HP Sygate Security Agent: Frequently Asked Questions

Question and Answers

This paper provides answers to commonly asked questions about the HP Sygate Security Agent.

Overview

Q: What is HP delivering in the factory image?

A: The image contains the following: HP Sygate Security Agent.

Q: What is the free functionality?

A: Once installed, HP Sygate Security Agent provides a customizable firewall that helps protect your computer 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 the use of various networking services, applications, ports, and components.

HP Sygate Standalone Agent has the ability to allow or block any port or protocol, inbound or outbound, by either application or traffic signature. The Agent not only blocks according to these parameters, but can also link them with logical and/or conditional statements, increasing the scope and flexibility of polices that can be applied. The Agent can also block and apply policy to custom protocol adapters, enabling enterprises to use custom network-enabled applications and to block applications that circumvent the TCP/IP stack with custom protocol adapters.

Firewall Questions

Q: What approach has HP taken to secure my thin client?

A: In addition to following strict security-centric image design policies, HP also provides Sygate Firewall software on all new t5710 thin clients with Windows XPe SP2 preinstalled. HP also provides Windows XPe SP2 as a Web deliverable for existing t5700 and t5710 thin clients, which provides end-users with restricted firewall control and administrators with full agent access privileges to the agent software.

Q: How is HP Sygate Security Agent different than Microsoft Windows Firewall?

A: HP Sygate Security Agent is a stateful or dynamic firewall while the Microsoft Windows Firewall is primarily static. A stateful firewall can selectively enable a specific port for outbound traffic for a specific application and it can dynamically react and allow incoming traffic on that port to reach the application with outbound rights. A static firewall would enable the port and any application could use it. A stateful firewall is a lot more secure.

HP Sygate Security Agent is a much more feature-rich software package which gives you more tools to provide a secure environment. As a stateful firewall, Sygate provides the ability to define inbound ports specific to an application which offers administrators additional control over network traffic. HP Sygate Security Agent also has the ability to define which application has outbound access to the network.

Q: What is the difference between a whitelist and a blacklist approach?

A: In a "whitelist" environment, all network traffic is blocked with the exception of listed programs. A "blacklist" environment allows all traffic except that which is known to be harmful.

HP will be implementing a port-level locked-down whitelist. The following table compares the advantages of the whitelist and blacklist policies:

Policy	Advantages	Disadvantages
Blacklist Firewall Policy	• Building and managing a firewall policy can normally be a time-consuming and frustrating process for both the administrators and the users. A firewall with a default blacklist can be installed without first defining a security policy for access through the firewall. • With a default blacklist policy, it is possible to quickly install a firewall without a significant amount of upfront security competency required by the installers.	• It is more prone to allow undesired behavior and security policy violations, such as reverse-tunnels, trojans, worms and similar attacks. • It is difficult to switch from a default blacklist to a whitelist model.
Whitelist Firewall Policy	• Greater security because unknown services and network activity is not allowed by default. This minimizes the effectiveness of trojans, viruses and worms. • It is easy to switch a default whitelist firewall to a blacklist firewall.	• Installing a whitelist firewall takes more up-front time, because the list of what is to be allowed through the firewall must be determined before it is installed and functional. • Managing a whitelist firewall policy is more time consuming in a network with actively changing needs and demands. • It can be a greater frustration to the users, because they have to to request access to services, rather than having access by default.

Q: What viruses, worms or vulnerabilities will HP Sygate Security Agent block?

A: Both Microsoft Windows Firewall and HP Sygate Security Agent would have prevented worm attacks like Blaster and Sasser; however, only HP Sygate Security Agent has the ability to help stop propagation to other systems.

Assessing your vulnerability to an attack is one of the most important steps that you can take to ensure that your system is protected from possible intruders. The information from this assessment can help you set the various options on your Agent to protect your system from attack. The Sygate Online Services (SOS) scanner scans your computer and attempts to determine your IP address, operating system, Web browser, and other information about your system.

You can then choose one of the following more focused scans.

- Quick Scan: 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 Scan: 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 Scan: 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 Sygate Web site.
- TCP Scan: 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.
- UDP Scan: 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 Scan: 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.

Q: How do I use the SOS scanner?

A: To perform the SOS scan, log in as an administrator and perform the following steps:

1. Launch the HP Sygate Security Agent GUI by doubleclicking the Sygate icon.
2. Select Tools > Test Your System Security. This automatically launches Internet Explorer and links to SOS at **http://scan.sygate.com**.
3. From the Sygate site, select the tests you wish to perform.

Q: Which inbound and outbound ports has HP allowed?

A: For detailed information on ports, please see the following tables:

Remote Ports

Application	Executable	Allowed UDP Ports	Allowed TCP Ports
Internet Explorer	c:\program files\Internet Explorer\iexplore.exe		20,21,22,80, 443, 8080, 8000
Media Player 9	c:\program files\Windows Media Player\wmplayer.exe		20,21,22,80, 443, 8080, 8000
Remote Desktop	c:\windows\system32\mstsc.exe		3360-4020
Windows Messenger	c:\program files\messenger\msmsgs.exe	1900, 6801, 6901	1863, 6901, 8080,80,443,8000, 6801
Altiris	c:\program files\altiris\aclient\ACLIENT.exe	All	All
Citrix MetaFrame	c:\program files\citrix\ica client\wfica32.exe, pn.exe, wfcrun32.exe	1604, 1494	2598, 1494, 80, 8080,8000,443, 2512, 2513
NTOSKRNL	c:\windows\system32\ntoskrnl.exe	53, 67, 68, 137, 138	
TeemNT	c:\program files\teemNT\TeemNT.exe	23	23, 515
FTP	c:\windows\system32\ftp.exe, c:\program files\Internet Explorer\iexplore.exe		20,21,22,80, 443, 8080, 8000
NDISUIO	c:\windows\system32\drivers\ndisuio.sys	53, 67, 68, 137, 138	
TCPIP6	c:\windows\system32\drivers\tcpip6.sys	53, 67, 68, 137, 138	
TCPIP	c:\windows\system32\drivers\tcpip.sys	53, 67, 68, 137, 138	
IPX Driver	c:\windows\system32\drivers\nwlnkipx.sys	53, 67, 68, 137, 138	
SVCHost UDP	c:\windows\system32\svchost.exe	53, 123, 389	

Application	Executable	Allowed UDP Ports	Allowed TCP Ports
Windows Time Service	c:\windows\system32\svchost.exe, ntoskrnl.exe	123	
LPD / LPR Printing	c:\windows\system32\spoolsv.exe		515
LSASS	c:\windows\system32\lsass.exe	53, 123, 389	1025-1030
SNMP	c:\windows\system32\snmp.exe	1029	
SVCHost TCP	c:\windows\system32\svchost.exe		389, 1025-1030
VPN Support	c:\windows\system32.ntoskrnl.exe	1723	
Microsoft Management Console	c:\windows\system32\mmc.exe		389, 1025-1030
RDP Clipboard Function	c:\windows\system32\mstsc.exe	1024-4900	

Local Ports

Application	Executable	Allowed UDP Ports	Allowed TCP Ports
SVCHost TCP	c:\windows\system32\svchost.exe		3360-4020
RDP Clip	c:\windows\system32\rdpclip.exe	1000-2000	

Q: What is the HP Sygate Policy Editor and what does it do?

A: The editor is an administrator-only tool. It runs on a Microsoft Windows PC, not on a thin client. HP Sygate Policy Editor allows the administrator to customize the security rules for the clients.

Q: Where do I obtain the HP Sygate Policy Editor?

A: The HP Sygate Policy Editor is delivered in standard Softpaq format.

Q: Is there a fee associated with the HP Sygate Policy Editor?

A: No, the HP Sygate Policy Editor is provided to all customers at no charge.

Q: Who do I contact for technical support on the HP Sygate Policy Editor?

A: For HP and Compaq products, call 800-HP Invent (800-474-6836).

Q: How do I modify the ports against the applications already specified by HP?

A: To modify the default HP security configuration, you must download the HP Sygate Policy Editor. This file includes documentation on how to customize the default security policy.

Q: Is there a limitation to which ports and/or applications that can be added?

A: No. By using the HP Sygate Policy Editor the policy can be configured to specifically fit your network environment.

Q: What if my application uses a range of ports?

A: You can easily allow a range or set of ports when creating a rule with the provided HP Sygate Policy Editor.

Q: Can I or do I need to specify whether my application uses UDP or TCP?

A: Though it is not required when creating a rule, narrowing down a given application to a specific type of traffic is ideal in a secure network environment. Sygate supports individual blocking of TCP, UDP, ICMP or all protocols for inbound or outbound traffic.

Q: Is there a risk to opening all ports for an application?

A: Yes. Although only the application specified in a rule may use the given port range, the more ports available to a given application, the less secure it becomes.

Q: Is there a limit to the number of rules I can add?

A: There is currently no limit to the number of rules that can be created.

Q: Is there a list of well-known ports and their respective applications?

A: A list of common port assignments is available on the Web at http://www.iana.org/assignments/port-numbers. In addition, you can use freeware tool port scanners to determine which ports are in use on the system and what applications are using ports.

Log Files

Q: How do I view the log files while at the thin client?

A: A log viewer is built into the Sygate Agent on every system. To access this functionality, log in as Administrator and right-click the Sygate icon in your system tray. From this screen, select Logs.

Q: How do I retrieve the log files remotely?

A: Log files can only be saved to the local default location. Currently there is no means of remotely storing log files to a network share.

Q: What does the log file reveal?

A: HP Sygate Security Agent includes four different log files:

- Security log: This log tracks any security-related events that may occur. DOS attacks and ports scans against the machine are examples of these events.
- Traffic log: This log tracks all network traffic into and out of the thin client machine. Ports, IP addresses, and applications are tracked here.
- System Log: This log tracks system events such as the Sygate loading errors or various system errors.
- Packet log: This log, though disabled by default, is a much more detailed version of the traffic log. It is best enabled and used for troubleshooting purposes.

Q: How do I know that a port or application has been blocked?

A: When an application tries to access the network and is blocked, the user will see a pop-up message in the lower right corner of the screen. Clicking on this message will open the log viewer and point to the entry detailing the blocked traffic.

Q: What should I do when an application is blocked?

A: Contact your network administrator. In some cases, you will receive warnings about traffic that was intentionally blocked. If the blocked traffic is causing a loss of functionality, a change to your default policy may have to be made using the Policy Editor.

Intrusion Detection

Q: What is the functionality of an Intrusion Detection System (IDS)?

A: An IDS detects and identifies known Trojans, port scans, and other common attacks, and selectively enables or blocks the use of various networking services, ports, and components.

The agent also provides deep packet inspection, further enhanced intrusion detection and prevention capabilities, including alerts when another user attempts to compromise your system. The end result is a system that analyzes network packets and compares them with known attacks and known behavioral patterns of attack, and then intelligently blocks the malicious attacks.

The latest IDS signatures are available with the purchase of the HP Compaq t5710 thin client and continued operating system image updates. However, this will not protect you from the latest threats. This protection is only available through the subscription service in which you will have available the latest signature updates as specific industry threats arise.

Q: How do I obtain the latest IDS signatures?

A: HP will deliver IDS signatures through a subscription service. See next question.

Q: How do I deploy new or modified policies with Altiris?

A: To deploy new or modified policies to terminals, perform the following:

- See question "How do I modify the ports against the applications already specified by HP?" to make policy updates.
- See question "Are there best practices for automating deployment?" for instructions on deploying the updates.
- See question "How do I make IDS files persistent?" for instructions on retaining policy updates across reboots.

Q: How do I deploy software updates with Altiris?

A: To deploy software updates, follow the instructions included in Softpaqs delivered via the subscription service. To set up the subscription service, perform the following steps:

1. Visit **http://www.hp.com**.
2. Select Online shopping.
3. Select HP Software store.
4. Select the Software category.
5. Select Sygate subscription service.
6. Fill in the necessary information.
7. Download software.

The subscription provides Sygate agent updates with Altiris scripts for deployment, enhancements to the whitelist, updates to IDS and a copy of the user guide.

Q: Are there best practices for automating deployment?

A: Example scripts for Altiris remote deployment are available as a Softpaq for the general public with the Policy Editor. The subscription provides Sygate agent updates with Altiris scripts for deployment, enhancements to the whitelist, updates to IDS and a copy of the user guide.

Q: How do I make IDS files persistent?

A: Using the script with the IDS Softpaq will allow the administrator to make IDS files persistent. To manually configure the files, the administrator must disable the enhanced write filter (EWF). For additional information about the EWF, please refer to the Using the Enhanced Write Filter at:

http://h200005.www2.hp.com/bc/docs/support/SupportManual/c00101105/c00101105.pdf

For more information

For additional HP Compaq t5000 thin clients information, please refer to the following:

http://h18004.www1.hp.com/products/thinclients/index_t5000.html

382993-001, 1/2005