine is back online.
16. **IPS Filter Alert:** This alert is raised when a particular IPS Filter is triggered on a particular Computer or on a group of Computers to which a particular Security Profile has been applied. (To configure a Computer or a Security Profile to raise an alert when a particular IPS Filter is triggered, go to the **Alerts** tab on the **IPS Filter Properties** screen. From there you can configure the system to raise an alert when the IPS Filter is triggered on particular Computers or on Computers to which a particular Security Profile has been assigned.)


Note that you can configure an IPS Filter to raise an alert on a particular Computer *even if the IPS Filter has not been assigned to the Computer.* This way, if ever the filter *does* get assigned to the Computer, an alert will be raised if the filter is triggered.

17. **IPS Filter Recommendation:** the Server Plug-in has determined that a Computer on your network should be assigned an IPS Filter. This could be because a Client Plug-in was installed on a new Computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the IPS Filter to the Computer, open the 'Computer Properties' dialog box, click on the 'IPS Filters' tab, and assign the IPS Filter.


As of version 1.0, a single less verbose Recommendation Alert (called simply "**Recommendation**") is included. It is intended to replace the following three recommendation alerts: **Application Type Recommendation, IPS Filter Recommendation,** and **IPS Filter Removal Recommendation**. The three older alerts are turned off by default, but can be turned on if you want information that is more granular in your alerts. If you do turn them on, you should turn off the newer **Recommendation** alert to avoid redundant alerts.

18. **IPS Filter Removal Recommendation:** the Server Plug-in has determined that a Computer on your network has an IPS Filter assigned to it that is not required. This could be because a vulnerable application was uninstalled, an existing vulnerability was patched, or the filter was unnecessarily assigned to begin with. To un-assign the IPS Filter from the Computer, open the 'Computer Properties' dialog box, click on the 'IPS Filters' tab, and clear the check box next to the IPS Filter.


As of version 1.0, a single less verbose Recommendation Alert (called simply "**Recommendation**") is included. It is intended to replace the following three recommendation alerts: **Application Type Recommendation, IPS Filter Recommendation,** and **IPS Filter Removal Recommendation**. The three older alerts are turned off by default, but can be turned on if you want information that is more granular in your alerts. If you do turn them on, you should turn off the newer **Recommendation** alert to avoid redundant alerts.

19. **IPS Filter Requires Configuration:** An IPS Filter requires configuration before use. Open the IPS Filter properties and select the ''Options'' tab for more information.
20. **Logs Suppressed:** The Intrusion Defense Firewall Client Plug-in has reported that one or more individual logs were suppressed in order to protect the Client Plug-in from a potential Denial of Service. Check the Client Plug-in's firewall events to determine the cause of the suppression.
21. **Newer version of the Server Plug-in is available:** A more recent version of the Server Plug-in software is available for download.

22. **Newer versions of Client Plug-in(s) are available:** New Client Plug-ins of the same major version are available. Go to the **System > Security Updates** screen to down load the new Client Plug-in software.
23. **Number of Computers exceeds license:** Client Plug-ins are running on more Computers than is permitted by your license agreement. Please contact Trend Micro if you wish to extend your license.
24. **Number of Gateway Client Plug-ins exceeds License:** (Not applicable to this version of Intrusion Defense Firewall.)
25. **Number of Server Plug-in Nodes Exceeds License:** (Not applicable to this version of Intrusion Defense Firewall.)
26. **Recommendation:** the Server Plug-in has determined that a Computer on your network should be assigned Application Types or IPS Filters. This could be because a Client Plug-in was installed on a new Computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the Application Type to the Computer, open the 'Computer Properties' dialog box, click on the 'IPS Filters' tab, and assign the Application Types or IPS Filters.
27. **Reconnaissance Detected: Computer OS Fingerprint Probe:** The Client Plug-in detected an attempt to identify the Computer operating system via a "fingerprint" probe. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the Computer's events to see the details of the probe.
28. **Reconnaissance Detected: Network or Port Scan:** The Client Plug-in detected network activity typical of a network or port scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the Computer's events to see the details of the scan.
29. **Reconnaissance Detected: TCP Null Scan:** The Client Plug-in detected a TCP "Null" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the Computer's events to see the details of the scan.
30. **Reconnaissance Detected: TCP SynFin Scan:** The Client Plug-in detected a TCP "SynFin" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the Computer's events to see the details of the scan.
31. **Reconnaissance Detected: TCP Xmas Scan:** The Client Plug-in detected a TCP "Xmas" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the Computer's events to see the details of the scan.
32. **Security Update is Available:** Go to the **System > Security Updates** screen and click ''Update From Security Center...'' or ''Update From Disk...'' in the **Security Update** box.
33. **Server Plug-in Offline:** The Server Plug-in is offline. It is possible the machine has experienced a hardware or software problem, or has simply lost network connectivity. Please check the status of the Server Plug-in's Computer.
34. **Server Plug-in Time Out of Synch:** The clock on each Server Plug-in Node must be synchronized with the clock on the database. If the clocks are too far out of synch (more than 30 seconds) the Server Plug-in Node will not perform its tasks correctly. Synchronize the clock on your Server Plug-in Node with the clock on the database.
35. **Trial Expires Soon:** This alert begins to appear seven days before your trial expires (if you have been issued an evaluation license). Once the trial period expires, you will no longer be able to log into the Server Plug-in. The Client Plug-ins running on your Computers will remain active and continue applying all filters, but you will not be able to make any modifications to them. Please contact Trend Micro to extend your trial period or to acquire a full license.
36. **Unable to Activate Client Plug-ins:** This could occur for a number of reasons. Look on the **Computer Properties** screen, or check the details of the system event for the Computer in question for more information. Commonly, this alert is raised when a Client Plug-in Deactivate is required (because the Client Plug-in is currently managed by another Server Plug-in), there is no Client Plug-in at all, or there is some sort of communication problem.
37. **Unable to Update Security Configuration:** This alert can be raised for a number of reasons -- usually a communication problem. Check the system and Computer events for details.
38. **Unable to Upgrade the Client Plug-in software:** (Not Applicable to this version of Intrusion Defense Firewall.)
39. **Upgrade of the Client Plug-in Software Recommended:** This alert is raised when the Server Plug-in detects that an older version of the Client Plug-in is in use. The Client Plug-ins for which this alert is raised are still compatible with the Server Plug-in but may not support some of its newer features. Upgrading to the latest version is recommended but not required since the older Client Plug-ins will ignore settings that they do not recognize. Go to the **System > Security Updates** screen to down load the new Client Plug-in software.
40. **Upgrade of the Client Plug-in Software Recommended (Incompatible IPS Filter(s)):** The current version of the Client Plug-in you are running on your Computer(s) cannot implement the latest filters from the Trend Micro Security Center because it is too old. You must upgrade the Client Plug-in software on this Computer. Go to the **System > Security Updates** screen to down load the new Client Plug-in software.
41. **Upgrade of the Client Plug-in Software Required:** This alert is raised when an older version of the Client Plug-in, which is not compatible with the current version of the Server Plug-in, is in use. While the Client Plug-in is in this state only heartbeat, check status, reactivate, and upgrade

operations are permitted until the Client Plug-in is upgraded. The Client Plug-in must be upgraded to resolve this incompatibility.

Alert Properties

The actions precipitated by each alert can be configured by opening the **Properties** screen () for the alert. Use the **Properties** screen to turn the alert on or off and change the email notification settings.

Settings

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

The **Settings** screen has eleven tabs: **Computers**, **Firewall**, **IPS**, **Analysis**, **Scan**, **Notifications**, **Ranking**, **System Events**, **Security**, **Security Center**, and **System**.

Note that the **Settings** screen has a **Save** button at the bottom right. Changes made to these **System > Settings** (all tabs) must be saved before they take effect.

1. 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-client communications are initiated by the Server Plug-in. This includes security configuration updates, heartbeat operations, and requests for Firewall or IPS Filter 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 (for example, 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 Client Plug-in can reach the Server Plug-in URL and heartbeat port. 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. The Server Plug-in URL and the heartbeat port are listed on the **Server Plug-in** tab on the **System > Settings** screen.

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

filter 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 filter will replace the hidden filter. 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: Turn this option on if, for example, your network has no DNS and you are using dynamic IPs. (The Server Plug-in always identifies Computers/Client Plug-ins by their unique fingerprint, not their IP addresses.)

Remote Activation

N/A

Heartbeat

- **Heartbeat Frequency (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 raises an alert. (For example, entering three will cause the Server Plug-in to raise 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 raised.

Note that this communication between the Server Plug-in and the Client Plug-in is distinct from the communication between the OfficeScan server and the OfficeScan client.

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

Don't forget to save your changes.

Automatically Update Computers

By default, any time you make a change to any element in the Server Plug-in, 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.) Changing the **Automatically Update Computers** option to "I will manually update Computers" means that after any changes, you will have to find affected Computers in the **Computers** screen, right-click on them and choose "Update Client Plug-in(s) Now" from the context menu.

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 pushed out 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 raises an alert can be configured on the **System > Alert Configuration** screen.

2. Firewall

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. Firewall 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 Firewall Rules in place.

- **Collect Firewall Events from Client Plug-in:** Retrieve the latest Firewall logs from the Client Plug-in at every Heartbeat.

Logs are records of individual events. **Counters** are a record of the number of times individual events have occurred. Logs are used to populate the "Events" screens (Firewall Events, IPS Events, System Events). 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 log collection; logs can potentially take up a lot of disk space and you might not want to store the data twice.

- **Do Not Record Logs with Source IP of:** This option is useful if you do not want Intrusion Defense Firewall to log traffic from certain trusted Computers.
- **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.)

Advanced Firewall

Custom Driver Settings

Although these settings are designed to be used for performance tuning, some of the timeouts can also be used to foil attempts at OS fingerprinting.

- **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.
- **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. (IPS Filtering of IPv6 traffic is not supported. It can only be blocked or allowed.)
- **Connection Cleanup Timeout:** Time to wait before cleanup of connection information after connection has closed.
- **Block Same Src-Dest IP Address:** Block or allow packets with same source and destination IP address. (Doesn't apply to loopback interface.)

Don't forget to save your changes.

3. IPS

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

- **Collect IPS Events from Client Plug-in:** Retrieve the latest IPS logs from the Client Plug-in at every Heartbeat.

Logs are records of individual events. **Counters** are a record of the number of times individual events have occurred. Logs are used to populate the "Events" screens (Firewall Events, IPS Events, System Events). 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 log collection; logs can potentially take up a lot of disk space and you might not want to store the data twice.

- **Do Not Record Logs with Source IP of:** This option is useful if you want Intrusion Defense Firewall to not make log entries for traffic from certain trusted Computers.
- **Allow IPS Filters to capture data for the first hit of each filter:** Keep the data from the packet that triggered a log entry. (The packet's data can be viewed with the log entry. Each filter will only capture data from one packet in five to avoid unduly large log files.)

Advanced IPS Settings

Custom Driver Settings

- **Fragment Timeout:** How long to keep fragmented packets.
- **Maximum number of fragmented IP packets to keep:** If configured to do so, the IPS filters 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.

4. Analysis

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

- **Detection Enabled:** Turn traffic analysis on or off.
- **Computers and networks to analyze:** 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.)
- **Computers and networks to ignore:** 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 Server Plug-in where an alert will be raised. You can configure the Server Plug-in to send an email notification when the alerts are raised. (See **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 Immediately** for this option.

Once an attack has been detected, you can direct the Client Plug-ins to block traffic from the source IPs for a period. 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 machine will only see traffic destined for itself, so a port scan is by far the most common variation that will be detected. If a machine however is acting as a router or bridge, it could see traffic for a number of other machines, making it possible for the Client Plug-in to detect a Computer scan (ex. scanning a whole subnet for machines 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.

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. April 2006.

For the "Notify IDF Immediately" option to work, the Client Plug-ins must be configured for **Client Plug-in-initiated** or **bi-directional** communication. (See **System > Settings > Computers.**) If enabled, the Client Plug-in will initiate a Heartbeat to the Server Plug-in immediately upon detecting the attack or probe.

5. Scan

Scanning For Open Ports

Select a port list to be used when the 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 filtering recommendations based on what is detected. This setting sets the interval between scans on Computers that have been configured to allow them. (Client Plug-ins can be configured to allow scans from their **Properties** screens.)

6. Notifications

Alert Notification (from the Server Plug-in)

Enter an email address to which all alert emails will be sent regardless of whether any administrators have been set up to receive notifications. (Which alerts will trigger the sending of an email can be configured from the **System > Alert Configuration** screen.)

Firewall And IPS Event Notification (from the Client Plug-ins)

Forward Firewall and IPS Events to a Remote Computer (via Syslog)

If you wish to store your logs on a dedicated syslog server, enter the required information in these fields. For information on configuring Syslog, see **How To... Set Up Syslog Integration**.

System Event Notification (from the Server Plug-in)

Forward System Events to a Remote Computer (via Syslog)

Notifications can be sent to a Syslog server. Enter the details of your syslog server here. For information on configuring Syslog, see **How To... Set Up Syslog Integration**.

Forward System Events to a Remote Computer (via SNMP)

Intrusion Defense Firewall also supports SNMP. The MIB file ("snmp.mib") is located in `\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall\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.

7. Ranking

The Ranking system provides a way to quantify the importance of IPS and Firewall Events. By assigning "asset values" to Computers, and assigning "severity values" to IPS Filters 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 IPS or Firewall Events.

Firewall Rule Severity Values

Severity values for Firewall Rules are linked to their actions: Deny, Log Only, and Packet Rejection. Use this panel to edit their values. A Firewall Rule's actions can be viewed and edited from the Rule's **Properties** screen.

IPS Filter Severity Values

IPS Filter Severity Values are linked to their severity: Critical, High, Medium, or Low. Use this panel to edit their values. An IPS Filter's severity can be viewed and edited from the Filter's **Properties** screen.

Computer Asset Values

Computer Asset Values are not associated with any of their other properties like IPS Filters or Firewall Rules. Instead, Computer Asset Values are properties in themselves. You can view and edit a Computer's Asset Value from the Computer's **Properties** screen. To simplify the process of assigning asset values, you can predefine some values that will appear in the **Asset Value** drop-down list on the Computer's **Properties** screen. To view existing predefined Computer Asset Values, click the **View Asset Values...** button in this panel. The **Asset Values** screen displays the predefined settings. You can change these values and create new ones. (New settings will appear in the drop-down list for all Computers.)

8. System Events

"System Events" include changes to the configuration of a Client Plug-in or the Server Plug-in. They also include errors that may occur during normal operation. Use this screen to set whether particular events are recorded and whether email notifications should be sent if they occur.


Don't forget to save your changes.

9. Security

N/A

10. Security Center

N/A

11. System

SMTP

Enter 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, enter the username and password credentials. Once you've entered the necessary information, use the **Test SMTP Settings** to test the settings.

Web service API

You can control much of the Server Plug-in's functionality via SOAP-invoked Web services. The WSDL can be found at the URL displayed in the panel on the screen. For assistance with the Server Plug-in's Web services API, please contact Trend Micro.

Prune

These settings define how long to keep log data on System and Firewall/IPS events. You should base your decisions regarding these settings 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. Do this through the **Advanced Settings** on the **Computer Properties** screen or the **Security Profile Properties** screen.
- 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 IPS Filters, the best practice is to log only dropped packets. Logging packet modifications may result in a lot of log entries.
- For IPS Filters, only include packet data (an option on the IPS Filter's **Properties** screen) 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 (Firewall, IPS, and System). **Counters** are data aggregated from the logs and are used to generate Reports and populate the Dashboard.

Export

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

WHOIS

The WHOIS lookup to be used when logging IPS and Firewall Events.

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. Once they incorporated into the Server Plug-in, they are pushed out to the Client Plug-ins immediately.

This screen lets you check for the latest updates and incorporate them into the Server Plug-in. It also lets you automate the process of retrieving updates and incorporating them into the Server Plug-in. For more information on applying and automating security Updates, see **How To... Apply Security Updates**.

Product License

The purpose of the product 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 of your license based on the Trend Micro activation servers

Expiry and # 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 for your license.

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

How To...

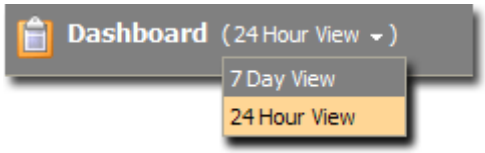
Customize the Dashboard

The Dashboard is the first screen that comes up after you log in to the 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.)

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 Computer Domains

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

Select Dashboard Widgets

Click the **Add to Dashboard...** button ( ) to bring up 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 on the **Dashboard** button to save, load, or delete a dashboard layout.

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 > Security 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 Security Updates...** button to open a new window displaying all downloaded updates. The listed updates will have a green check mark in the "Applied" column indicating if they have been applied to the Client Plug-ins.
3. Select the latest Security Update from the list and click "Apply…" 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 Security Update:

1. Select the check box next to "Automatically".
2. Select "Download" from the drop-down menu.
3. Enter a time of day to regularly check for updates.

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. Select the check box next to "Automatically"
2. Select "Download and Apply" from the drop-down menu
3. Enter a time of day to regularly check for updates, download, and apply them.

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

Configure Alerts

There are just over thirty conditions that raise Alerts in the Server Plug-in. Generally, Alerts exists to warn of system status anomalies like Computers going offline or IPS filters being out of date, although there are some alerts for the detection of fingerprinting scans and other security-related events. (For notifications of individual IPS and Firewall Events, consider setting up a Syslog server.) The list of possible alerts can be viewed by going to the **System > Alert Configuration** screen.

The actions precipitated by each alert can be configured by opening the **Properties** screen () for the alert. Alerts can be turned on or off; their severity can be switched between Warning and Critical; and their email settings can be changed (whether or not an email is sent out and under what conditions.)

There is also an option to enter a default email address to which all email alerts will be sent in addition to the administrator. This option is found on the **System > Settings > Notifications** screen.

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

Set Up Email Alerts

The Server Plug-in will send out an email message when it raises alerts. To enable the email system, you must give the 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 > Settings > System**.

Enter 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, enter 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 raise 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 **System > Alert Configuration**. This screen displays all alerts. The check mark next to the alert indicates whether the alert is "On" or not. If it is on, it means the alert will be raised if the corresponding situation arises, but it does not mean an email will be sent out. Double-click on 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" check boxes must be selected.

Back Up and Restore Intrusion Defense Firewall

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.

Intrusion Defense Firewall ships with two DOS Batch files (.BAT) that allow administrators to backup and restore the database using Microsoft SQL Server's BACKUP command.

These two DOS batch files are found in the Intrusion Defense Firewall root directory (typically `C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall`):

- IDFBackup.bat
- IDFRestore.bat

By default `IDFBackup.bat` will store backups in a Microsoft SQL Server backup file named `IDFBackup.bak`.

This backup file will be located in the Microsoft SQL Server's backup directory (typically `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\IDFBackup.bak`).
When restoring, `IDFRestore.bat` will attempt to restore from `IDFBackup.bak` found in the same Microsoft SQL Server backup directory.

Each time a backup is run, 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 run.

Modifying Backup and Restore options

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.

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

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

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

To change the directory and file from which backups will restored from, 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"
```

Setting up Scheduled Backups

To schedule regular backups, 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.

Restoring from Backup

To restore from the last backup, you will need to:

1. Stop the "Third Brigade Deep Security Manager" 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 "Third Brigade Deep Security Manager" service.

Note: If the location of the backup file has changed, you will need to edit `IDFRestore.bat` and change the backUpFile parameter. Please refer to the above Modifying Backup and Restore options section.

If the backup file has been moved to a different Computer and restored, you will need to update the Intrusion Defense Firewall URL Setting by executing the following `dsm_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.)

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

For example, to change the Computer name to **OfficeScan_Win2K**, you would execute:

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

Filter SSL Data Streams

The Server Plug-in supports IPS Filtering of SSL traffic. The SSL dialog allows the user to create SSL Configurations for a given credential-port pair on one or more interfaces. Credentials can be imported in **PKCS#12** or **PEM** format, and Windows Computers have the option of using **CryptoAPI** directly.

Configuring SSL Data Stream Filtering on a Computer

SSL Computer Configuration

Open the **Properties** screen of the Computer you wish to configure and click on the **SSL...** button to bring up the **SSL Computer Configurations** screen.

Click **New** to bring up the first page of the **SSL Computer Configuration** wizard.

SSL Configuration Wizard

Select Port(s)

Either enter the (comma-separated) ports you want this configuration to apply to, or select a Port List.


You will also have to change the port settings on the Computer's **Properties** screen. (See below.)

Select Interface(s)

Specify whether this configuration will apply to all interfaces on this Computer or just one.

IP Selection

Specify whether SSL Payload inspection should take place on all IP addresses for this Computer, or just one. (This feature can be used to set up multiple virtual Computers on a single machine.)

Specify Source of Credentials

Specify whether you will provide the credentials file yourself, or whether the credentials are already on the Computer.

Specify Type of Credentials

If you have chosen to provide the credentials now, enter their type, location, and pass phrase (if required). If you've indicated that the credentials are on the Computer, specify the type of credentials to look for.

Provide Credential Details

If you are using PEM or PKCS#12 credential formats stored on the Computer, identify the location of the credential file and the file's pass phrase (if required).

If you are using Windows CryptoAPI credentials, choose the credentials from the list of credentials found on the Computer.

Name and Describe this Configuration

Give a name to and provide a description of this SSL configuration. Look Over the Summary and Close the SSL Configuration Wizard. Read the summary of the configuration operation and click **Finish** to close the wizard.

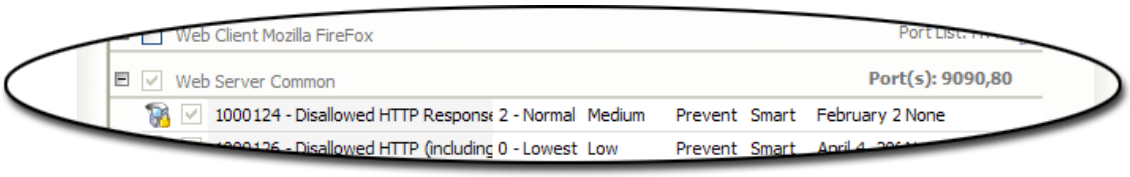
Change Port Settings on the Computer Properties Screen to Monitor SSL Port.

Finally, you need to make sure that the Client Plug-in is performing the appropriate IPS Filtering on the SSL-enabled port(s). Click the **IPS Filters** tab on the Computer's **Properties** screen to see the list of IPS Filters being applied on this Computer. Make sure the filters are being sorted by Application Type. Scroll down the list to find the Application Type(s) running on this Computer (in the example pictured here, "Web Server Common").

Right-click on the "Web Server Common" Application Type heading and choose "Application Type Properties (For This Computer)". This will bring up the **Application Type Properties** screen.

Instead of using the inherited "HTTP" Port List, we will override it to include the port we defined during the SSL Configuration setup (port 9090 in this case) as well as port 80. Enter ports 9090 and 80 as comma-separated values and click **OK** to close the dialog. (Since you have selected "Application Type Properties (For This Computer)", the changes you make will only be applied to this Computer. The "Web Server Common" Application Type will remain unchanged on other Computers.)

The IPS Filters list in the Computer's **Properties** screen will now refresh itself to show the changes. Note that the Port List for The "Web Server Common" Application Type on this Computer is now in **bold type**, indicating the default Port List has been overridden on this Computer:



This Computer is now configured for filtering SSL encrypted data streams.

Maximize Logging Efficiency

By default the 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. This can be done through the **Advanced Settings** on the **Computer Properties** screen or the **Security Profile Properties** screen.
- 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 IPS Filters the best practice is to log only dropped packets. Logging packet modifications may result in a lot of log entries.
- For IPS Filters, only include packet data (an option on the IPS Filter's **Properties** screen) when you are interested in examining the source of attacks. Otherwise leaving packet data inclusion on will result in much larger log sizes.

Configure Communications between the Server Plug-in and the Client Plug-in

Initiating 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 want to completely close off the Computer to communications initiated by any remote source, you may 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 **System > Settings** screen and click on 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.

On a Computer to which a particular Security Profile has been assigned

1. Go to the **Security Profiles** screen and double-click on the Security Profile whose communications settings you want to configure.
2. Click on the **Advanced...** button at the bottom of the **Security Profile Properties** screen to bring up the **Advanced Settings** window, and select the **Computer tab.**
3. In the "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 what ever setting was specified on the **System > Settings** screen. Selecting one of the other options will override the **System Settings** selection.
4. Click **OK** to close both windows and to apply the changes.

On an individual Computer

1. Go to the **Computers** screen and double-click on the Computer you want to configure.
2. Click the **Advanced...** button at the bottom of the **Computer** tab.
3. Select your choice from the drop-down list on the **Computer** tab .
4. As above, choose from one of the usual options or choose "Inherit". Choosing anything but inherit will override the system setting *and* the Security Profile settings.

Note that Client Plug-ins identify the Server Plug-in on the network by the Server Plug-in's hostname. Therefore the Server Plug-in's hostname **must** be in your local DNS if Client Plug-in-initiated or bi-directional communication is to work.

Configure Notifications

In addition to alert emails via SMTP and logging to the database, the Server Plug-in 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 IPS and Firewall Event information, and the Server Plug-in will send System Information. To configure the Syslog settings, go to **System > Settings > Notifications**:

Notice that there are two panels for configuring Event Notification: one for Firewall and IPS Events (from the Client Plug-ins), and one for System Events (from the Server Plug-in).

For information on configuring Syslog, see **How To... Set Up Syslog Integration**

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 ("snmp.mib") is located in `\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall\util`.

Scripts

If the Syslog and SNMP options do not meet your event notification requirements, it may be possible for Trend Micro to provide a solution using custom-written scripts. Please contact Trend Micro for more information.

Configure Port Scan Settings

Port scans can be initiated by right-clicking on an existing Computer on the **Computers** screen and choosing "Scan Computer for Open Ports".

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 (**Computer Properties > Advanced > Computer > Communication Direction**), 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. Enter 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 enter "100" on the first line "105" on the second, and "110-120" on the third.) Click **OK**.
3. Now go to **System > Settings > Scan** and click on the "Ports to Scan" drop-down menu. Your newly defined Port List will be one of the choices.

Protect Virtual Machines

Security of Networked Virtual Machines

Most virtual machines allow you to configure how the virtual machines connect to your network. The network options can allow for bridged networking, NAT networking or internal networking. The virtual server software provides internal virtual networks to enable the possibility of using a NAT network or an internal network. These three different network configurations require that security be handled differently.

Internal Network

Configuring a virtual machine to use the internal virtual network requires the least amount of security, as the virtual machine is not connected to the local network or the internet.

NAT and Bridged Networks

Allowing the virtual machine to have network access using NAT via the Computer, or direct access through bridging, creates a situation where multiple operating systems and services are now available from a single physical machine.

The operating systems on the virtual machines will contain the same flaws and require the same patches that would be applied had the operating system been applied to a real machine.

Should the Computer be compromised, the virtual machine is subject to risks that range from being compromised itself to being shut off, creating a permanent DoS attack.

Having the virtual machine compromised seems to be less dangerous, as it does not control the Computer and can be reset to a previous state (before it was infected). However restoring a virtual machine to a previous state only postpones the problem, as it merely removes the virus or malware. It does not deal with the issue of the vulnerability that allowed the attacker into the machine in the first place. In addition, the way that most of the virtual machines interact with the stack of the Computer can present a problem. Because the Computer has to have a way to send packets destined for the virtual machine to the virtual machine, the Computer stack and the virtual machine stack must interact. If the virtual machine is trying to send packets to the Computer, this interaction bypasses the stack in the same way packets being sent to 127.0.0.1 bypass the stack, presenting a possible way to bypass standard firewalls.

SSL for Multiple Virtual Computers

If you have multiple virtual Computers with multiple SSL certificates you can configure your Client Plug-in to filter the traffic based on the IP address of your virtual Computers. (See **How To... Filter SSL Data Streams**.) The SSL Configuration wizard will prompt you to specify whether the SSL configuration will apply to all IP addresses on the Computer or just one. For multiple virtual Computers, enter the IP address of the virtual Computer that you wish to have SSL filtering configured for. You can then repeat this to set up each of the virtual Computers with their appropriate certificates.

Protection with the Client Plug-in

The recommended security strategy for virtual machines that have access to the local network or internet through the Computer is to have the Client Plug-in installed on both the virtual machine and the Computer.

This configuration allows both the Computer and the virtual Computer to be protected from attacks originating from either the local network or the internet. This configuration also protects the Computer from attacks from the virtual machine should the virtual machine be compromised, and protects the virtual machine should the Computer be compromised.

Because traffic passing to the virtual machine must pass through the physical interface of the Computer, that traffic will pass through the Client Plug-in on the Computer first.

To allow services on the virtual machine to be accessible from the local network or the internet, the applicable ports must be opened in the Client Plug-ins of both the virtual machine and the Computer. To prevent the Computer from being open to attack, the packet filter rules configured in the Computer's Client Plug-in should allow traffic through to the required ports only when it is destined for the virtual machine's IP address. This allows the Computer to be protected even while the ports required by the virtual machine are accessible.

Set Up Syslog Integration

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 Server Plug-in does not affect default logging. That is, enabling syslog will not "turn off" the normal logging mechanisms.

Server Plug-in Settings

You can configure the Server Plug-in to instruct all managed Computers to send logs to the Syslog machine, 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 > Settings** screen and click on the **Notifications** tab. In the panel called "System Event Notification",

1. Select the "Forward System Events to a remote Computer (via Syslog) " check box,
2. specify the hostname or the IP address of the Syslog machine,
3. specify which UDP port to use (usually 514),
4. select which Syslog facility to use (Local4 from the RedHat 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 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 properties. Click the **Advanced** button to bring up the **Advanced** properties screen, and go to the **Notifications** tab. Like many other settings on a Client Plug-in, you can instruct it to inherit default settings, or override them. To instruct this Computer to ignore any inheritable default settings, select the "Forward Logs 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-ins send two types of logs to Syslog: Firewall Event Logs, and IPS Event Logs. Firewall Event Logs are prefixed with "dsa_mpf:" and IPS Event Logs are prefixed with "dsa_mpld:". The content of the log is a space-separated string 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 filter 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 filter 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 Information	The "DF" field is present if the 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.	DF 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 contain 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	RES=0x00 ACK RES=0x00 SYN ACK

	up in the two least significant bits of this field.	
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

IPS 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 filter 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 IPS Filter that caused the log. Space characters in the IPS Filter 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 IPS 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 IPS Filter definition. If the IPS Filter is an incoming filter the interface name follows IN=, and the OUT= field contains nothing. The opposite is true for outgoing IPS Filters. 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 contain 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 IPS Filter rule. It contains one of the strings "Block", "Reset", "Insert", "Delete", "Replace", "Log". If the rule or the IPS 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 IPS 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 IPS Filter 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	FLAGS=0 FLAGS=9

	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`	

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 Server Plug-in has been configured to send the data using Trend Micro's format (DSM) 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.

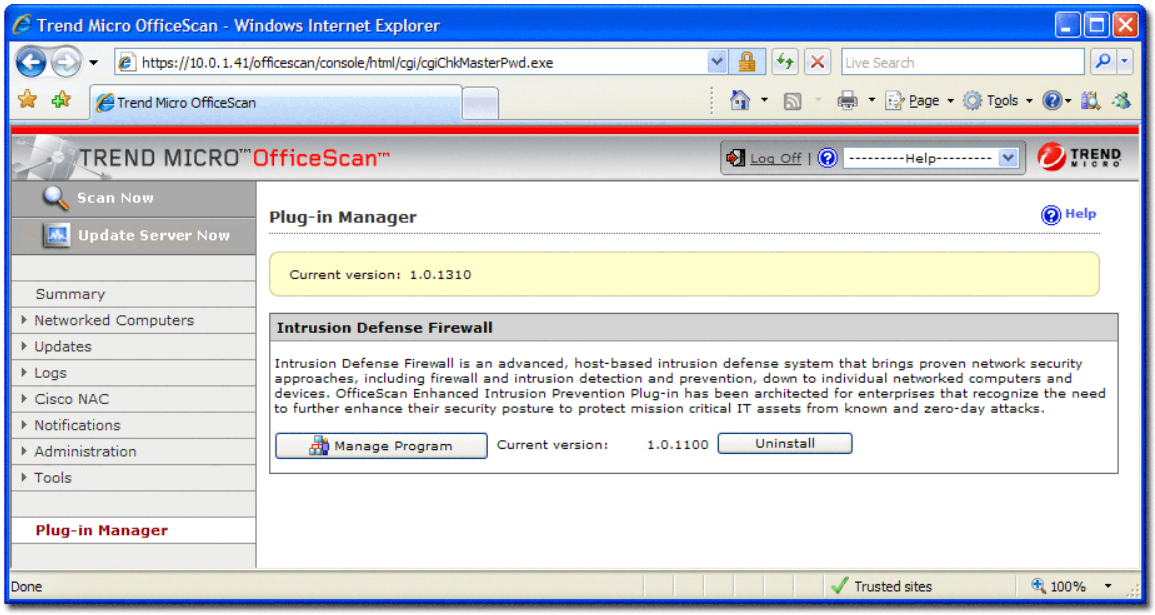
Name	Description	Examples
Time/Date and DSM Node	The time and date the event occurred and the Server Plug-in node on which it occurred.	Jun 8 11:00:08 mckinley-lab DSM Jun 8 11:00:38 mckinley-lab CEF
EVENTNUMBER	Numeric ID of the Event.	701 (The list of System Events elsewhere in this reference section includes the Event number.)
TITLE	Title of the Event.	Administrator signed in. Alert ended. IPS Filter updated.
TARGET	The target (if applicable) of the Event.	This can be a username, a hostname, an IPS filter, etc. depending on the nature of the event.
ACTIONBY	Which entity initiated the Event.	This will be either "System" or the username of an administrator.
DESCRIPTION	A textual description of the details of the Event.	Alert: Client Plug-in Offline Severity: Critical Administrator 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 DSM: 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: Agen

Uninstall the Intrusion Defense Firewall Server Plug-in

From the OfficeScan Plug-In Manager, select Intrusion Defense Firewall and click **Uninstall**.

Note: The Intrusion Defense Firewall Plug-in cannot be uninstalled from the Control Panel, Add or Remove Programs screen.



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**, enter the following:

   ```
   rundll32 "C:\Program Files\Trend Micro\IDF Client\IdfClientAgent.dll",Uninstall
   ```

   For **64 bit Windows**, enter the following:

   ```
   rundll32 "C:\Program Files (x86)\Trend Micro\IDF Client\IdfClientAgent.dll",Uninstall
   ```

Migrate Managed Computers to a New Intrusion Defense Firewall 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 on 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 `dsm_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.)

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

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

   ```
   dsm_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 Intrusion Defense Firewall 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 on 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. Make sure the Computer is listed in the **Networked Computers** section of the new OfficeScan server by using the "Move Client" feature of the OfficeScan management console. (Computers listed in the OfficeScan server are automatically listed in the **Computers** screen of the Intrusion Defense Firewall Server Plug-in.)
3. Right-click on the Computer in the **Computers** screen of the new Intrusion Defense Firewall 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.

Reference

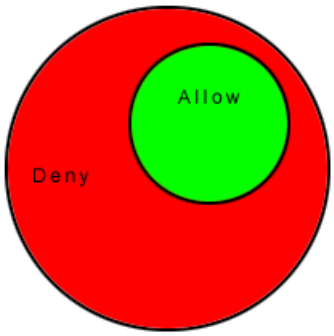
About Firewall Rules

Firewall Rules have both a filter action and a filter 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, Intrusion Defense Firewall firewall rules are run in a deterministic order based on a the filter action and the filter priority, which is independent of the order in which they are defined or assigned.

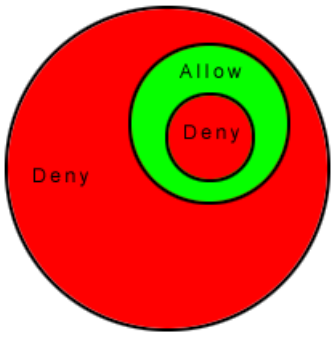
Filter Action

Each filter can have one of four filter actions.

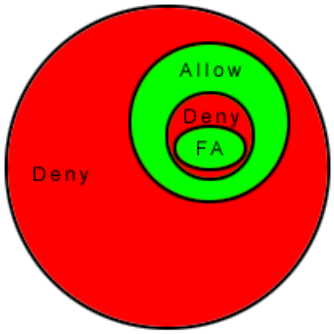
1. **Bypass:** if a packet matches a **bypass** rule, it is passed through both the firewall *and the IPS filters* regardless of any other filters (at the same priority level).
2. **Force Allow:** if a packet matches a **force allow** rule it is passed regardless of any other filters (at the same priority 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 filter will deny everything but the allow



A DENY filter can be installed over an ALLOW to block certain kinds of traffic



The FORCE ALLOW filter can be placed over the denied traffic to allow certain exceptions to go through

Filter Priority

Filter 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** filters. Filters are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the filters are processed in order based on the filter action (force allow, deny, allow, log only).

The priority context allows an administrator 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.

Filter Actions of type **allow** run only at priority 0 while filter actions of type **log only** run only at priority 4.

Putting Filter Action and Priority together

Filters are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level, the filters are processed in order based on the filter action. The order in which filters 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** filter and a **deny** filter at the same priority the **force allow** filter takes precedence over the **deny** filter and therefore traffic matching the **force allow** filter will be permitted.

Stateful Filtering

When stateful filtering 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 filters.
- 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 filters.

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** filters to describe allowed traffic and **deny** filters 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** filters 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** filters 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** filter with the protocol set to "TCP + UDP" and select the **Not** check box and the **Syn** check box 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 filtering options enabled in step 1, this filter allows a user on this machine 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** filter with the protocol set to "ICMP" and select the **Any Flags** check box. This means that a user on this machine can ping other workstations and receive a reply but other users will not be able to ping this machine.
4. Add a Firewall Rule to allow incoming TCP traffic to port 80 and 443 with the **Syn** check box checked in the **Specific Flags** section. This means that external users can access a Web server on this machine.

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 machine all other incoming traffic is denied.

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

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

We may, however, want to refine this policy further to allow incoming traffic from the mail server that 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 machine 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** filters 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** filter 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** filter must be used to allow unsolicited ICMP traffic. For example if you wish to allow outside ping requests a **force allow** filter 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.

Inheritance and Overrides

An object can have certain of its properties overridden at lower levels. For example, let's say we have a Firewall Rule called FirewallRuleAlpha and among its properties is the fact that it operates on incoming port 12345 because the application we have designed the Firewall Rule for usually operates on that port.

However, let's say we have an unusual Computer running that application which in this one instance operates on port 44444. Instead of writing a new Firewall Rule for this Computer, we can simply open the unusual Computer's **Properties** screen, click on the **Firewall Rules** tab, find the Firewall Rule in the list, right-click on it and select "Firewall Rule Properties (for this Computer)".

On the **Properties** window for this Firewall Rule, you will now see that many of the properties have a check box called "Inherit" next to them. This means that the setting is inherited from the level above it in the scoping hierarchy (either from a Security Profile or from the Global list). Unchecking "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 **Properties** window and make the same changes. (You could then of course override those again on a particular Computer.)

The 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 undergo IPS filtering
2. Unlike Force Allow, Bypass will not automatically allow the responses on a TCP connection when Stateful Filtering 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)

Using Bypass when Stateful Filtering is On

If you plan to use a Bypass Rule to skip IPS filtering 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 filter 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:

- **Filter Action:** whether the Client Plug-in will allow packets matching the filter's criteria through regardless of any other filters that would block them ("force allow"); block packets matching the filter's criteria ("deny"); exclusively allow only packets matching the filter's criteria and block all others ("Allow"); or log packets matching the filter's criteria and let them pass ("log only"). Within a priority level (see next item), filters 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 filters 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. Enter a name and description for your new Firewall Rule.
3. Select a filter action, priority, and packet direction from the drop-down lists.
4. Define the criteria that this filter will look for in the packets' control information. (Note that as well as inclusive criteria, you can define exclusive criteria by checking the "Not" check box at the right of each option.)
5. Click on the **Options** tab and select whether you want the filter to only be active during certain scheduled periods. Specify whether you want this filter to raise 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 group 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 on the Security Profile to which you want to assign a new filter. This will open the Profile's **Properties** screen.
2. Click on the **Firewall Rules** tab.
3. Find your new Firewall Rule in the list and put a check in its check box.
4. Click OK.

If the "Update all affected Computers immediately when I edit any element of the Intrusion Defense Firewall" option is enabled on the Computers tab, on the **System > Settings** screen, all Computers to which that Security Profile has been assigned will be updated with the new filter.

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

1. Go to the **Computers** screen and double click on the Computer to which you want to assign the new filter.
2. Click on the **Firewall Rules** tab.
3. Find your new Firewall Rule in the list.
4. Select the check box for the Firewall Rule and click the **OK** button.

As before, if the "Update all affected Computers immediately when I edit any element of the Intrusion Defense Firewall" option is enabled on the Computers tab, on the **System > Settings** screen, all Computers to which that Security Profile has been assigned will be updated with the new filter.

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.

Firewall Rule Sequence

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

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.

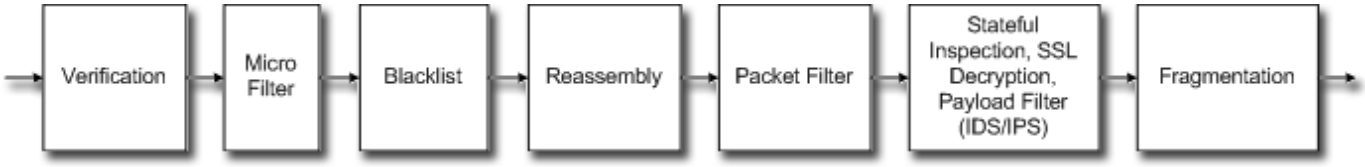
Log-only rules will only generate a log entry if the packet in question is not subsequently stopped by either:

- 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 of course generate an entry.

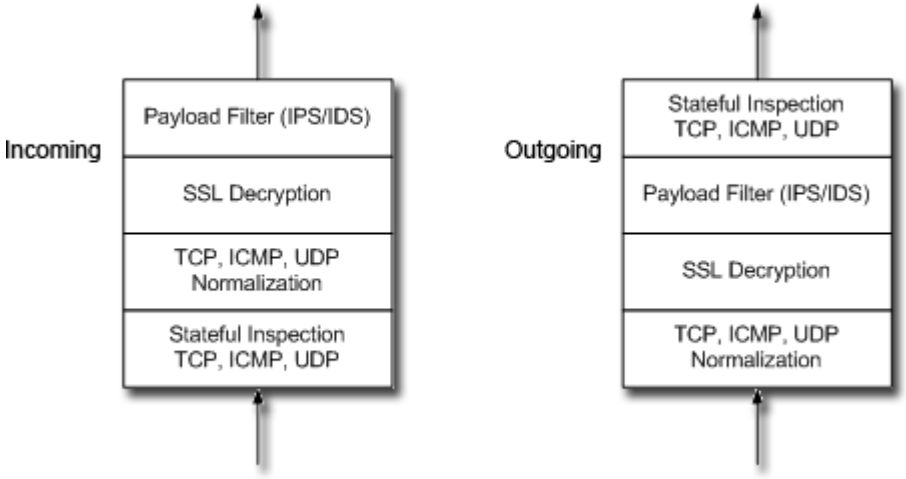
Packet Processing Sequence

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
- **Reassembly:** Reassembles fragmented packets for later use by the Payload Filter
- **Packet Filter:** All firewall rules not processed by the Micro Filter are processed by the Packet Filter
- **Stateful, SSL, and Payload Filter (IDS/IPS):** 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:** If required and configured this feature decrypts the SSL protected traffic for analysis by the Payload Filter
    - **Payload Filter (IDS/IPS):** Deep packet inspection engine that does pattern matching and custom code operations
- **Fragmentation:** Fragments packets that are larger than the MTU

Although incoming and outgoing traffic flow through the pipeline in the same order, the internal sub-order inside the Stateful Inspection, SSL, and Payload Filter (IDS/IPS) module depends on traffic direction:



Required Ports

For the Server Plug-in and the Client Plug-ins to function as expected, a number of ports must be accessible. 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: Server Plug-in
- Connected To: Client Plug-in
- Proxy: No
- Configuration: This port is not configurable

Port: 4119 (default)

- Use: Access to Server Plug-in remotely
- Protocol: TCP
- Initiated By: Web Browser
- Connected To: Server Plug-in
- Proxy: No
- Configuration: This port is not configurable

Port: 4120 (default)

- Use: Client Plug-in to Server Plug-in communication
- Protocol: TCP
- Initiated By: Client Plug-in
- Connected To: Server Plug-in
- Proxy: No
- Configuration: This port is not configurable

Port: 514 (default)

- Use: Syslog
- Protocol: UDP
- Initiated By: Client Plug-in
- Connected To: Syslog facility
- Proxy: No
- Configuration: This port can be configured in the **System > Settings > Notifications** section

Port: 25 (default)

- Use: E-mail Alerts
- Protocol: TCP

- Initiated By: Server Plug-in
- Connected To: Specified SMTP server
- Proxy: No
- Configuration: This port is not configurable

Port: Randomly selected

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

Firewall Events

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 invalid (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.

IPS Events

Base 64 Decoding Error

Packet content that was expected to be encoded in Base64 format was not encoded correctly.

Computer Attempted to Rollback

A Computer attempted to roll back to an earlier version of the SSL protocol than that which was specified in the ComputerHello message.

Corrupted Deflate/GZIP Content

Invalid Deflate/GZIP content.

Deflate/GZIP Checksum Error

Checksum Error detected in Deflate/GZIP content.

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 ComputerKeyExchange 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 filter 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 character.

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, the product returns an error at this limit and drops the connection because it usually indicates a garbage or evasive packet that the product does not need to process.

Maximum Edits Exceeded

The maximum number of edits (32) in a single region of a packet was exceeded.

Memory Allocation Error

An internal memory allocation error occurred.

Out Of Bounds

The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (maximum 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (maximum 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

The IPS engine has experienced a Runtime Error.

Search Limit Reached

A protocol-decoding filter defined a limit for a search or PDU object but the object was not found before the limit was reached.

Stack Depth

A filter programming error attempted to cause recursion or use too many nested procedure calls.

Type Nesting Too Deep

A protocol-decoding filter 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 Computer attempted to negotiate an SSL V2 session.

URI Path Depth Exceeded

Too many "/" separators, maximum 100 path depth.

URI Path Length Too Long

Path length is greater than 512 characters.

Client Plug-in Events

The following table lists all possible Client Plug-in Events.

Client Plug-in Events are displayed within a System Event on the System Events screen. For example, double clicking on the "Client Plug-in Events Retrieved" System Event will bring up 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 Filter Priority
2017	Invalid Schedule Length
2018	Invalid Schedule String
2019	Unrecognized IP Format
2020	Object Not Found
2021	Object Not Found
2022	Invalid Filter Assignment
2085	IPS Filter Rules 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

System Events

The following table lists all possible System Events.

Number	Event
0	Unknown Error
100	the Server Plug-in Started
101	License Changed
102	Trend Micro 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	IPS Events Exported
113	Scheduled Security Update Download Failed
114	Scheduled Security Update Downloaded
115	Security Update Downloaded
116	Security Update Applied
117	the Server Plug-in Shutdown
120	Heartbeat Server Failed
121	Scheduler Failed
130	Credentials Generated
131	Credential Generation Failed
140	Discover Computers
141	Discover Computers Failed
142	Discover Computers Requested
143	Discover Computers Canceled
150	System Settings Saved
151	Client Plug-in Software Added
152	Client Plug-in Software Deleted
153	Client Plug-in Software Updated
155	Client Plug-in Platforms Changed
160	Authentication Failed
180	Alert Type Updated
190	Alert Started

191	Alert Changed
192	Alert Ended
197	Alert Emails Sent
198	Alert Emails Failed
199	Alert Server Plug-in Failed
250	Computer Created
251	Computer Deleted
252	Computer Updated
253	Security Profile Assigned to Computer
254	Computer Moved
255	Computer Activate Requested
256	Computer Update Now Requested
257	Computer Locked
258	Computer Unlocked
259	Computer 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
270	Computer Creation Failed
275	Duplicate Computer
280	Computers Exported
281	Computers Imported
286	Computer Log Exported
290	Computer Group Added
291	Computer Group Removed
292	Computer Group Renamed
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
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	Administrator Synchronization
326	Administrator Synchronization Finished
327	Administrator Synchronization Failed
328	Administrator Synchronization Requested
329	Administrator 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	IPS Filter Created
471	IPS Filter Deleted
472	IPS Filter Updated
473	IPS Filter Exported
474	IPS Filter 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 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	Administrator Signed In
601	Administrator Signed Out
602	Administrator Timed Out
603	Administrator Locked Out
604	Administrator Unlocked
608	Administrator Session Validation Failed
609	Administrator Made Invalid Request
610	Administrator Session Validated
611	Administrator Viewed Firewall Event
613	Administrator Viewed IPS Event
615	Administrator Viewed System Event
650	Administrator Created
651	Administrator Deleted

652	Administrator Updated
653	Administrator Password Set
660	Administrator Role Created
661	Administrator Role Deleted
662	Administrator Role Updated
663	Administrator Roles Imported
664	Administrator 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
720	Client Plug-in Updated
721	Client Plug-in Update Failed
722	Get Interfaces Failed
723	Get Interfaces Failure Resolved
724	Insufficient Disk Space
726	Get Client Plug-in Events Failed
727	Get Client Plug-in Events Failure Resolved
728	Get Firewall/IPS Events Failed
729	Get Firewall/IPS 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	Get Status Failure Resolved
737	Get Status Failed
738	IPS Filter Engine Offline
739	IPS Filter Engine Back Online
740	Client Plug-in Error
750	Last Automatic Retry

760	Client Plug-in Version Compatibility Resolved
761	Client Plug-in Upgrade Recommended
762	Client Plug-in Upgrade Required
763	Incompatible Client Plug-in Version
764	Client Plug-in Upgrade Recommended (Incompatible IPS Filter(s))
765	Computer Reboot Required
770	Client Plug-in Heartbeat Rejected
771	Contact By Unknown Computer
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 FIN Scan
854	Reconnaissance detected: TCP Xmas Scan
900	the Server Plug-in Audit Started
901	the Server Plug-in Audit Shutdown
902	the Server Plug-in Installed
970	Command Line Utility Started
978	Command Line Utility Failed
979	Command Line Utility Shutdown
980	System Information Exported
998	System Event Notification Error
999	Internal Software Error

Troubleshooting

General Troubleshooting

Sympton: OfficeScan Server UI cannot be accessed externally after installing Intrusion Defense Firewall Client Plug-in on the server computer
Solution: Ensure that the **OfficeScan Server** firewall rule is assigned to the server computer, or that the server computer is using the **OfficeScan Server Profile** security Profile.
Solution: Open Computer Properties for the server computer select the **OfficeScan Server Profile** security Profile, or click on the Firewall Rules tab, and check the **OfficeScan Server** firewall rule.

Sympton: Intrusion Defense Firewall cannot be accessed when clicking on the "Manage Program" button in the OfficeScan Plug-in Manager screen after installing Intrusion Defense Firewall Client Plug-in on the server computer
Solution: Ensure that the **Intrusion Defense Firewall Server Plug-in** firewall rule is assigned to the server computer, or that the server computer is using the **OfficeScan Server Profile** security Profile.
Solution: Open Computer Properties for the server computer select the **OfficeScan Server Profile** security Profile, or click on the Firewall Rules tab, and check the **Intrusion Defense Firewall Server Plug-in** firewall rule.

Client Plug-in Installation Troubleshooting

Symptom: The client plug-in fails to install
Solution: Open Computer Properties for the computer that failed to install the client plug-in. Click on the hyperlink for the error which opens the event viewer. This viewer will provide more information as to the source of the failure.
Suggestions for possible error conditions:

- For the error: "Client Plug-in Software Deployment Failed"
    - If the event description is "Client plug-in deployment failed to complete before the maximum allowed time. Please re-try the deployment." Please see the next section in troubleshooting.
    - If the event description is "Client plug-in installation failed (reason: ? state: ?, last error code: ?)" check the reason for more information. Common reasons include:
        - Start Item Failed: The plug-in failed to initiate the installation. Please contact support
        - Prerequisite Check Failed: The plug-in found one or more missing prerequisites. Please ensure that you have MSXML 3 or higher installed and that you meet the minimum requirements
        - Copy Files Failed: The plug-in was unable to access the file system. Please contact support
        - Open Package Failed: The plug-in was unable to open the installer. Please contact support
        - Install Failed: The plug-in had a general install failure. Please note that the file system must be NTFS. If the file system is NTFS Please contact support
        - AOS Registration Failed: The plug-in was unable to register with the client plug-in manager. Please contact support
        - Unsupported Platform : Ensure that you are running one of the supported client platforms
- For the error: "Unable to activate client plug-in" there are several possible issues:
    - Unable to connect: Please ensure you have connectivity to the client plug-in and that the server can reach port 4118 on the client computer. Proxy communication between the server and client is not supported at this time. If the activation failure was caused by a disruption of communication please try to re-activate by using Actions > Activate/Reactivate Client Plug-in
    - Incorrect IP: Check the IP used by the Intrusion Defense Firewall server by opening Computer Properties and looking at the last IP used beside the host name. If this value is incorrect please wait 60 seconds and re-try the activation (there is a 60 second cache on the DHCP)

Symptom: The client plug-in remains in the deploying state
Solution: By default initiated deployments will wait for a result for up to 3 hours. When the client plug-in takes more than a few minutes to install it is likely:

- Offline: Ensure the computer is on and accessible via the network
- Considered offline by OfficeScan: Check the Networked Computers > Client Management section in OfficeScan to see if the host is in an online or offline state. If the computer is listed as offline it has likely not received the command to initiate the plug-in installation. The server will automatically retry every 15 minutes for 3 hours. To return the computer to the online state try using the Networked Computers > Connection Verification tool. Note that if you are "Re-deploying" the client plug-in, and you have unselected the **OfficeScan Client (Incoming) – Port XXXXX and OfficeScan Client (Outgoing) – Port XXXXX** firewall rules, this will prevent the deployment from being initiated. These two rules must be assigned in order for installs to occur.
- Installed but unable to report back to the server the success/failure status: After installation the client plug-in relies on a TCP channel back to OfficeScan server. It is possible an intermediate firewall or network issues can disrupt the communication. Please see the Client Plug-in Communication troubleshooting section.

Once the 3 hours have passed the computer will show an error state that the plug-in installation has failed. You may either:

- Retry the client plug-in installation: Right click on the host and choose Actions > Deploy Client Plug-in(s)
- Attempt to activate the plug-in: Right click on the host and choose Actions > Activate/Reactivate Client Plug-in

If the above does not resolve the solution please contact support.

Client Plug-in Removal Troubleshooting

Symptom: The client plug-in fails to remove
Solution: Open Computer Properties for the computer that failed to remove the client plug-in. Click on the hyperlink for the error which opens the event viewer. This viewer will provide more information as to the source of the failure.
Suggestions for possible error conditions:

- For the error: "Client Plug-in Software Removal Failed"
    - If the event description is "Client plug-in removal failed to complete before the maximum allowed time." Please see the next section in troubleshooting.
    - If the event description is "Client plug-in removal failed (reason: ? state: ?, last error code: ?)" check the reason for more information. Common reasons include:
        - Open Package Failed: The plug-in was unable to open the uninstaller. Please contact support
        - AOS Unregistration Failed: The plug-in was unable to unregister from the client plug-in manager. Please contact support
        - Uninstall Failed: The plug-in was unable to uninstall. Please contact support

Symptom: The client plug-in remains in the removing state
Solution: By default initiated removals will wait for a result for up to 3 hours. When the client plug-in takes more than a few minutes to remove it is likely:

- Offline: Ensure the computer is on and accessible via the network
- Considered offline by OfficeScan: Check the Networked Computers > Client Management section in OfficeScan to see if the host is in an online or offline state. If the computer is listed as offline it has likely not received the command to initiate the plug-in installation. The server will automatically retry every 15 minutes for 3 hours. To return the computer to the online state try using the Networked Computers > Connection Verification tool. Note that if you have unselected the **OfficeScan Client (Incoming) – Port XXXXX** and **OfficeScan Client (Outgoing) – Port XXXXX** firewall rules on the computer properties screen, this will prevent the uninstall from being initiated. These two rules must be assigned in order for uninstalls to occur.
- Installed but unable to report back to the server the success/failure status: After removal the client plug-in relies on a TCP channel back to OfficeScan server. It is possible an intermediate firewall or network issues can disrupt the communication. Please see the Client Plug-in Communication troubleshooting section.

Once the 3 hours have passed the computer will show an error state that the plug-in installation has failed. The computer should be checked to see if the client plug-in is still installed. If it is still installed a second attempt can be initiated.

If remote removal is not possible local removal can be performed using the following steps:

1. Open a command prompt window (Start > Run > cmd.exe)
2. For 32 bit Windows, enter the following:
   `rundll32 "C:\Program Files\Trend Micro\IDF Client\IdfClientAgent.dll",Uninstall`
   For 64 bit Windows, enter the following:
   `rundll32 "C:\Program Files (x86)\Trend Micro\IDF Client\IdfClientAgent.dll",Uninstall`

Please note that "Uninstall" at the end of the command is case sensitive.

Client Plug-in Communication Troubleshooting

Symptom: The client plug-in is incorrectly reported as being in an Offline state, and/or Intrusion Defense Firewall Server cannot communicate with the Client Plug-in.
Solution: Ensure that the Intrusion Defense Firewall Client Plug-in is installed on the client computer, and that communication between the Client Plug-in and Intrusion Defense Firewall Server is possible.
Please ensure that:

- Within the Intrusion Defense Firewall Server Computers screen, that the client computer is not in a **New** state. If it is, then you will need to deploy the Client Plug-in: Right click on the host and choose Actions > Deploy Client Plug-in(s)

- The client computer can successfully resolve the hostname of the Intrusion Defense Server computer to the correct IP. This can be verified by using the Windows **ping** command from the command-line: `ping <server computer name>.` If the hostname is resolved to the incorrect IP, you can attempt to clear the DNS cache on the client computer by executing the following from the command-line: `ipconfig /flushdns` Next attempt to ping the server again. If the incorrect IP is again displayed, you will need to contact your IT Department or System Administrator.

- The Intrusion Defense Firewall Server computer can successfully resolve the hostname of the client computer to the correct IP. This can be verified by using the Windows **ping** command from the command-line: `ping <client computer name>.` If the hostname is resolved to the incorrect IP, you can attempt to clear the DNS cache on the server computer by executing the following from the command-line: `ipconfig /flushdns` Next attempt to ping the client computer again. If the incorrect IP is again displayed, you will need to contact your IT Department or System Administrator.

- A proxy is not being used for communication between the Intrusion Defense Firewall Server and the Client Plug-in. Communication via a proxy is not supported.

- On the Client Plug-in computer, port 4118 is open and can be accessed externally. This can be verified by attempting to telnet to that computer/port from the server computer using the Windows **telnet** command from the command-line: `telnet <server computer name> 4118` If a telnet session cannot be opened, then the following will need to be verified:

    - The server computer that is attempting to telnet to the client plug-in does not have a firewall enabled that is blocking outgoing telnet sessions. Please consult the firewall documentation in order to allow outgoing TCP/telnet communication.

    - The client plug-in computer does not have a firewall enabled that is blocking incoming TCP connections to port 4118. Please consult the firewall documentation in order to allow incoming TCP communication on port 4118.

- On the Intrusion Defense Firewall server computer, port 4120 is open and can be accessed externally. This can be verified by attempting to telnet to that computer/port from another computer using the Windows **telnet** command from the command-line: `telnet <server computer name> 4120` If a telnet session cannot be opened, then the following will need to be verified:

    - Ensure that the **Intrusion Defense Firewall Server Plug-in** firewall rule is assigned to the server computer, or that the server computer is using the **OfficeScan Server Profile** security Profile. Open Computer Properties for the server computer select the **OfficeScan Server Profile** security Profile, or click on the Firewall Rules tab, and check the **Intrusion Defense Firewall Server Plug-in** firewall rule.

    - The computer that is attempting to telnet to the server does not have a firewall enabled that is blocking outgoing telnet sessions. Please consult the firewall documentation in order to allow outgoing TCP/telnet communication.

- The server computer does not have another firewall enabled that is blocking incoming TCP connections to port 4120. Please consult the firewall documentation in order to allow incoming TCP communication on port 4120.

Trend Micro Control Manager Troubleshooting

Sympton: When accessing Intrusion Defense Firewall server via the Trend Micro Control Manager on Windows 2003 using Internet Explorer 6, an error is displayed stating that the session could not be validated.
Solution: Within Internet Explorer, go to **Tools > Internet Options...** and click on the Security tab. Click on the **Local Intranet** icon, and then click the "Sites..." button. Add the following URL to the Web sites list:

https://<hostname>:4119

where the **<hostname>** is the computer that is running OfficeScan Server.

Server Plug-in Installation Troubleshooting

Error Message: "Unable to proceed. The Trend Micro Plug-in Manager must be version 1.0.1332 or greater."
Solution: Please check the version of Trend Micro Plug-in Manager and contact support if you are unable to download and install version 1.0.1332 or higher. The Plug-in Manager must be upgraded before the Intrusion Defense Firewall is installed.

Error Message: "Unable to proceed. A minimum of 1500 MB of free disk space is required and only ? MB is available."
Solution: Free additional disk space and re-try the installation. The disk space must be available on the same drive that OfficeScan Server is installed on.

Error Message: "Windows Installer Version 3.1 or higher is required."
Solution: Run Windows Update and ensure you have the latest version of Windows Installer.

Error Message: "Microsoft Data Access Components (MDAC). Version 2.81 or higher is required."
Solution: Download and Install MDAC from Microsoft using the following location: http://www.microsoft.com/downloads/details.aspx?familyid=78CAC895-EFC2-4F8E-A9E0-3A1AFBD5922E&displaylang=en (MDAC is not installed or updated during Windows Update)

Error Message: "Microsoft .NET Framework. Version 2.0 or higher is required."
Solution: Download and Install Microsoft .NET 2.0 using Windows Update or from the following location: http://www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en

Error Message: "Unable to proceed. The system directory could not be located."
Solution: Please contact support. They will assist you in collecting a log that will be used to diagnose the problem.

Error Message: "Unable to write to the add-on registry key '?'. Please check the registry permissions before trying again."
Solution: Check the permissions of the Plug-in Manager service and make sure it has the privileges required to write to the registry.

Error Message: "SQL installation failed. Check the logs in C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files"
Solution: Please ensure your system meets the Hardware and Software requirements for SQL Server Express 2005: http://msdn2.microsoft.com/en-us/library/ms143680.aspx
If your system meets the requirements please consult the logs referred to in the error message. If the SQLSetup?_?_Core(Local).log file contains an error similar to:

"C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0004_D-A-13_.NET Framework 2.0.log" to cab file : "C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\SqlSetup0004.cab" Error Code : 2"

re-install Microsoft .NET Framework 2.0. The .NET installation is likely corrupt. If that does not remedy the situation please contact support.

For other SQL Errors please contact support and send them the log files in the directory referred to in the error message.

Error Message: "Installation of the Intrusion Defense Firewall failed. Check the logs in ? and ?"

Solution: A general unexpected error has occurred. Please consult the logs referred to in the error message and contact support if required.

It is possible that even though Intrusion Defense Firewall failed to install, the SQL Server Express 2005 installation completed successfully and is still installed on your system. Subsequent attempts to install Intrusion Defense Firewall will use this first instance SQL Server Express. If you do not plan to install Intrusion Defense Firewall again and would like to remove this instance of SQL, manually uninstall the database instance by executing the following command:

"C:\Program Files\Trend Micro\OfficeScan\PCCSRC\Admin\Utility\SQL\sql.exe" /qn REMOVE=SQL_Engine INSTANCENAME=IDF

After the database has been removed, verify that the following directory either does not exist or that the IDF.mdf file has been removed (If needed delete IDF.mdf and IDF_log.LDF) located in:

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data

Also ensure that the following directory has been removed (delete it if needed):

C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall