HP Sygate Security Agent 4.0
User Guide

Documentation Build 1004
Published: May 1, 2005

Copyright Information

Table of Contents

List of Tables

List of Figures

Preface

This document, the *HP Sygate Security Agent User Guide*, describes how to distribute, install, and use the HP Sygate Standalone Agent (the Agent).

For late-breaking news about known problems with this release, refer to the `Readme.txt` file that is included with this software.

Related Documentation

- *HP Sygate Security Agent User Guide* (online Help)—The online Help is a subset of information in this document. Click **Start | All Programs | Sygate | HP Sygate Security Agent**. The Agent starts and displays the user interface. You can then choose **Help | Help** topics... from the menu bar, click the **Help** button, or press **F1**. However, the Help may not have been included with the Agent.
- *HP Sygate Policy Editor User Guide* (online Help)—Describes how to modify a security policy for the HP Sygate Security Agent using the HP Sygate Policy Editor. You can access the *User Guide* after you install the Policy Editor. On the **Start** menu, click **All Programs | Sygate | Policy Editor Help**.

Intended Audience

This documentation is written for system administrators and end users of the Agent software.

This documentation assumes that the user is familiar with the basic functioning of Windows operating systems and standard Windows items, such as buttons, menus, toolbars, windows, and so forth. Furthermore, this guide assumes that the user has an Internet connection, whether through a local area network, DSL connection, dial-up modem, wireless access point, or other connection method.

Technical Support

HP provides a variety of service and support programs.

To contact HP:

1. Locate the www.hp.com/support web site.
2. From the drop-down menu, select the country and language and click the double arrow.
3. On the **Support & Drivers** page, under **Or Select a product category**, click **Desktops & Workstations**.
4. Click **Thin Clients** and then the specific product.

   Note: You can also click the **Contact HP** link for additional contact and resources links.

Chapter 1. Overview of the Agent

The HP Sygate Security Agent (the Agent) is security software that is installed on embedded devices, such as ATMs and thin clients, that run the Windows XP Embedded operating system. Once installed, the Agent provides a customizable firewall that protects the device from intrusion and misuse, whether malicious or unintentional. It detects and identifies known Trojans, port scans, and other common attacks, and in response, selectively allows or blocks *traffic*, or various networking services, applications, ports, and components.

The Agent uses a customizable *security policy*, which includes *security rules* and *security settings*, to protect an individual device from network traffic that can cause harm. The Agent uses security rules to determine whether your device either blocks or allows an incoming or outgoing application or service from gaining access through your network connection. The Agent uses security settings to detect and identify common attacks, send e-mail messages after an attack, display customizable pop-up messages, and accomplish other related security tasks.

Modifying the Security Policy

The security policy that the Agent uses to protect the embedded device is stored in the *policy file*. You can modify the policy file, adding new rules and changing security settings.

If you are a system administrator, you can modify the security policy on your system and then deploy the settings in the policy file to each device where the Agent immediately applies them. To modify the security policy, you use the Policy Editor.

Using the Policy Editor

The Policy Editor is a separate tool from the Agent that you install on a separate system.

To install the Policy Editor:

1. From the Sygate FTP site, download the Policy Editor installer package, `PolicyEditorInstaller.exe`, to the image-building system.
2. Follow the instructions when prompted for your agreement to the license agreement, location of the software on your hard drive, and so on.

When you install Policy Editor, the default policy file is automatically installed with it. When you open the Policy Editor, the default policy file's advanced rules and options appear.

To open the Policy Editor:

- On the image-building system, click **Start | All Programs | Sygate | HP Sygate Policy Editor**.

For more information on using the Policy Editor:

- On the image-building system, click **Start | All Programs | Sygate | Policy Editor Help**.

Chapter 2. Getting Around

This chapter describes the tools that you use in getting around in the Agent.

Starting the Agent

The Agent is designed to start automatically when you turn on your device, protecting you immediately. To configure your Agent or review logs of potential attacks on your Agent, you open the Agent first.

You can open the Agent in two ways:

- **System tray icon**—Double-click the icon  on the right side of the taskbar, or right-click it and click **HP Sygate Security Agent**.
- **Start menu**—Click **Start | All Programs | Sygate | HP Sygate Security Agent**.

Any method opens the *main console*, or the main screen that is the control center for the Agent.

Option Alert: You can only open the Agent if you have logged on using an Administrator account. Users with a User account only see the system tray icon on the taskbar, although the Agent is still protecting the device.

Navigating the Main Console

Once you open the Agent, you see the main console. The main console provides real-time network traffic updates, online status, and links to logs, Help files, and access to various rules and options.

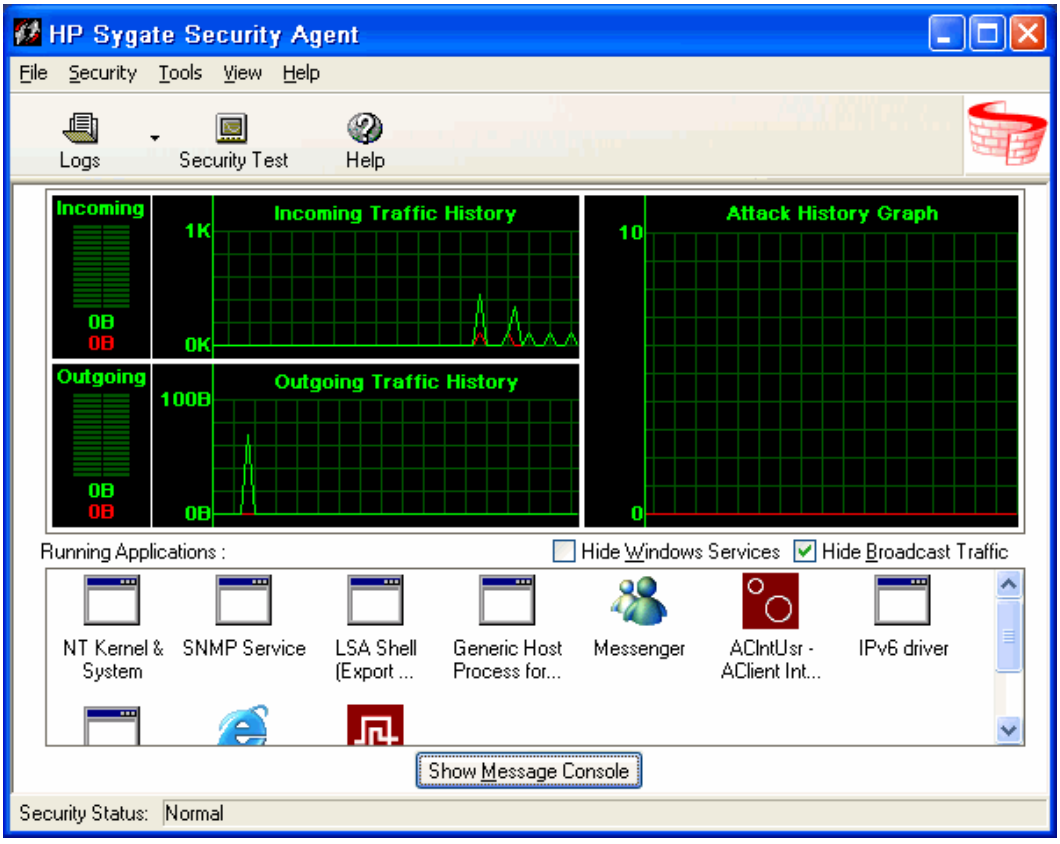


Figure 1. Main Console

The Agent interface is resizable, so you can view it as a full-screen or part-screen image.

Menus and Toolbar Buttons

The top of the screen displays a standard menu and toolbar. The toolbar buttons can be used to quickly access logs, view the Help file, or test your system.

Traffic History Graphs

Below the toolbar are the Traffic History graphs.

The Traffic History graphs produce a real-time picture of the last two minutes of your traffic history. The graphs reload new information every second, providing instant data, as measured in bytes, about your incoming and outgoing network traffic.

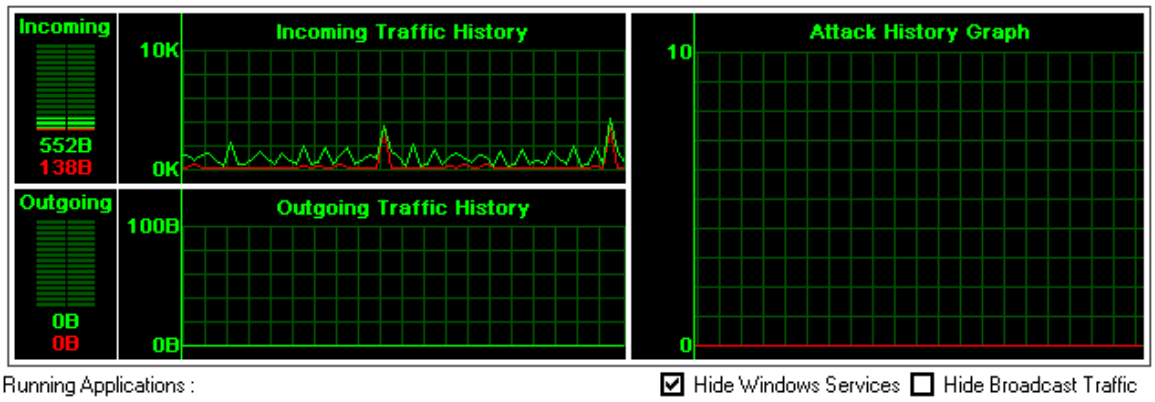


Figure 2. Traffic History Graph

The Traffic History graphs are broken into three sections. On the left side of the graphs section are the Incoming and Outgoing Traffic History graphs. These provide a visual assessment of the current traffic that is entering and leaving your device through a network interface. This includes traffic that is allowed and traffic that is blocked. The green lines and bars indicate traffic that is allowed to pass through, and the red coloring indicates traffic that is being blocked by the Agent.

Additionally, the Attack History graph on the right side of the console provides information on attempted attacks against your machine.

Broadcast Traffic

Broadcast traffic is network traffic that is sent to every device in a particular subnet, and thus is not directed specifically to your device. If you do not want to see this traffic, you can remove it from this graphical view by clicking **Hide Broadcast Traffic**. You will then only see "unicast" traffic in this graph, which is traffic that directed specifically to your device. To redisplay broadcast traffic, click to clear **Hide Broadcast Traffic.**

Running Applications Field

The Running Applications field provides a list of all applications and system services that are currently running on your system.

An application icon displays a small blue dot on lower left-hand or right-hand corner to indicate if it is receiving (left-hand) or sending (right-hand) traffic.

You can hide the display of system services by clicking **Hide Windows Services** above the Running Applications field. There are a number of services running at any given time, and

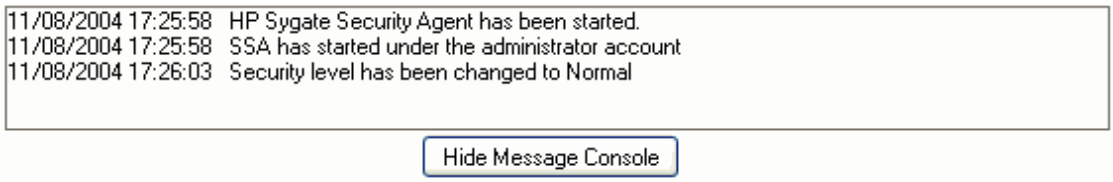
since they are often crucial to the operation of your device, you most likely want to allow them.

To change the display of application names, either click the **View** menu or right-click the Running Applications field and select the desired view.

You can stop an application or service from running by right-clicking the application in the Running Applications field and clicking **Terminate**.

Message Console

The Message Console of the Agent is located below the Running Applications field on the main console. It provides a real-time update of your Agent's communication status.



The Message Console is, by default, hidden.

To show or hide the Message Console:

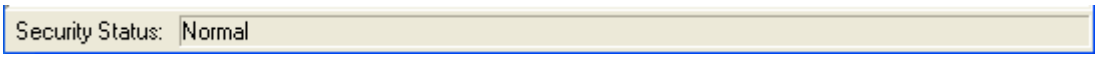
1. Below the Running Applications field, click **Show Message Console**. The Message Console appears.

2. To hide the Message Console from view, click **Hide Message Console**.

   The Message Console collapses so that only the **Show Message Console** button is apparent.

Status Bar

The Status Bar, located along the bottom of the Agent main console, provides the user with the current location profile information.



Using the Menus and the Toolbar

The top of the Agent screen displays a standard menu with the following options: **File**, **Security**, **Tools**, **View**, and **Help**.

Table 1. Menus

Menu	Menu choices
File	• **Close**—Closes the Agent main console. • **Exit Sygate Agent**—Exits the Agent, effectively turning off security on your machine.
Security	• **Block All**—Blocks all network traffic on your machine. If you use this command but then want to unblock the traffic, click the system tray icon on the taskbar and click **Normal**. • **Normal**—Blocks only selective traffic. This is the default configuration, and is a prudent choice.
Tools	• **Logs**—Opens the Logs. • **Options**—Opens the Options dialog box, which contains many security options, including email alerts, Network Neighborhood browsing rights, and log file configuration. • **Advanced Rules**—Opens the Advanced Rules dialog box, where you can set very specific rules for implementing security on your Agent. • **Update Signature**—Not enabled for the Agent. • **Automatically Start Service**—Not enabled for the Agent. • **Test Your System Security**—Opens the Sygate Technologies scan site so you can test the effectiveness of the Agent. • **Disable/Enable Sygate Security Agent**—Disables and reenables the Agent. The Agent is running but not protecting your system while it is disabled.
View	The View menu gives users the option to alter the display of software programs in the Running Applications field: • **Large Icons**—Displays 32x32 icons in the field. Each icon represents a software application or a system service. • **Small Icons**—Displays 16x16 icons. Both the large and small icon displays provide the full name of the application below the icon itself, and the icons are displayed in a "corkboard" fashion. • **List**—Provides small icon representations, with the icons displayed in a standard list. • **Applications Details**—Provides not only a list of all running applications, but also useful information on the version number and location path of each application.

Table 1. Menus

Menu	Menu choices
	• **Connection Details**—Provides further information on the type of connection being made by an each application accessing the network adapter, as well as the protocol, local and remote ports and IP addresses being used, the application path, and more. • **Hide Windows Services**—Toggles the display of Windows Services in the Running Applications field. • **Hide Broadcast Traffic**—Toggles the display of broadcast traffic in the Running Applications field.
Help	• **Help Topics...**—Opens the Agent online Help files. • **About**—Opens the About screen.

Toolbar Buttons

The buttons located below the menu provide shortcuts that can be used to quickly block all applications, change your application profiles, access the logs, test your Agent using the Sygate Technologies web site, or view the Help file.

Using the System Tray Icon

Once installed, the Agent displays a small icon in your system tray (located on the right-hand side of your taskbar), which you can double-click to open the Agent or right-click to see a menu of commands.

The icon  consists of two arrows that represent system traffic: the upward-pointing arrow is outgoing traffic; the downward-pointing arrow is incoming traffic.

These arrows give you a real-time update of your device's traffic flow. You might not see a constant icon appearance for more than a few seconds, especially if you frequently use the Internet or your network connection.

What the System Tray Icon Tells You

The colors of the arrows are always changing (as is the traffic flow on your device). For most users, it should be sufficient to remember the following points about the colors of the icon.

Table 2. System Tray Icon Colors

If the color of the arrow is...	...then...
RED	...traffic is being blocked by the Agent.
BLUE	...traffic is flowing uninterrupted by the Agent
GRAY	...no traffic is flowing in that direction.

The following table illustrates the different appearances that the system tray icon may have, and what they mean.

Table 3. System Tray Icon Appearance

Icon	Description
	The Agent is in Alert Mode. This means that an attempted attack against your device has been recorded in your Security Log. To make the icon stop flashing, double-click the icon. The Security Log will open, displaying a new log entry.
	The Agent is in Block All mode.
	Incoming traffic is flowing uninterrupted; there is no outgoing traffic.
	Both incoming and outgoing traffic are flowing uninterrupted.
	There is no incoming traffic; outgoing traffic is flowing uninterrupted.
	Incoming traffic is blocked; outgoing traffic is flowing uninterrupted.
	Incoming traffic is blocked; there is no outgoing traffic.

Table 3. System Tray Icon Appearance

Icon	Description
	Both incoming and outgoing traffic are blocked.
	There is no incoming traffic; outgoing traffic is blocked.
	Incoming traffic is flowing uninterrupted; outgoing traffic is blocked.
	No traffic is flowing in either direction.
	Both incoming and outgoing traffic flows uninterrupted; the Agent is disabled.

What Does the Flashing System Tray Icon Mean?

The system tray icon sometimes flashes on and off.  This means that the Agent is in Alert mode, which is caused by an attack recorded in the Security Log. When you point your mouse over the flashing icon, a tooltip appears above the icon describing the type of attack . The icon stops flashing after one minute. For users with an Administrator account, you can also stop the icon from flashing by opening the Security Log.

The System Tray Icon Menu

You can easily configure basic aspects of the Agent without even opening the main console. By right-clicking the system tray icon, you can change your security level, view Help or log files, or disable the Agent. You can roll your mouse over the system tray icon to see your current security level.

The system tray icon includes the following right-click commands.

Table 4. System Tray Icon Menu

Menu Option	Description
HP Sygate Security Agent	Opens the Agent's main console.
Block All	Blocks all network traffic.
Normal	Provides your preconfigured list of advanced rules and applies them.
Logs	Opens the Agent logs.
Options...	Opens the Options dialog box, where you can configure the settings for the Agent.
Advanced Rules	Opens the Advanced Rules dialog box, where you can write specific rules for allowing or blocking network access.
Disable/Enable Sygate Security Agent	Disables and reenables the Agent. The Agent is running but not protecting your system while it is disabled.
Help Topics...	Opens the online Help system.
About...	Opens the About dialog box, providing information on your version of the Agent.
Exit Sygate Agent	Stops the Agent from running. You need to restart the Agent to protect your system.

Enabling Password Protection

You can set your Agent to require a password prior to making any security changes, and to require a password before exiting the Agent.

To enable password protection:

1. Click the **Tools|Options|General** tab.
2. Click the **Set Password...** button at the bottom right of the dialog box. The following **Password** dialog box appears.

3. Enter your new password in the **New Password** and **Confirm New Password** fields.

   Note: You can disable password protection by making no entry in the **New Password** field and confirming that in the **Confirm New Password** field.

4. To have the Agent prompt you for a password before exiting the Agent, on the **General** tab, click **Ask password while exiting**.
5. Click **OK** to confirm or click **Cancel** to discard your changes.

Chapter 3. Testing Your System's Vulnerability

This chapter describes ways to test the vulnerability of your system to outside threats by scanning your system. The test is available directly from Sygate using an online connection.

Scanning Your System

Assessing your vulnerability to an attack is one of the most important steps that you can take to ensure that your device is protected from possible intruders. With what you learn from this battery of tests, you can more effectively set the various options on your Agent to protect your device from attack.

To scan your system:

1. Do one of the following:
   - On the toolbar, click the **Security Test** button.

   - On the **Tools** menu, click **Test Your System Security**.
   - In your Internet browser window, open the Sygate Technologies web page (http://scan.sygate.com) directly.
2. On the web page, click **Scan Now**. The Sygate Online Services scanner scans your computer and attempts to determine your IP address, operating system, web browser, and other information about your system.
3. For a specific type of scan, click one of the following web pages:
   - Quick Scan
   - Stealth Scan
   - Trojan Scan
   - TCP Scan

- UDP Scan
- ICMP Scan

4. Click **Scan Now**.

A brief document of frequently asked questions about Sygate Online Services is also available from the main scan page. Click **Scan FAQ** at the bottom left side of the screen.

Types of Scans

On the Sygate Technologies web site, you can choose from one of the following types of scans.

Quick Scans

The Quick Scan is a brief, general scan that encompasses several scanning processes. It usually takes 20 seconds or less to accurately scan your device's ports, protocols, services, and possible Trojans. The results are recorded in the Agent's Security Log.

Stealth Scans

The Stealth scan scans your device using specialized stealthing techniques, which mimic portions of legitimate computer communication to detect the presence of a computer. The Stealth scan takes about 20 seconds to complete and is most likely not recorded in the Security Log.

Trojan Scans

The Trojan scan feature scans all of your device's 65,535 ports for active Trojan horse programs that you or someone else may have inadvertently downloaded. The Trojan scan takes about 10 minutes to complete. A list of common Trojans is available on the web site.

TCP Scans

The TCP scan examines the 1,024 ports that are mainly reserved for TCP services, such as instant messaging services, to see if these ports are open to communication. Open ports can indicate a dangerous security hole that can be exploited by malicious hackers.

It scans ports on your device that are connected to devices such as routers and proxies for users connecting to the web site through such a device. The scan takes about 20 minutes to complete and is logged by the Agent as a scan event in the Security Log.

UDP Scans

The UDP scan uses various methods and protocols to probe for open ports utilizing UDP. The UDP scan will scan ports on your device that are connected to devices such as routers

and proxies for users connecting to the web site through such a device. The scan takes about 10 minutes and should be logged in the Security Log as a port scan from Sygate.

ICMP Scans

When an ICMP scan has completed scanning a user's device, it displays a page with the results of the scan. If a user is running the Agent, all scans are blocked.

Chapter 4. Working With Rules

This chapter describes how to protect your system by creating security rules for applications that you have running on your system.

About Rules

A firewall is hardware, software, or a combination of both that is used to prevent unauthorized Internet users from accessing a private network. All information entering or leaving the network must pass through the firewall, which examines the information packets and blocks those that do not meet the security criteria.

Using Rules to Protect Your System

The Agent uses *firewall rules*, or *security rules,* to systematically *allow* or *block* incoming and outgoing traffic from specific applications, ports, and IP addresses during designated time periods.

Each rule specifies the conditions and characteristics (such as the time of day, type of traffic, and port number) that must exist for the rule to take effect as well as the effect the rule has. For example, a security rule may state that "Port 80 is allowed." The Agent supports *advanced rules*, which exhibit complex relationships between applications, IP addresses, and services. For example, an advanced rule may state that remote port 80 is allowed to devices in subnet 193.58.74.0/24, between 9 AM and 5 PM, Monday through Friday.

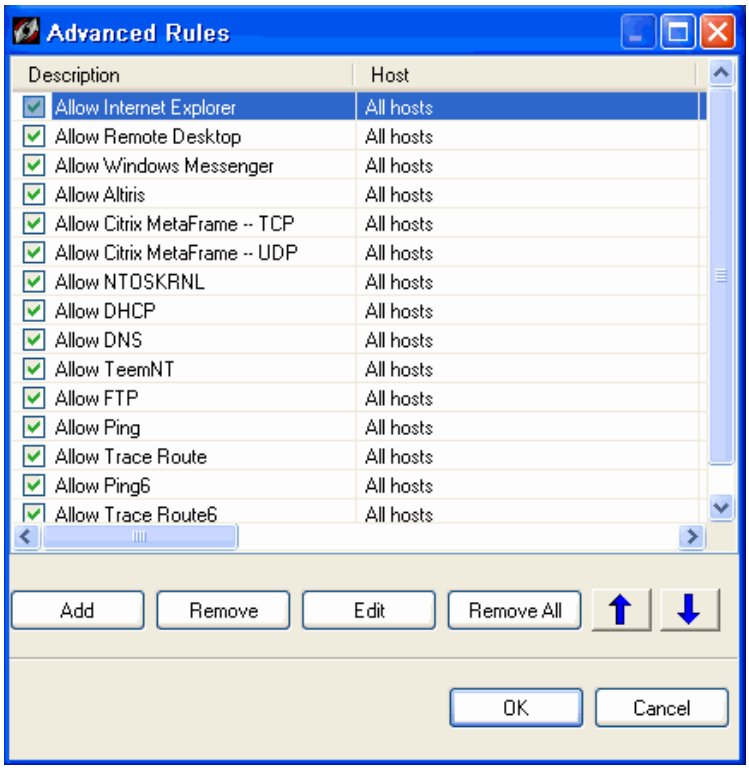
You can set up your own advanced rules or import them from an administrator or third party.

Setting Up Advanced Rules

When you set up an advanced security rule, first decide what effect you want the rule to have. For example, do you want to block all traffic when your screensaver is on? Would you like to allow all traffic from a particular source? Do you want to block UDP packets from a web site?

To set up an advanced rule:

1. On the **Tools** menu, click **Advanced Rules**. The Advanced Rules dialog box opens.



2. Click **Add**. The Advanced Rule Settings dialog box opens with the **General** tab displayed.
3. Enter a name for the rule in the **Rule Description** text box, and click **Block this traffic** or **Allow this traffic**.
4. Click the **Applications** tab, and either click the check box for the application you want to allow or block, or click the **Browse** button to locate it.
5. To create a rule with the default settings, click **OK**. Or, to change these settings on the other tabs, including **General**, **Hosts**, **Ports and Protocols**, **Scheduling**, and **Applications**.

   These five tabs on the Advanced Rule Settings dialog box provide additional settings for traffic for each rule. The more information that you enter on each tab, the more specific the rule will be.

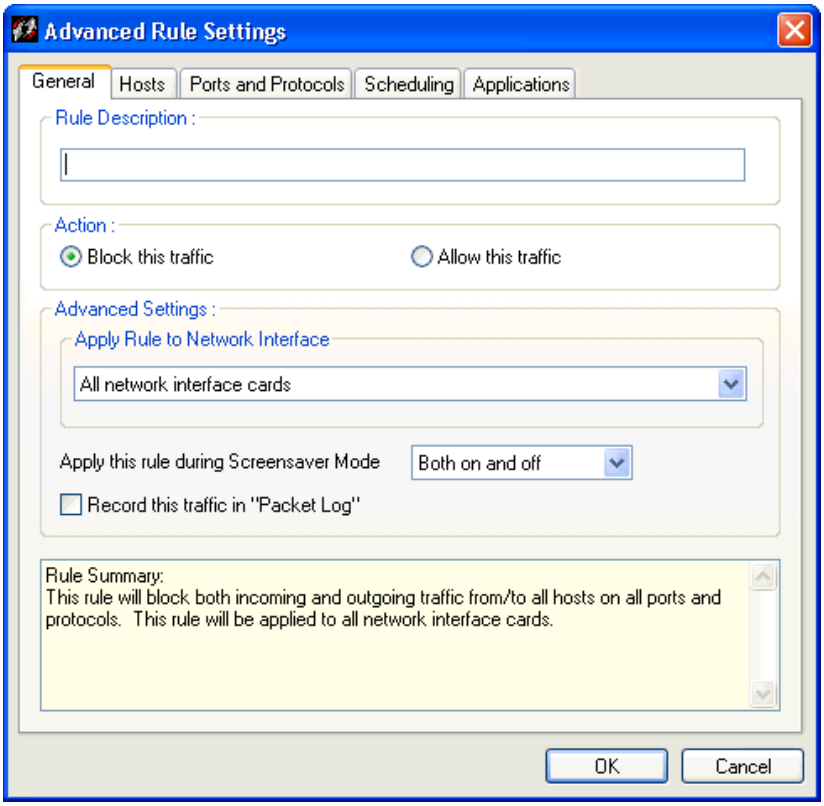
6. Click the **Move Up** or **Move Down** buttons to change the order that the rule is applied.

Rules are applied in the order they are listed. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the Agent blocks all traffic at all times.

7. To enable a rule on the Agent, make sure the check mark appears in the **Description** column.

General Tab

The **General** tab is used to provide a name for the rule you are creating, as well as the effect that the rule will have (allowing or blocking traffic).



Rule Description

Functions as the name of the rule, and it should indicate qualities of the rule. For instance, "Rule1" may not be a very good name for a rule, but "Block After 1 AM" would be.

Block this traffic

Denies traffic specified by the rule from accessing your network.

Allow this traffic

Allows traffic specified by the rule from accessing your network.

Apply Rule to Network Interface

Specifies which network interface card this rule will apply to. If you have multiple network cards, select one from the list box, or select **All network interface cards** to apply the rule to every card.

Apply this rule during Screensaver Mode

Activates the rule even if your device's screensaver is on (if applicable).

- **On**—The rule will be activated only when the screensaver is on. Enable this if you want to block all traffic and all ports while you device is idle.
- **Off**—This rule will be activated only if the screensaver is off and all other conditions are satisfied.
- Both **On** and **Off**—This rule is unaffected by the screensaver.

Record this traffic in "Packet Log"

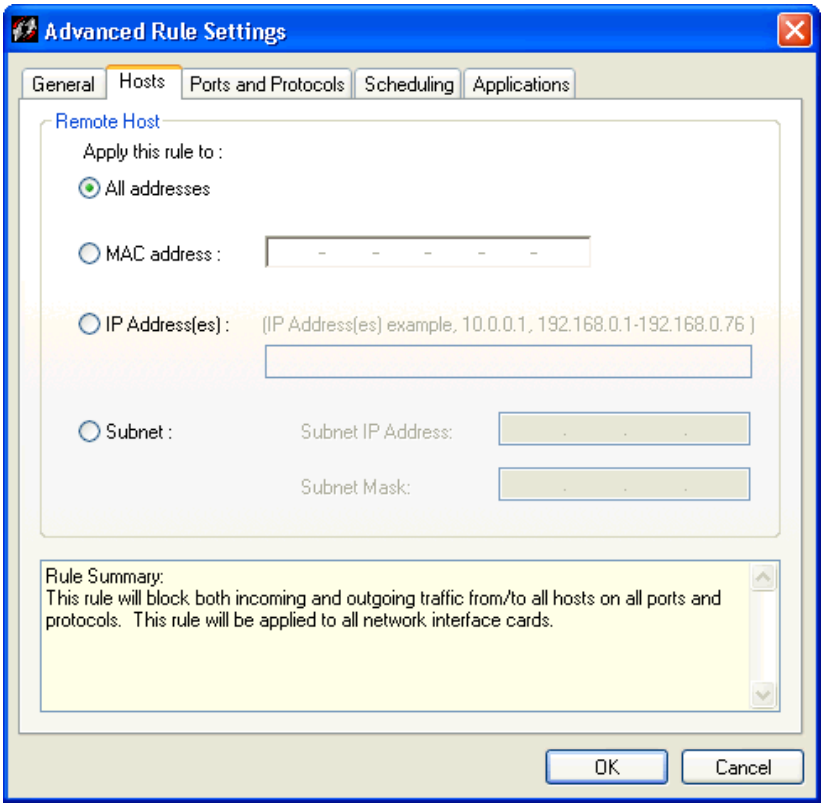
Records traffic affected by this rule in the Packet Log.

Rule Summary field

Provides a summary of the rule's functionality.

Hosts Tab

The **Hosts** tab is where you can specify the source (IP address, MAC address, or subnet range) of traffic that you want the rule apply to.



All addresses

Applies rule to all addresses.

MAC addresses

Applies rule to the MAC address of the traffic.

IP Address(es)

Applies rule to the IP address or address range of the traffic.

Subnet

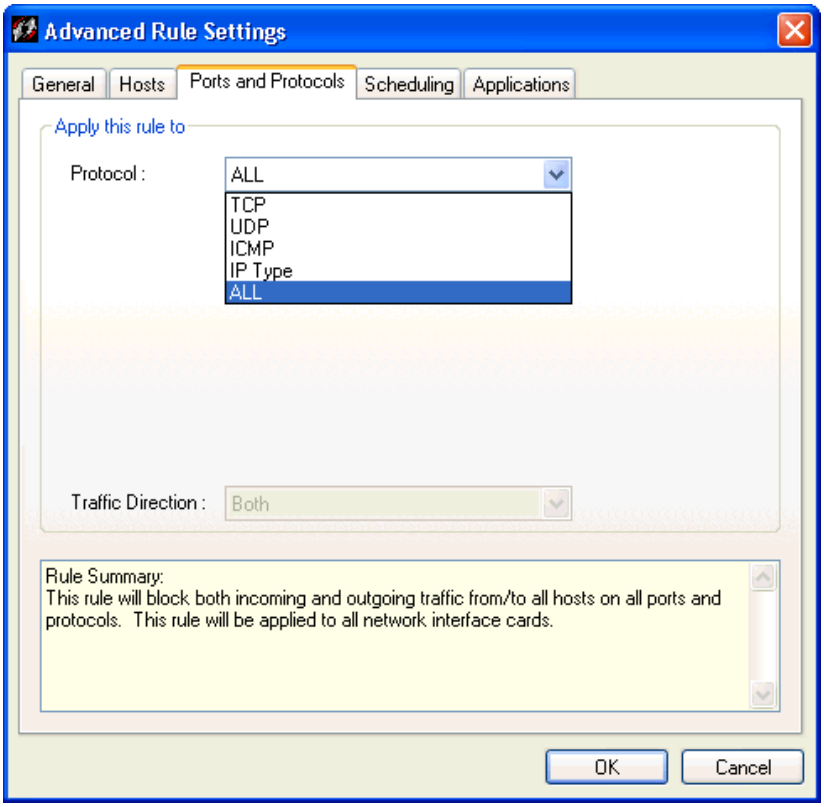
Applies rule to the subnet address and subnet mask of the traffic.

Rule Summary field

Provides a summary of the rule's functionality.

Ports and Protocols Tab

The **Ports and Protocols** tab provides an area to specify which ports and protocols, if any, should be affected by the traffic specified in the rule.



Protocol

Specifies a protocol for the rule.

All Protocols

Applies to all protocols on all ports, for both incoming and outgoing traffic.

TCP

Displays two more list boxes in which you can specify which ports (remote and/or local) should be affected by the rule. You can type the port numbers or select the port type from the list boxes for the both local and remote ports.

If you do not enter or select a port number, then all ports will be affected by the rule. If you enter a port number for the local port entry, but not for the remote port entry, then the local port you entered and ALL remote ports will be affected by the rule.

Then, select which traffic direction should be affected by the rule.

UDP

Displays two port list boxes. You can type the port numbers or select the port type from the list boxes for both local and remote ports. If you do not enter or select a port number, then

all ports will be affected by the rule. If you enter a port number for the local port entry, but not for the remote port entry, then the local port you entered and ALL remote ports will be affected by the rule.

Then, select which traffic direction should be affected by the rule.

ICMP

Displays a list of ICMP types. Select the types of ICMP that you wish allow or block by placing a check next to them. Then select which traffic direction should be affected by the rule.

IP Type

Displays a list of IP protocol types displayed on the lower half of the Ports and Protocols tab.

Traffic Direction

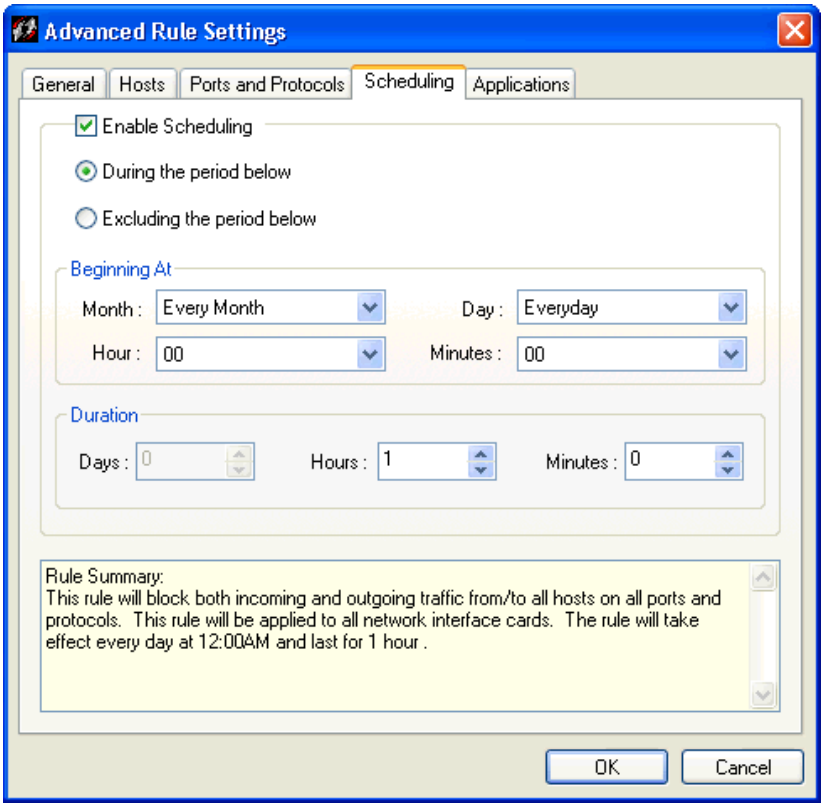
Specifies the traffic direction, either **Incoming**, **Outgoing**, or **Both**.

Rule Summary field

Provides a description of the rule and what traffic it affects on your system.

Scheduling Tab

The **Scheduling** tab provides a way for you to create a rule that you want to take effect only during (or excluding) certain time periods. For instance, if you want to block all traffic after 1 AM, then you can create a schedule that will permit the rule to do so.



Enable Scheduling

Enables the scheduling feature.

During the period below

Enables scheduling to take place during a certain time period.

Excluding the period below

Enables scheduling to take place outside of a certain time period.

Beginning At

Specifies the time that the scheduling begins, including a month, day, hours, and minutes. You can also leave the default settings, which apply the schedule all day, every day, all year.

Duration

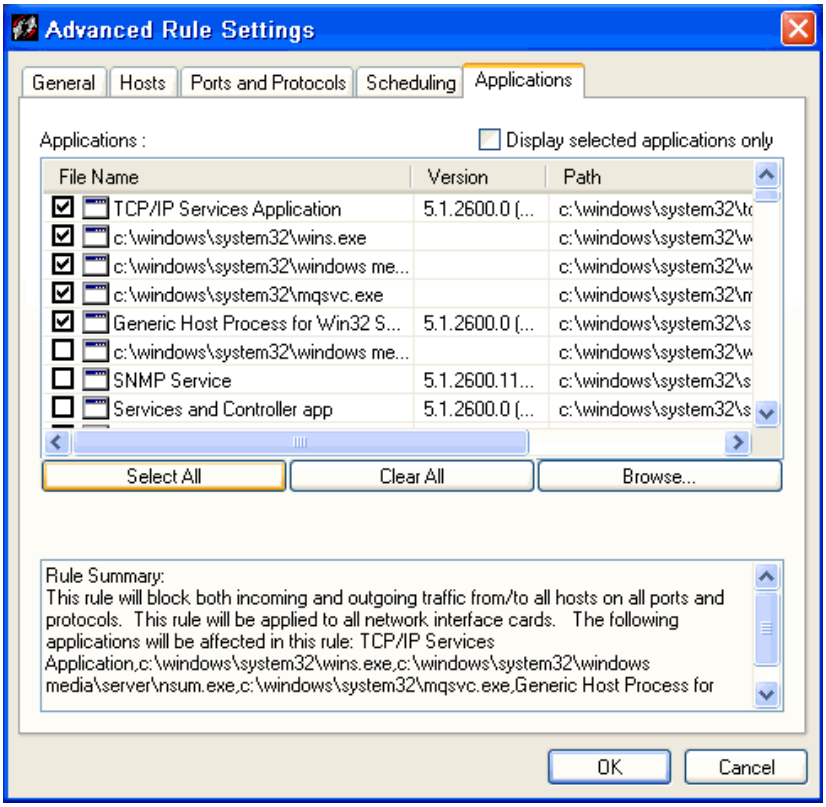
If you have specified a beginning time, specifies how long the rule will be in effect.

Rule Summary field

Provides a summary of the rule's functionality.

Applications Tab

You can specify applications that will be affected by advanced rules. The **Applications** tab provides a list of all applications that have accessed your network connection.



Display selected applications only

Displays only the applications that you have selected to be controlled by this rule.

Applications

Lists the traffic coming in and out of all ports and protocols. To select an application to be affected by this rule, click the box next to its name under the **FileName** column.

Select All

Selects all applications in the table.

Clear All

Clears all applications in the table.

Browse

Opens the Open dialog box so you can search for applications that are not displayed in the table.

Rule Summary field

Provides a description of the rule and what traffic it will affect on your system.

Chapter 5. Monitoring and Logging

This chapter describes how you can monitor your system by using the logs that are present in the Agent. It begins with an overview of logs, their types, and the tasks you can do with logs, such as back tracing logged events.

The Agent's *logs* are an important method for tracking your device's activity and interaction with other devices and networks. The logs record information about the Agent's status and about traffic attempting to enter or exit your device through your network connection.

There are four separate logs that monitor different aspects of your network connection. These logs tell you when your device has been blocked from the network and to some extent why. They are particularly useful in detecting potentially threatening activity, such as port scanning, that is aimed at your device. They also help you troubleshoot connectivity problems or possible network attacks.

The Agent's logs can also do back tracing, which enables you to use ICMP to determine all the hops between your device and an intruder on another computer.

Types of Logs

On the Agent, you can view four types of logs:

- **Security**—Records potentially threatening activity directed towards your device, DoS attacks, port scans, executable file alterations, and Trojan horse attacks.
- **Traffic**—Records every connection your device makes through the network.
- **Packet**—Captures every packet of data that enters or leaves a port on your device.
- **System**—Records all operational changes for the Agent, such as the starting and stopping of services, detection of network applications, software configuration modifications, and software execution errors.

Viewing Logs

To view logs on the Agent:

1. Do one of the following:
   - Click **Tools|Logs**.
   - On the toolbar, click the drop-down arrow next to the **Logs** icon.

   Note: Click the **Logs** icon to display the most recently viewed log.

2. Click one of the following log types: **Security Log**, **Traffic Log**, **Packet Log**, or **System Log**.

   Each log opens the Log Viewer dialog box. The Log Viewer is a data sheet, where each row represents a logged event, and the columns display information regarding the event. For more information on the differences between the icons and parameters of each log, see Security Log, Traffic Log, Packet Log, and System Log.

3. In the Log Viewer dialog box, click the **View** menu and click either **Local View**, the default setting, or **Source View**.

   Depending on whether you choose the local view or source view, you can view various options, which vary between each log.

4. In the **View** menu, click a different log name if you wish.
5. Click **Refresh** or press **F5** to update the log that you are viewing.
6. Click **File|Exit** to close the log.

Security Log

The Security Log records potentially threatening activity directed towards your device, such as port scanning, or denial of service attacks. The Security Log is probably the most important log file in the Agent.

Icons for the Security Log

When you open a Security Log, icons are displayed at the left side of the first column. These are graphical representations of the kind of attack logged on each line, and they provide an easy way to scan the Security Log for possible system errors.

Table 5. Security Log Icons

Icon	Description
	Critical attack
	Major attack
	Minor attack
	Information

Security Log Parameters and Description

The columns for logged events are:

Table 6. Security Log Parameters and Description

Name of Parameter	Description
Time	The exact date and time that the event was logged
Security Type	Type of Security Alert (for example: DoS attack, executable file, Ping of Death)
Severity	The severity of the attack (either Critical, Major, Minor, or Information)
Direction	Direction that the traffic was traveling in (incoming, outgoing, or unknown)—Most attacks are incoming, that is, they originate in another computer. Other attacks, like Trojan horses, are programs that have been downloaded to your device and therefore are already present; they are considered outgoing. Still other attacks are unknown in direction; they include Active Response or application executable changed.
Protocol	Type of protocol—UDP, TCP, and ICMP
Remote Host	Name of the remote computer *(only appears in Local View - this is the default)*
Remote MAC	MAC address of the remote device. If outside the subnet, it is the MAC address of the router. *(only appears in Local View - this is the default)*
Local Host	IP address of the local computer *(only appears in Local View - this is the default)*
Local MAC	MAC address of the local computer *(only appears in Local View - this is the default)*
Source Host	Name of the source computer *(only appears in Source View)*
Source MAC	MAC address of the source computer *(only appears in Source View)*
Destination Host	IP address of the destination computer *(only appears in Source View)*
Destination	MAC address of the destination computer *(only appears in Source View)*

Table 6. Security Log Parameters and Description

Name of Parameter	Description
MAC	
Application Name	Name of the application associated with the attack
User Name	User or Computer client that sent or received the traffic
Domain	Domain of the user
Security	Security level for the Agent, set to either **Block All** or **Normal**.
Occurrences	Number of occurrences of the attack method
Begin Time	Time the attack began
End Time	Time the attack ended

Description and Data Fields for the Security Log

Below the rows of logged events are the **Description** and **Data** fields. When you click an event row, the entire row is highlighted. A description of the event, such as "Somebody is scanning your device, with 13 attempts," appears in the **Description** field.

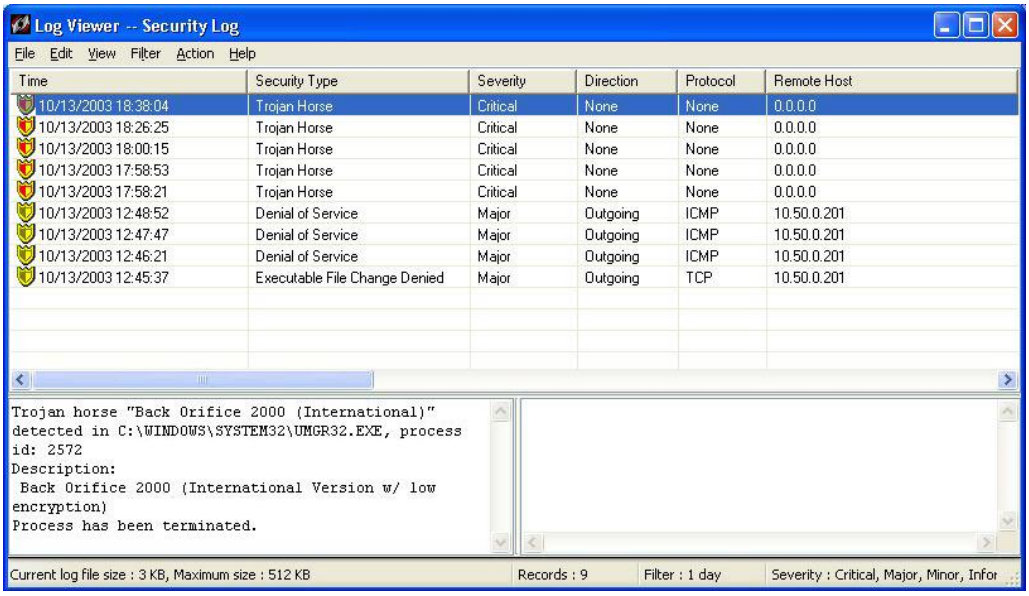


Figure 3. Security Log

Traffic Log

Whenever your device makes a connection through the network, this transaction is recorded in the Traffic Log.

Icons for the Traffic Log

When you open a Traffic Log, icons are displayed at the left side of the first column. They are graphical representations of the kind of traffic logged on each line and provide an easy way to scan the Traffic Log. Traffic Log includes information about incoming and outgoing traffic.

Table 7. Traffic Log Icons

Icon	Description
	Incoming traffic; passed through the Agent
	Incoming traffic; blocked by the Agent
	Outgoing traffic; passed through the Agent
	Outgoing traffic; blocked by the Agent
	Traffic direction unknown; passed through the Agent
	Traffic direction unknown; blocked by the Agent

Traffic Log Parameters and Description

The columns for logged events are:

Table 8. Traffic Log Parameters and Description

Name of Parameter	Description
Time	The exact date and time that the event was logged
Action	Action taken by the Agent: Blocked or Allowed
Severity	The severity of the traffic, set to 10.
Direction	Direction that the traffic was traveling in (incoming or outgoing)
Protocol	Type of protocol - UDP, TCP, and ICMP
Remote Host	Name of the remote computer *(only appears in Local View - this is the default)*
Remote MAC	MAC address of the remote device. If outside the subnet, it is the MAC address of the router. *(only appears in Local View - this is the default)*
Remote Port/ICMP Type	Port and ICMP type on the remote computer *(only appears in Local View - this is the default)*
Local Host	IP address of the local computer *(only appears in Local View - this is the default)*
Local MAC	MAC address of the local computer *(only appears in Local View - this is the default)*

Table 8. Traffic Log Parameters and Description

Name of Parameter	Description
Local Port/ICMP Code	Port and ICMP code used on the Agent device *(only appears in Local View - this is the default)*
Source Host	Name of the source computer *(only appears in Source View)*
Source MAC	MAC address of the source computer *(only appears in Source View)*
Source Port/ICMP Type	Port and ICMP type on the source computer *(only appears in Source View)*
Destination Host	IP address of the destination computer *(only appears in Source View)*
Destination MAC	MAC address of the destination computer *(only appears in Source View)*
Destination Port/ICMP Code	Port and ICMP code used on the destination computer *(only appears in Source View)*
Application Name	Name of the application associated with the attack
User	Login name of the user
Domain	Domain of the user
Security	Security level for the Agent, set to either **Block All** or **Normal**.
Location	The Location (Office, Home, VPN, etc.) that was in effect at the time of the attack
Occurrences	Number of packets each piece of traffic sends between the beginning and ending time
Begin Time	Time traffic starts matching the rule
End Time	Time traffic stops matching the rule
Rule Name	The rule that determined the passing or blockage of this traffic

Description and Data Fields for the Traffic Log

Below the rows of logged events are the **Description** and **Data** fields. When you click an event row, the entire row is highlighted. A description of the event is displayed in the **Description** field.

Packet Log

The Packet Log captures every packet of data that enters or leaves a port on your device. The Packet Log is disabled by default in the Agent because of its potentially large size. You must enable the Packet Log first.

Icons for the Packet Log

There is only one icon displayed in the Packet Log. It indicates the capturing of raw data packets.

Table 9. Packet Log Icons

Icon	Description
	Full data packet captured

Packet Log Parameters and Description

The columns for logged events are:

Table 10. Packet Log Parameters and Description

Name of Parameter	Description
Time	The exact date and time that the packet was logged
Remote Host	Name of the remote computer *(only appears in Local View - this is the default)*
Remote Port	Port on the remote host that sent/received the traffic *(only appears in Local View - this is the default)*
Local Host	IP Address of the local computer *(only appears in Local View - this is the default)*
Local Port	Port used on the Agent device for this packet *(only appears in Local View - this is the default)*
Source Host	Name of the source computer *(only appears in Source View)*
Source Port	Port on the source host that sent/received the traffic *(only appears in Source View)*
Destination Host	IP Address of the destination computer *(only appears in Source View)*
Destination Port	Port used on the destination computer for this packet *(only appears in Source View)*
Direction	Direction that the traffic was traveling in (incoming or outgoing)
Action	Action taken by the Agent: Blocked or Allowed
Application Name	Name of the application associated with the packet

Packet Decode and Packet Dump for the Packet Log

Below the **Log Viewer** are two additional data fields that provide further detail regarding the selected event. In the Packet Log, these fields are labeled **Packet Decode,** which provides data on the type of packet logged, and **Packet Dump**, which records the actual data packet.

System Log

The System log records all operational changes, such as the starting and stopping of services, detection of network applications, software configuration modifications, and software execution errors. All information provided in the System Log also appears in real-time in the Message Console. The System Log is especially useful for troubleshooting the Agent.

Icons for the System Log

When you open the System Log, icons are displayed at the left side of the first column. These are graphical representations of the kind of event logged on each line, and they provide an easy way to scan the System Log for possible system errors.

Table 11. System Log Icons

Icon	Description
	Error
	Warning
	Information

System Log Parameters and Description

The columns for logged events are:

Table 12. System Log Parameters and Description

Name of Parameter	Description
Time	The date and time that the event has been logged
Type	The type of event represents an Error, Warning, or Information. An Error log indicates a problem with the source; a Warning log indicates a potential problem; and an Information log provides information about an event involving the Agent.
ID	The ID assigned to the event by the Agent
Summary	Summary description of the event

Description and Data Fields for the System Log

Below the rows of logged events are the **Description** and **Data** fields. When you click on an event row, the entire row is highlighted. A description of the event, such as "Install WsProcessSensor successful....," appears in the **Description** field.

Enabling and Clearing Logs

The Security, Traffic, and System Logs are enabled by default. You must enable the Packet Log before you can view the contents.

To enable the log and set the log size:

1. On the **Tools** menu, click **Options**.
2. Click the **Log** tab.
3. Click the appropriate log check box to enable it.
4. Click the appropriate **Maximum Log File Size is** field and enter a size, in kilobytes, of the maximum size for the log file. 256 KB is the default setting.
5. Click **OK**.

To set the number of days to save the log:

1. On the **Tools** menu, click **Options**.
2. Click the **Log** tab.
3. Click the appropriate log check box to enable it.
4. Click the appropriate **Save log file for the past** field for the log you want to configure.
5. Enter the number of days.
6. Click **OK**.

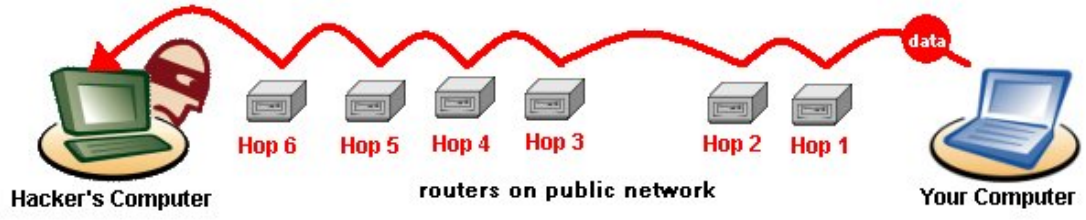
To clear the log:

1. In each log, click **File|Options**.
2. Make sure the Log tab is selected.
3. Click the **Clear Logs** button for the log you want to clear.

Note: For each log, you can also click **File|Clear**.

Back Tracing Logged Events

Back tracing enables you to pinpoint the source of data from a logged event. Like retracing a criminal's path at a crime scene, back tracing shows the exact steps that incoming traffic has made before reaching your device and being logged by the Agent.



Back tracing is the process of following a data packet backwards, discovering which routers the data took to reach your device. In the case of a Security Log entry, you can trace a data packet used in an attack attempt. Each router that a data packet passes through has an IP address, which is provided in the **Trace Route** field.

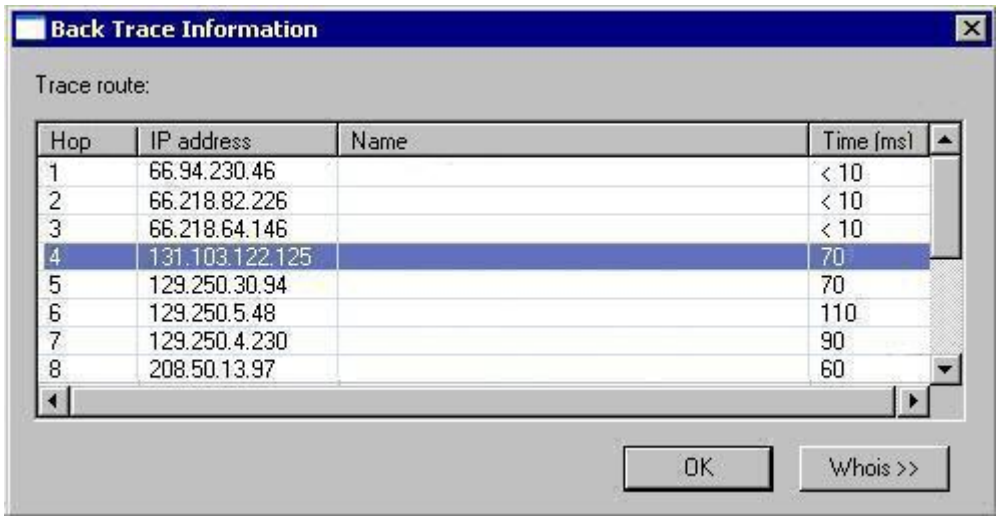
You can back trace a logged event in the Security, Traffic, and System logs.

To back trace a logged event:

1. Open the log file and click an event so that the entire row is selected.
2. Either right-click and click **BackTrace**, or click **Action|BackTrace**.

   The Agent begins back tracing the event.

3. The **Back Trace Information** dialog box appears.



The **Trace route** field provides details, such as IP address, on each *hop* made by the data packet that was logged by the Agent. A hop is a transition point, usually a router, that a packet of information travels through at as it makes its way from one computer to another on a public network, such as the Internet.

4. To view detailed information on each hop, click the **WhoIs>>** button.

   A drop panel displays detailed information about the owner of the IP address from which the traffic event originated. Note that the information displayed does not guarantee that you have discovered who the hacker actually is. The final hop's IP address lists the owner of the router that the hackers connected through, and not necessarily the hackers themselves.

5. Click either **Whois<<** again to hide the information.

   Note: You can cut and paste the information in the **Detail information** panel by pressing **Ctrl+C** to copy the information into the Clipboard.

   It is not advisable to contact persons listed in the **Detail information** panel unless you are experiencing a high number of security logs in which the attacks originate from one particular IP address.

6. Click **OK** to return to the Log Viewer dialog box.

Saving Logs

The contents of the logs can be saved to different locations. You may want to do this to save space, but is it more likely that you do this for security review, or to import them into a tool such as Microsoft Excel.

To save a log file:

1. Open the log in the Log Viewer.
2. Click **File|Export...**.
3. In the **Save As** dialog box, select the location for the log file.
4. Click **OK**.

Stopping an Active Response

Any security attack that is detected on the Agent triggers an active response. The active response automatically blocks the IP address of a known intruder for a specific amount of time (the default is 10 minutes). If you don't want to wait the default amount of time to unblock the IP address, you can stop the active response immediately.

You can stop active responses in the Security Log only.

To stop an active response:

1. On the main console, click **Tools|Logs|Security**.
2. Select the row for the application or service you want to unblock. Blocked traffic is specified as **Blocked** in the **Action** column.
3. On the **Action** menu, click **Stop Active Response** to block the selected application, or click **Stop All Active Response** if you want to unblock all blocked traffic.
4. When the Active Response dialog box appears, click **OK**.

Chapter 6. Configuring the Agent's Settings

You can set and import security options for the Agent, including e-mail notification of attacks, customizable pop-up messages, heartbeat settings, log file configuration, file sharing options, computer control settings, and advanced security measures such as Smart DHCP and Anti-MAC spoofing.

To configure the Agent:

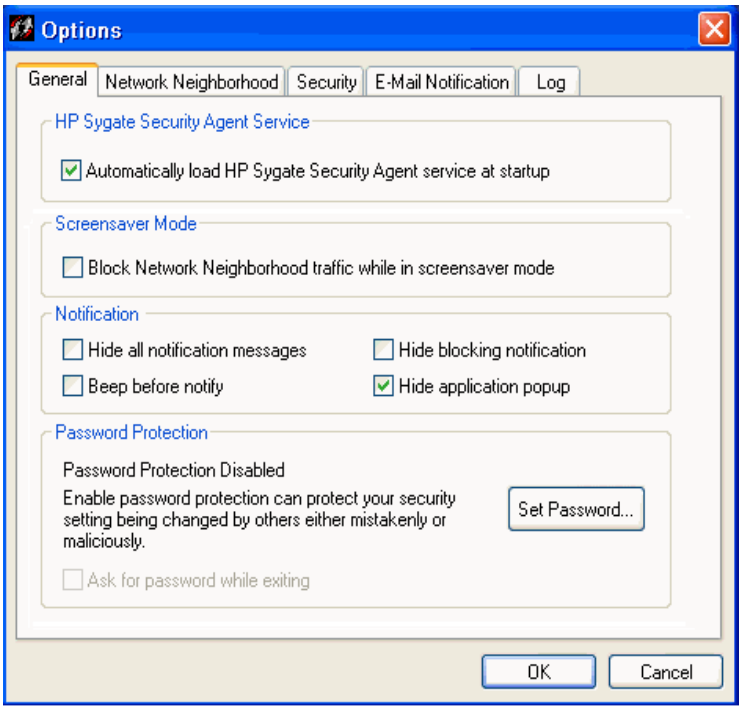
1. Do one of the following:
    - On the **Tools** menu, click **Options**.
    - Right-click the system tray icon and click **Options**.
    - In any log, on the **File** menu, click **Options**.

    The Options dialog box consists of the following tabs:
        - **General** tab
        - **Network Neighborhood** tab
        - **Security** tab
        - **E-Mail Notification** tab
        - **Log** tab

2. On any tab, click **OK** to apply all changes that you have made in the Options dialog box.

General Tab

The broadest level of configuration options for protecting your Agent appears on the **General** tab. This tab provides access to options for the basic running of the Agent.



Automatically load HP Sygate Agent service at startup

Automatically launches the Agent at startup.

Block Network Neighborhood traffic while in screensaver mode

Automatically sets your security level to **Block All** when your device's screensaver is activated. As soon as the device is used again, the security level returns to the previously assigned level.

Hide all notification messages

Causes the Agent to not display any notification messages. It also disables the **Beep before notify**, **Hide blocking notification**, and **Hide application popup** check boxes. By default, this option is not checked.

Beep before notify

Allows audio announcement first before system tray notification messages appear.

Hide blocking notification

Hides a pop-up message from appearing every time a blocked application or service tries to access the device from the network.

Hide application popup

Hides a dialog box that appears when you open an application that has been modified since you first installed it. For example, if Internet Explorer 5.0 was installed on the device and then you install Internet Explorer 6.0, the device assumes that Internet Explorer 6.0 is a new application with no associated rule to allow it.

You can use the dialog box to allow or block the modified application. The pop-up message appears for 15 seconds, by default. Click **Yes** to allow the application; click **No** to block it. If you do not respond to the message within 15 seconds, the Agent blocks the application from accessing the device.

Set Password

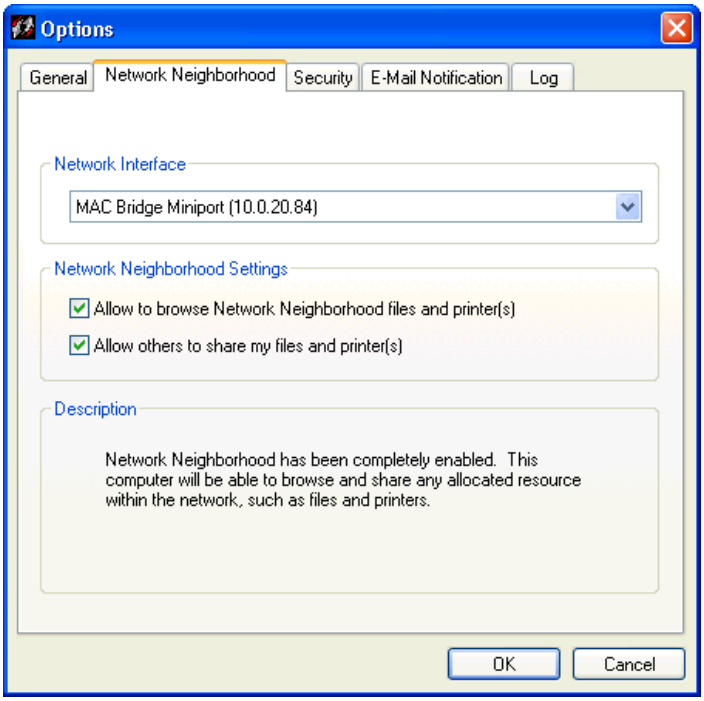
Opens the Password dialog box so that you can set password protection. This prohibits other users to access your Agent and possibly change your settings. If enabled, password protection prompts you to enter your password every time you access the Agent main console.

Ask password while exiting

Prompts you to enter your password when closing the Agent.

Network Neighborhood Tab

The **Network Neighborhood** tab provides multiple interface support and network browsing rights configuration.



Network Interface

Specifies the network you want to access.

Allow to browse Network Neighborhood files and printer(s)

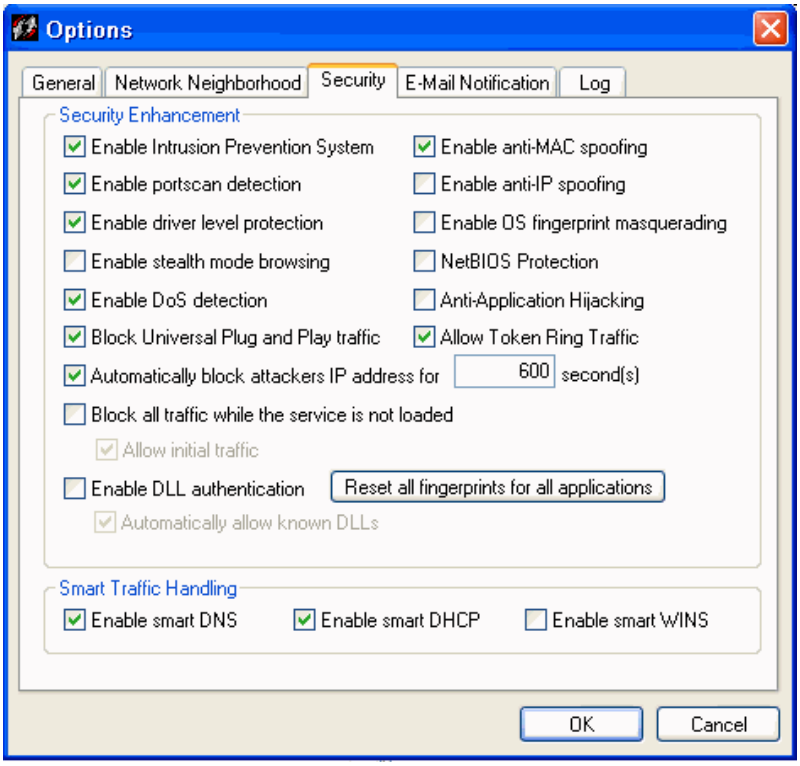
Enables you to browse other computers, devices, and printers on the selected network. This allows you to access other files on your network. If you disable this, you cannot copy files from network locations.

Allow others to share my files and printer(s)

Allows other users of the selected network to browse your device.

Security Tab

The **Security** tab offers a way to enable and disable some of the more complex security options. You should test settings made here before propagating them to other devices, to make certain that they work as you intend.



Enable Intrusion Prevention System

Provides you with alerts when another user attempts to compromise your system. Intrusion prevention on the Agent actually enables a combination of both an intrusion detection system (IDS) and an intrusion prevention system (IPS). The end result is a system that

analyzes network packets and compares them with both known attacks and known patterns of attack, and then blocks those attacks. One of the key capabilities of the Intrusion Prevention System is its capability to do deep packet Inspection. By default, this option is enabled on the Agent.

Enable port scan detection

Detects if someone is scanning your ports, and notifies you. Port scanning is a popular method that hackers use to determine which of your device's ports are open to communication. Ports are dynamically blocked by the Agent and are therefore protected from hacking attempts.

If disabled, the Agent does not detect scans or notify you of them, but still protects your ports from hacking attempts. By default, this option is enabled on the Agent.

Enable driver level protection

Blocks protocol drivers from accessing the network unless the user gives permission. If a protocol driver attempts to access the network, you will see a pop-up message asking if you want to allow it. By default, this option is already enabled on the Agent.

Enable stealth mode browsing

Stealth mode describes a computer that is hidden from web servers while on a network. A computer on the Internet, for instance, if in stealth mode, cannot be detected by port scans or communication attempts, such as **ping**. By default, this option is disabled on the Agent.

Enable DoS detection

Causes the Agent to check incoming traffic for known Denial of Service (DoS) attack patterns. DoS attacks are characterized by an explicit attempt by an intruder to prevent legitimate users of a service from using that service. By default, this option is enabled on the Agent.

Block Universal Plug and Play Traffic

Causes the Agent to look for and block UPnP traffic to counter the vulnerabilities that are introduced by this operating system feature: The first vulnerability could enable an attacker to gain complete control over an affected system, while the second vulnerability could enable an attacker to either prevent an affected system from providing useful service or utilize multiple users' systems in a distributed denial of service attack against a single target. Users can disable this feature when using applications that require the UPnP protocol to operate. By default, this option is enabled in the Agent.

Automatically block attacker's IP address for... second(s)

Blocks all communication from a source host once an attack has been detected. For instance, if the Agent detects a DoS attack originating from a certain IP address, the Agent will block any and all traffic from that IP for the duration specified in the seconds field. By default, this option is enabled in the Agent.

Block all traffic while the service is not loaded

Prevents any traffic from entering or leaving your device during the seconds between the time that your machine turns on and the Agent is launched. This time frame is a small security hole that can allow unauthorized communication. Enabling this feature prevents possible Trojan horses or other unauthorized applications from communicating with other computers or devices. This also takes effect if the Agent crashes or if the Agent is shut down. By default, this option is enabled in the Agent.

Allow initial traffic

Enables initial traffic, needed for basic network connectivity, to take place. This includes initial DHCP and NetBIOS traffic so that the Agent can obtain an IP address, for example. By default, this option is enabled in the Agent.

Enable DLL authentication

Allows the Agent to determine which DLLs are used by which trusted applications and to store that information. The Agent then blocks applications that are using DLLs that are not associated with a trusted application or DLLs that are associated with a trusted application and that have changed. Note that this may take place if you download a patch to an application that modifies that application's DLL, in which case you are prompted to approve or reject using this changed DLL.

A DLL (dynamic link library) is list of functions or data used by Windows applications. Most, if not all, Windows applications use DLLs to run, and each application uses specific DLLs. Often, several applications will access the same DLL. However, some hackers try to disguise malicious code or applications as DLLs, and use them to hack computers. Most DLLs have a file extension of .dll, .exe, .drv, or .fon.

Because this option can interfere with the functioning of Windows applications, it is recommended that only users who have a firm understanding of Windows and DLLs enable this feature. By default, this option is disabled in the Agent.

Reset all fingerprints for all applications

Clears the Agent's memory of all application fingerprints. The result is that each time you use an application that uses the network, you are prompted through a pop-up message to **Allow** or **Block** that application's activity. By default, this option is enabled in the Agent.

Automatically allow all known DLLs

Automatically allows DLL modules that are commonly loaded by the network application. Disabling this feature will cause the engine to prompt for permission on all new DLLs that are loaded, and may cause very frequent prompting when using a complex network application, such as an Internet browser. By default, this option is enabled in the Agent.

Enable anti-MAC spoofing

Allows incoming and outgoing ARP traffic only if an ARP request was made to that specific host. It blocks all other unexpected ARP traffic and logs it in the Security Log. By default, this option is enabled on the Agent.

Some hackers use MAC spoofing to attempt to hijack a communication session between two computers in order to hack one of the machines. MAC (media access control) addresses are hardware addresses that identify computers, devices, servers, routers, etc. When Computer A wants to communicate with Computer B, it may send an ARP (Address Resolution Protocol) packet to the computer.

Enable anti-IP spoofing

IP spoofing is a process used by hackers to hijack a communication session between two computers, which we will call Computers A and B. A hacker can send a data packet that causes Computer A to drop the communication. Then, pretending to be Computer A, the hacker can communicate with Computer B, thus hijacking a communication session and attempting to attack Computer B.

Anti-IP spoofing foils most IP spoofing attempts by randomizing the sequence numbers of each communication packet, preventing a hacker from anticipating a packet and intercepting it. It is recommended that you enable this option along with **Enable OS fingerprint masquerading**. By default, this option is enabled on the Agent.

Enable OS fingerprint masquerading

Keeps programs from detecting the operating system of a device running the Agent software. When OS Fingerprint Masquerading is enabled, the Agent modifies TCP/IP packets so it is not possible to determine its operating system. It is recommended that you enable this option along with **Enable anti-IP spoofing**, discussed previously. By default, this option is enabled on the Agent.

NetBIOS protection

Blocks all communication from computers located outside the Agent's local subnet range. NetBIOS traffic is blocked on UDP ports 88, 137, and 138 and TCP ports 135, 139, 445, and 1026. Be aware that this can cause a problem with Outlook if connecting to an Exchange server that is on a different subnet. If that occurs, you should create an advanced

rule specifically allowing access to that server. By default, this option is disabled on the Agent.

Anti-Application Hijacking

Causes the Agent to check for malicious applications that work by interjecting DLLs and Windows hooks into Windows applications, and to block those malicious applications when found. By default, this option is disabled on the Agent.

Allow Token Ring Traffic

Allows Agents connecting through a token ring adapter to access the corporate network. By default, this option is enabled in the Agent.

Enable smart DNS

Blocks all DNS traffic, except for outgoing DNS requests and the corresponding reply. This means that if your computer sends out a DNS request, and another computer responds within five seconds, the communication will be allowed. All other DNS packets will be dropped.

If you disable this feature, please note that you will need to manually allow DNS name resolution by creating an advanced rule that allows UDP traffic for remote port 53. By default, this option is enabled in the Agent.

Enable smart DHCP

Allows only outgoing DHCP requests and incoming DHCP replies, and only for network cards that allow DHCP.

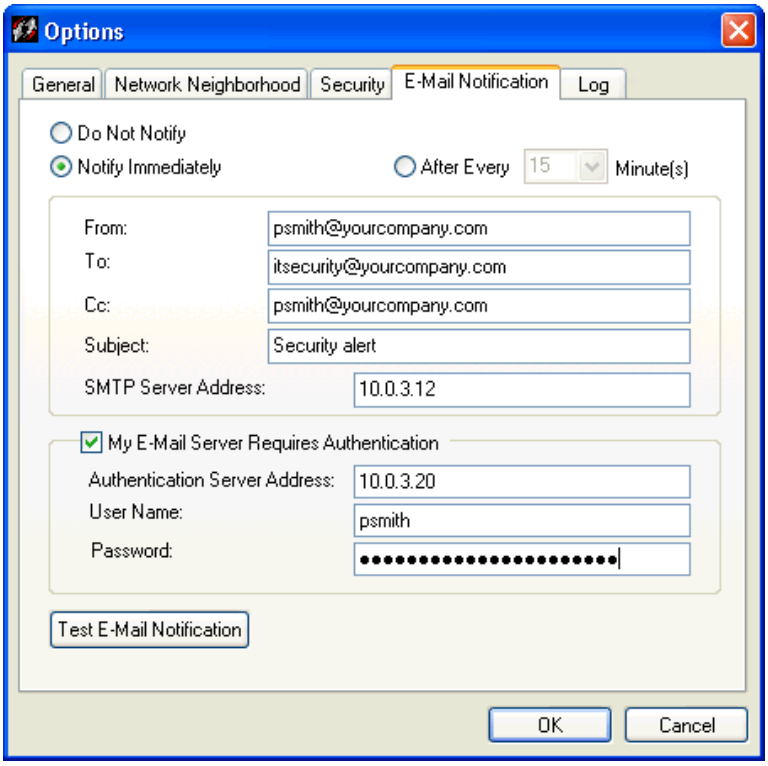
If you disable this feature and need to use DHCP, you must create an advanced rule for UDP packets on remote ports 67 and 68. By default, this option is enabled on the Agent.

Enable smart WINS

Allows Windows Internet Naming Service (WINS) requests only if they were solicited. If the traffic was not requested, the WINS reply is blocked. By default, this option is disabled in the Agent.

E-Mail Notification Tab

The **E-Mail Notification** tab provides you with the option to automatically notify a specified recipient through an e-mail message of any attacks against your device.



The first three options set the frequency of the message.

Do Not Notify

Disables the e-mail notification option.

Notify Immediately

Sends an e-mail message immediately following an attack on your device.

After Every . . . Minutes

Sends an e-mail message at regular intervals following an attack, the intervals specified in the **After Every ... Minute(s)** dial.

From:

Specifies an e-mail address for the person sending the message. This can be your personal e-mail address or another e-mail address.

To:

Specifies a recipient email address. This can be an administrator's email address, or your email address, if you are accessing email remotely.

Cc:

Specifies an e-mail address to send a courtesy copy of each email message.

Subject:

Describes the subject of the e-mail message.

SMTP Server Address:

Specifies your SMTP Server Address.

My E-Mail Server Requires Authentication

Specifies whether your e-mail server requires authentication.

Authentication Server Address:

Specifies the address of the authentication server.

User Name/Password:

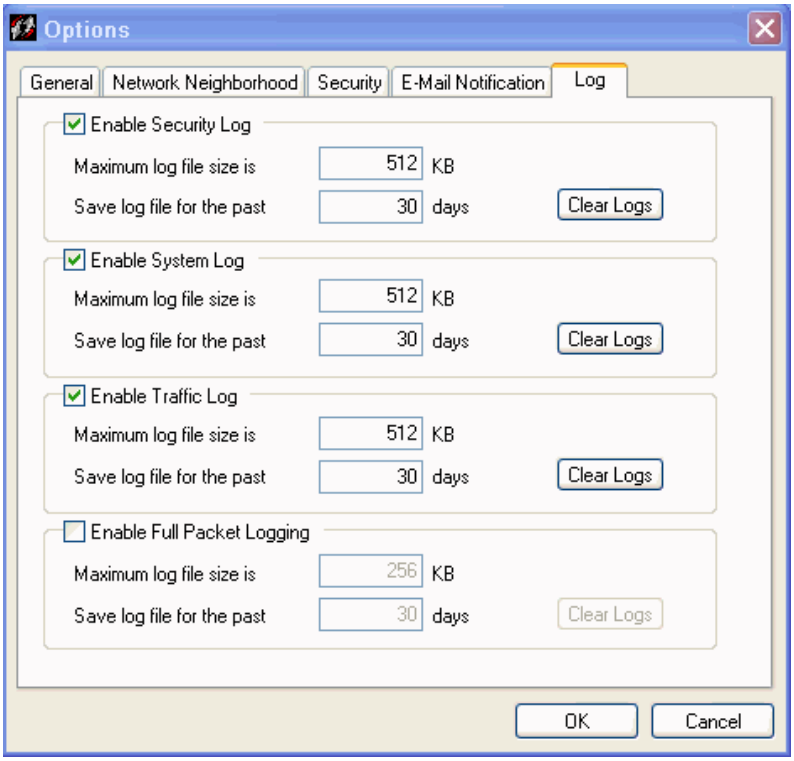
Specifies your username and password for the authentication server in the appropriate fields.

Test E-Mail Notification

Sends a test message to the e-mail address that you specified in the **To:** and **Subject:** fields.

Log Tab

The **Log** tab provides a central location to manage the logs for the Agent. You can determine the standard log size for each log, as well as specify how many days of entries are recorded in each log. You can also toggle whether or not logs are kept for each type of log.



Enable ... Log

Enables the Security, Traffic, System, and Packet Logs. The Packet Log is not enabled by default.

Maximum log file size is ... KB

Specifies the maximum size for the log file in kilobytes. The default setting is either 512 KB or 1024 KB.

Save log file for the past ... days

For the log you want to configure, specifies the number of days to save the log.

Clear Logs

Clears the selected log.

Glossary

A

access point: A network connection that allows a computer or user to connect to an enterprise network. Virtual Private Networks (VPNs), wireless communications, and Remote Access Service (RAS) dial-up connections are examples of access points. See also end point, wireless access point (wireless AP).

Active Response: The ability to automatically block the IP address of a known intruder for a specific amount of time. The amount of time that a Security Agent blocks an intruder's IP address can be modified to any interval from 1 to 65,000 seconds. By the way, a Trojan is not considered an attack because it is a program running on the same computer on which a Security Agent has detected a Trojan.

adapter: See network adapter.

Advanced rule: A rule that can be added on an Agent to enforce a security policy. Advanced Rules can exhibit complex relationships between applications, IP addresses, and services. See also firewall rule, simple rule.

Agent: A device running HP Sygate Security Agent software is also called an Agent device.

Anti-IP Spoofing: An advanced setting that prevents an intruder from taking advantage of the ability to forge (or spoof) an individual's IP address. See also IP Spoofing.

Anti-MAC Spoofing: An advanced setting that prevents an intruder from taking advantage of the ability to forge (or spoof) a Media Access Control (MAC) address of a computer. Anti-MAC Spoofing allows incoming and outgoing ARP (Address Resolution Protocol) traffic only if an ARP request has been made to a specific host. It blocks all other unexpected ARP traffic and logs it in a Security Log. See also Smart ARP, MAC address, MAC Spoofing.

antivirus: Software and technology that is used to detect malicious computer applications, prevent them from infecting a system, and clean files or applications that are infected with computer viruses. Sygate software works together with, but does not include, antivirus software.

application authentication: Authenticating an application that is running on a network is accomplished by taking the entire binary of an application and performing an MD5 hash and then comparing it with the application fingerprint stored on an Agent. If the application was changed, it may not be authenticated depending on the rules that an Agent is using. See also application control, application fingerprint, DLL authentication, MD5 hash.

application control: Applications and what versions of the particular application can either be allowed or disallowed via security policies.

application fingerprint: A 128-bit number that is generated by performing an MD5 hash of an entire application packet. It is unique for each application. If the application is changed in any way, the application fingerprint changes. See also application authentication.

authentication: The process by which a system identifies an individual or a computer to make sure that the user or computer is who they claim to be.

authorization: The process of granting or denying access to a specific network resource or domain based on the user's identity.

B

backtrace: A way of using ICMP to determine all the hops between your computer and an intruder on another computer. See also Internet Control Message Protocol (ICMP).

broadcast: Sending a packet to everybody on the network. See also multicast, unicast.

buffer overflow: Applications set aside areas of memory, or buffers, for use as storage, frequently setting aside a finite amount of memory for a buffer. A buffer overflow exists when an application attempts to store more data than can fit in a fixed-size buffer. Buffer overflow attacks occur when an intruder is able to send data in excess of a fixed-size application buffer and the application does not check to ensure this doesn't happen. By overflowing a buffer with executable code, an intruder can cause an application to perform unexpected and often malicious actions using the same privileges the application has been granted.

C

client: A device or program that uses shared resources from another computer, called a server. In the context of the Agent, client refers to a Sygate Security Agent running on a device that reports to a server.

computers: A personal computer, laptop, or workstation on which users perform work. In an enterprise environment, computers are connected together over a network.

D

demilitarized zone (DMZ): A security measure used by a company that can host Internet services and has devices accessible to the Internet; the DMZ is an area between the Internet and the internal network that prevents unauthorized access to the internal corporate network using a firewall or gateway.

Denial of Service (DoS): A network-based attack that is characterized by an explicit attempt by an intruder to prevent legitimate users of a service from using that service. See also Denial of Service Checking.

Denial of Service Checking: An advanced setting on the Agent that instructs the Agent to check for incoming traffic using known Denial of Service (DoS) techniques.

DES: See Data Encryption Standard (DES).

destination IP address: The IP address of the computer that is receiving packets of information.

destination port: The port of the computer that is receiving packets of information.

DHCP: See Dynamic Host Configuration Protocol (DHCP).

directory server: Software that manages users' accounts and network permissions. Active Directory is an example of a directory server accessed using Lightweight Directory Access Protocol (LDAP). See also Active Directory, Lightweight Directory Access Protocol (LDAP).

DLL: Dynamic link library, a list of functions or data used by Windows applications. Most DLLs have a file extension of .dll, .ocx, .exe, .drv, or .fon.

DLL authentication: The ability to validate shared or application-specific dynamic link libraries (DLLs) and ensure the integrity of applications. An Agent can be instructed to allow or block known DLLs. An added level of protection can also be enabled to block DLLs from being dynamically allowed when an application is executed. See also application authentication, application fingerprint, DLL, DLL fingerprint.

DLL fingerprint: A 128-bit number that is generated by performing an MD5 hash of an entire DLL packet. It is unique for each DLL. The MD5 hash or fingerprint of each DLL is stored on the Sygate Security Agent and forwarded to the Sygate Management Server. If the DLL is changed in any way, the DLL fingerprint changes. See also DLL, DLL authentication, MD5 hash.

domain: A group of computers that are part of a network and share a common directory database. Each domain has a unique name and is organized in levels that are administered as a unit using common rules.

domain name: The name by which a group of computers is known to the network. Most organizations have a unique name on the Internet that allows individuals, groups, and other organizations to communicate with them. See also domain.

DoS attack: See Denial of Service (DoS).

driver-level protection: A Sygate software feature that blocks protocol drivers from gaining access to the network unless a user gives permission. If a protocol driver attempts to gain access to the network through a client running the Sygate Security Agent, depending on the rule set, the protocol driver is allowed, blocked, or a pop-up message displays. See also protocol driver blocking.

Dynamic Host Configuration Protocol (DHCP): A TCP/IP protocol that provides dynamic configuration of host IP addresses and enables individual computers on an IP network to extract configuration parameters from a DHCP server. DHCP lets a system administrator supervise and distribute IP addresses from a central point in the network.

E

EAP: Extensible Authentication Protocol. Sits inside of PPP's authentication protocol and provides a generalized framework for several different authentication methods. EAP is used to pass the authentication information between the supplicant (the wireless workstation) and the authentication server. The actual authentication is defined and handled by the EAP type. The access point acting as authenticator is only a proxy to allow the supplicant and the authentication server to communicate.

encryption: The use of an algorithm to convert typically sensitive data into a form that is unreadable except by authorized users. See also Communications Channel Encryption.

endpoint: Any network device that connects to the enterprise network and runs network-based applications. Network devices can include laptops, desktop computers, servers, and PDAs. See also access point.

F

filtering logs: Viewing selected information from logged information. For example, a filter can be set up so that you can view only blocked traffic, critical information, or logged events occurring during the past day. See also logs.

firewall: Hardware, software, or a combination of both that is used to prevent unauthorized Internet users from accessing a private network. All information entering or leaving a network must pass through a firewall, which examines the information packets and blocks those that do not meet security criteria. The Sygate Security Agent Allows or Blocks whether incoming traffic is allowed to access an organization's network or resources. By using firewall rules, an Agent can systematically allow and block incoming traffic from specific IP addresses and ports. See also firewall rule, Sygate Security Agent.

firewall rule: A stipulation that helps determine whether or not a computer can gain access to a network. For example, a firewall rule may state "Port 80 is allowed."

G

groups: All users and computers on an enterprise network are organized into groups with similar security needs and settings. Computer and Users Groups are created and maintained by a system administrator on the Sygate Management Server. A group cannot be edited unless it is locked or checked-out first making it so only one administrator can make changes to it at any time. See also Computer Group, Users Group, Global Group.

GUID: Global Unique Identifier. See unique ID.

H

hijack: A type of attack where an intruder takes control of an existing communication session between a server and a legitimate user who has connected and authenticated with the server. The intruder can monitor the session passively recording the transfer of sensitive information such as passwords and code. Another type of hijacking involves an active attack done by forcing the user offline (with a Denial of Service attack) and taking over the session. The intruder begins acting like the user, executing commands, and sending information to the server.

HP Sygate Security Agent: See Sygate Security Agent.

I

ICMP: See Internet Control Message Protocol (ICMP).

icon: A small visual image displayed on a computer screen to represent an application, a command, an object, or to indicate status. On the Sygate Management Server, icons show when Agents are online and represent groups, users, and computers. Icons shown on screens in Sygate software are also used to display status. For example, in the Sygate Secure Agent interface, blinking blue lights indicate incoming and outgoing traffic.

IDS: See Intrusion Detection System (IDS).

inbound traffic: Traffic that was initiated from a remote computer. See also outbound traffic.

inheritance: A way of implementing security policies, which include rules and settings, across groups and subgroups of users and computers. Security policies can be created globally so that they filter down to all subgroups. Traits that can be inherited include Simple and Advanced Rules, IDS rules, Host Integrity rules, locations (except default locations, which are not inherited), and group settings. See also rule inheritance.

initialization files: Each component of Sygate Secure Enterprise includes an initialization file that allows for the component to be configured prior to its installation. For example, ServerSettings.xml is the initialization file for a Sygate Management Server. This file defines aspects of server administration including the default log server, port numbers, administrator console timeout, encrypted web console communication, and console access. Other initialization files are SetAid.ini (for Agent installation settings and AutoLocation method) and SyLink.xml (specifying Agent administrative details such as client vs. server control and server connections).

Internet Control Message Protocol (ICMP): An Internet protocol (defined in RFC 792) that is primarily for reporting errors in TCP/IP messages and exchanging limited status and control information.

Internet Information Services (IIS): Web services software from Microsoft that is the Hypertext Transport Protocol (HTTP) server for the Microsoft Windows platform. Microsoft IIS is required on the Sygate Management Server in order for Sygate Management Server to be installed successfully.

Intrusion Detection System (IDS): A device or software that detects and notifies a user or enterprise of unauthorized or anomalous access to a network or computer system. Sygate's IDS operates on every machine in an enterprise on which the Sygate Security Agent is installed by analyzing network packets targeted at the network node and comparing them with signature database entries. An IDS helps identify attacks and probes by monitoring traffic for attack signatures that represent hostile activity. See also Intrusion Prevention System (IPS).

Intrusion Prevention System (IPS): A device or software used to prevent intruders from accessing systems from malicious or suspicious activity. This is contrast to an Intrusion Detection System (IDS), which merely detects and notifies. Sygate Security Agent is both an IDS and an IPS product since the Agent includes both an IDS and firewall functionality making it capable of not only detecting but also blocking an attack. See also Intrusion Detection System (IDS).

IP address: A 32-bit address used to identify a node on a network. Each node on the network must be assigned a unique address in dotted decimal notation, such as 125.132.42.7. See also local IP address, remote IP address.

IP fragmentation: A packet that has been split into two or more packets. The Sygate Security Agent supports IP fragmentation, the ability to receive or send incomplete packets over the network. See also packets, Fragmented Packets.

IP spoofing: IP spoofing is a process where an intruder uses an IP address of another computer to acquire information or gain access. Because the intruder appears to be someone else, if a reply is sent, it goes to the spoofed address, not the intruder's address. See also Anti-IP Spoofing.

IPS: See Intrusion Prevention System (IPS).

L

LDAP: See Lightweight Directory Access Protocol (LDAP).

library: See signature library, System Library, custom library.

Lightweight Directory Access Protocol (LDAP): A standard directory access protocol for searching and updating information directories containing, for example, email addresses, phone numbers, and computer names and addresses. LDAP is the primary protocol used to access directory servers such as Active Directory. See also Active Directory, directory server.

local IP address: From the perspective of the Agent, the IP address of the computer the user is working on. See also IP address.

local port: From the perspective of the Sygate Security Agent, the port on the computer being used for this connection. See also port.

Location: A set of rules and regulations called a security policy that the Sygate Management Server sends to each Sygate Security Agent whenever the Agent sends a request to the Management Server. Location is defined by the network settings of the computer where the request was initiated. See also network settings.

logs: Files that store information generated by an application, service, or operating system. The information is used to track the operations performed. Sygate Secure Enterprise provides extensive logging capabilities that track events such as security violations, changes to security policies, network traffic, client connections, and administrator activities.

M

MAC address: A vendor's Media Access Control hardware address that identifies computers, servers, routers, or other network devices. See also Anti-MAC Spoofing.

MAC Spoofing: Intruders use a technique called MAC (media access control) spoofing to hack into a victim's computer by using the MAC address of another computer to send an ARP (Address Resolution Protocol) response packet to the victim even though the victim did not send an ARP request. The victim host renews the internal ARP table using the malicious ARP response packet. See also Anti-MAC Spoofing.

multicast: Sending a message simultaneously to more than one destination on a network. See also broadcast, unicast.

N

NetBIOS protection: An option on the Management Server that blocks all communication from computers located outside a client's local subnet range. NetBIOS traffic is blocked on UDP ports 88, 137, and 138 and TCP ports 135, 139, 445, and 1026. See also subnet.

network adapter: A device that connects a computer to a network.

network interface card (NIC): A device that is installed in a computer that provides the ability to communicate with other connected devices on the network.

network settings: Settings that determine the Location of an Agent attempting to gain access to the network. Network settings can check by MAC or IP address, DNS server IP address, WINS Server IP address, IP range, Sygate Management Server connection, and type of connection (VPN or dial-up networking). They are used for AutoLocation switching. See also AutoLocation Switching.

ntoskrnl.exe: NT Kernel & System, a standard Windows service that initializes the kernel and drivers needed during a session.

O

OS Fingerprint Masquerading: An option that keeps programs from detecting the operating system of a computer running the Agent. When OS Fingerprint Masquerading is enabled, the Agent modifies TCP/IP packets so it is not possible to determine its operating system.

outbound traffic: Traffic that was initiated from the local computer. See also inbound traffic.

P

packet: A unit of data sent over a network. It is accompanied by a packet header that includes information, such as the message length, priority, checksum, and the source and destination address. When packets are sent over a network protected by Sygate Secure Enterprise, each packet is evaluated for specific patterns that indicate known attacks. If a match occurs, the attack is blocked. See also Fragmented Packets.

policy: See security policy.

port: A connection on a computer where devices that pass data to and from the computer are physically connected. Ports are numbered from 0 to 65535. Ports 0 to 1024 are reserved for use by certain privileged services. See also Authentication port, local port, remote port, source port.

port scan: A method that hackers use to determine which computer's ports are open to communication. It is done by sending messages to computer ports to locate points of vulnerability. Although it can be a precursor to an intrusion attempt, port scanning does not in itself provide access to a remote system. See also Portscan Checking.

portscan checking: An option that monitors all incoming packets that are blocked by any security rule. If several different packets were blocked on different ports in a short period of time, a security log entry is generated. Portscan checking does not block any packets. A security policy needs to be created to block traffic in the event that a port scan occurs.

priority: The order in which rules take effect. Rules with a higher priority (0 being highest, 15 being lowest) take effect before rules with lower priority. Simple rules, by default, have a priority of 10. Advanced Rules, by default, have a priority of 5.

profile: See security policy.

Profile Serial Number: A number that the Policy Editor automatically generates every time an Agent's security policy changes. A system administrator can check the serial number on the Help|About menu of the Agent to verify that an Agent is running an up-to-date security policy.

protocol driver blocking: A security measure that blocks malicious applications from using their own protocol driver to exit the network surreptitiously.

R

remote IP address: The IP address of the computer to which information is being transmitted.

remote port: A port on another computer attempting to transmit information over a network connection.

rule: See Advanced Rule, firewall rule, Simple Rule.

Running Applications list: Located below the traffic flow graphs; a list of all applications and services that are currently accessing (or attempting to access) an Agent's network connection. The status of the applications is also displayed.

S

Schedule: An Advanced Rule that allows for triggering an event at certain times of the day.

security alerts: A sound or notification indicating that the Agent has detected an attack against the client computer.

security policy: A combination of all the security rules and settings that have been applied to a specific group to protect an enterprise's computing integrity. Security policies can include rules concerning the permitted applications, connection type, VPN, Ethernet, wireless, and any other restrictions or specifications that an organization wants to enforce.

service: A network port, a UDP port, an IP protocol type, or an ICMP type.

severity: A mechanism for the Agent logging system that indicates how critical an event is. Severity ranges from 0 to 15, where 0 is the most critical and 15 is least critical.

signature: A rule that defines how to identify an intrusion. Sygate's Intrusion Detection System identifies known attacks by pattern-matching against rules or 'signatures' stored in the System Library or a custom library. See also signature library, System Library.

signature library: A set of IDS signatures. Sygate provides a library of known signatures in the System Library, which can be kept up-to-date by downloading the latest version from the Sygate Technologies web site to your Sygate Management Server. Administrators can also specify new attack signatures of their own choosing in custom libraries. See also System Library.

silent mode: The ability to hide the Sygate Security Agent user interface from the end user.

simple rule: A type of firewall rule that enables a system administrator to create security rules without having to define priorities, severities, triggers, and events. Examples of simple rules could be a rule that allows trusted applications, a rule that allows hosts, a rule that allows VPNs, etc. Simple rules have a default priority of 10, where 0 is the highest and 15 is the lowest priority. The names of simple rules begin with "Srg". See also Advanced Rule.

Smart DHCP: Allows a Dynamic Host Configuration Protocol (DHCP) client to receive an IP address from a DHCP server while protecting the client against DHCP attacks from a network. If a Sygate Security Agent sends a DHCP request to a DHCP server, it waits for five seconds to allow for an incoming DHCP response. If a Sygate Security Agent does not send a DHCP request to a DHCP server, then Smart DHCP does not allow the packet. Smart DHCP does not block packets. It simply allows the packet if a DHCP request was made. Any other DHCP blocking or allowing is done by the normal security rule set. See also Dynamic Host Configuration Protocol (DHCP).

Smart DNS: Allows a Domain Name System (DNS) client to resolve a domain name from a DNS server while providing protection against DNS attacks from the network. This option blocks all Domain Name System (DNS) traffic except outgoing DNS requests and the corresponding reply. If a client computer sends a DNS request and another computer responds within five seconds, the communication is allowed. All other DNS packets are dropped. Smart DNS does not block any packets; blocking is done by the normal security rule set.

Smart WINS: Allows Windows Internet Naming Service (WINS) requests only if they have been requested. If the traffic is not requested, the WINS reply is blocked.

sniffing: The process of actively capturing datagram and packet information from a selected network. Sniffing acquires all network traffic regardless of where the packets are addressed.

source IP address: The IP address from which the traffic originated. See also IP address.

source port: The port number on which the traffic originated. See also port.

spoofing: A technique used by an intruder to gain unauthorized network access to a computer system or network by forging known network credentials. IP spoofing is a common method for intruders to gain unauthorized network access to a computer systems or network.

Stealth Mode Browsing: An option that detects all HTTP traffic on port 80 from a web browser and removes information such as the browser name and version, the operating system, and the reference web page. It stops web sites from knowing which operating system and browser you are using. Stealth Mode Browsing may cause some web sites not to function properly because it removes the browser signature, called the HTTP_USER_AGENT, from the HTTP request header and replaces it with a generic signature.

subnet: Portions of a TCP/IP network used to increase the bandwidth on the network by subdividing the network into portions or segments. All IP addresses within a subnet use the same first three sets of numbers (such as 192.168.1 in 192.168.1.180 and 192.168.1.170) indicating they are on the same network. A subnet is See also subnet mask.

subnet mask: A value that allows a network to be subdivided and provides for more complex address assignments. The subnet mask format is nnn.nnn.nnn.nnn, such as 255.255.255.0.

sweeping: The process that Sygate uses to eliminate old log files on the database. See also logs.

Sygate Security Agent: Software component that enforces rule-based security on devices, whether remote or behind a corporate firewall, using security policies defined using the Policy Editor. Also referred to as the Agent in Sygate documentation. The Agent must be installed on every device before it can connect to the enterprise network. The Agent can detect, identify, and block known Trojans and Denial of Service attacks, and also protects against new or unknown attacks by blocking applications and traffic that violates a defined set of security policies. Port scans are also detected and logged to alert users and system administrators of potential attacks, while maintaining system security.

synchronization: Refers to automatically keeping directory servers up-to-date with the user database including synchronizing between LDAP, Active Directory, and NT Domain. System administrators can specify how often to synchronize the user database with the directory server. See also Active Directory, Lightweight Directory Access Protocol (LDAP).

System Library: A Sygate library containing preconfigured IDS signatures to help detect and prevent known attacks. System administrators can use the System Library or create custom IDS signatures to be included in custom IDS signature libraries on the Sygate Management Server. The System Library is shown using a blue icon in the interface. Sygate periodically posts an updated System Library for download on the Sygate web site. See also custom library, signature library.

system tray: The lower right section of the taskbar on the Windows desktop that displays a clock and icons representing certain programs, such as volume control, network connection status, and antivirus software. The Agent icons can appear on their respective computers.

T

Transmission Control Protocol/Internet Protocol (TCP/IP): Internet protocols that every Internet user and every Internet server uses to communicate and transfer data over networks. TCP packages data into packets that are sent over the Internet and are reassembled at their destinations. IP handles the addressing and routing of each data packet so it is sent to the correct destination.

trigger: An event that causes a rule to take effect. When creating rules, you can assign specific triggers, which cause Agents to react in a specific way, and actions, which specify what to do when the trigger takes place. For example, you can block all traffic originating from a certain IP address or block traffic during certain hours of the day. Triggers can be linked to specific applications, hosts, schedules, and services.

Trojan, Trojan horse: An application that carries out an unauthorized function covertly while running an authorized application. It is designed to do something other than what it claims to and frequently is destructive in its actions. The Sygate Security Agent automatically detects and terminates known Trojan horse applications before a Trojan horse attempts to communicate.

trusted application: An application that is allowed to run on a Sygate Secure Agent.

trusted IP address: An IP address permitted access the enterprise network without running the Sygate Security Agent. See also IP address.

U

UDP: See User Datagram Protocol (UDP).

unicast: Sending a message to one specific computer. See also broadcast, multicast.

unique ID: A 128-bit hexadecimal number, also called the GUID, assigned to uniquely identify a client running Agent software.

User Datagram Protocol (UDP): A communications protocol for the Internet network layer, transport layer, and session layer that uses the Internet Protocol (IP) when sending a datagram message from one computer to another. UDP does not guarantee reliable communication or provide validated sequencing of the packets.

V

virtual private network (VPN): A secure network connection that connects different corporate network sites, allows remote users to connect to an enterprise network, and allows controlled access to different corporate networks. Although a VPN provides a secure tunnel for network traffic, it leaves connection points open to attack. Working with a corporate VPN server, Sygate Enforcer ensures that only computers running a valid security policy of the Sygate Security Agent can gain access to an enterprise network through a VPN. See also VPN enforcement.

virus: A program that is designed to spread from computer to computer on its own, potentially damaging the system software by corrupting or erasing data, using available memory, or by annoying the user by altering data. A virus is designed to replicate. Generally, it is spread by infecting other files.

VPN enforcement: A way to verify that VPN users are running the Sygate Security Agent and meet the security requirements before being granted access to the network. See also enforcement, virtual private network (VPN).

vulnerability scan: An attempt to use security attacks to detect security weaknesses in a computer. The Sygate Security Agent includes a Test button that assesses an Agent's vulnerability to attack. It requires a public IP address. See also port scan.

W

WINS: Short for Windows Internet Naming Service, a system that determines the IP address associated with a particular network computer. This is called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. Determining the IP address for a computer is a complex process when DHCP servers assign IP addresses dynamically. For example, it is possible for DHCP to assign a different IP address to a client each time a computer logs into the network. WINS uses a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.

worm: A type of computer virus that can replicate itself over a computer network and perform destructive tasks such as using up computer memory resources. Worms do not infect other files as viruses typically do, but instead worms make copies of themselves over and over depleting system resources (hard drive space) or depleting bandwidth (by spreading over shared network resources). See also virus.

Index

S

T