HP Sygate Security Agent and Symantec Embedded Security: Frequently Asked Questions

Question and answers 2
Overview 2
Firewall questions 4
Log files 9
Intrusion detection 10
For more information 10

Question and answers

This paper provides answers to commonly asked questions about the HP Sygate Security Agent and the Symantec Embedded Security subscription service. Currently, the firewall in Symantec Embedded Security is the same as in the HP Sygate Security Agent.

Overview

Q: Are thin clients susceptible to viruses or worms?

A: Server Based Computing with HP Compaq Thin Clients is, by nature, less susceptible to virus and worm attack than a PC with Windows XP Professional. When compared to the traditional unmanaged PC network model, the HP thin client computing model yields a less vulnerable, segregated approach to computing with substantially better recovery time, while minimizing total cost of ownership (TCO).

1. With the HP thin client computing model, your exposure to virus attack on the thin client system is less than a standard Windows PC. See the white paper titled "Thin Client Virus Vulnerability Analysis" at **http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00595181/c00595181.pdf** for more information.
2. The HP thin client computing model utilizes PC blades and/or servers located in the data center. You can protect and monitor these centralized devices more easily with centrally managed virus and firewall tools. Compromised resources can be quickly taken offline, or recovered faster and more cheaply than distributed PC resources.
3. Since no user data resides on the thin client, there is no risk of user data loss due to a virus or worm on the thin client.
4. If a thin client's image is compromised or corrupted, the recovery time is typically measured in minutes instead of hours. You can often perform recovery with a simple reboot of the client.

Additionally, HP follows strict security-centric image design policies and uses the Enhanced Write Filter to provides a more secure environment for thin-client computing. The Enhanced Write Filter protects the thin client from undesired flash memory writes (the operating system and functional software components reside in flash memory). If a thin client does become infected by a virus, a simple reboot cycle clears the system RAM and returns the client to its original state from the protected Flash memory.

HP believes the thin client computing model is an effective solution for the security conscious enterprise. However, the Windows XP Embedded operating system may have vulnerabilities that can be exploited by the increasingly sophisticated attacks on business networks. To provide further protection for our customers, HP has partnered with Symantec to deliver industry leading protection from worms, trojans and viruses.

Q: What does HP deliver in the factory image?

A: The image contains the HP Sygate Security Agent.

Q: What is the free functionality?

A: The 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 you can apply. 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.

Q: How can I get signature updates for the Sygate firewall to ensure protection from the latest threats?

A: Symantec Embedded Security (HP Part Number EL390AA) is available as a subscription service. Symantec acquired Sygate and has integrated the Sygate firewall into Symantec Embedded Security. Purchasing the Symantec Embedded Security subscription provides a full year of updates to the firewall, and additionally provides integrated anti-virus technology, a requirement in many business IT environments. HP offers leading firewall and antivirus technology from an industry leader: Symantec Embedded Security.

Q: How can I obtain antivirus support for my thin clients?

A: Symantec Embedded Security (HP Part Number EL390AA) is available as a one year, renewable, subscription service. With both antivirus and firewall protection, the Symantec Embedded Security agent provides an industry-leading level of protection for thin clients with Microsoft's XP embedded operating system. Symantec acquired Sygate and has integrated the Sygate firewall into Symantec Embedded Security. Purchasing the Symantec Embedded Security subscription provides a full year of updates to the firewall, and additionally provides integrated anti-virus technology, a requirement in many business IT environments. HP offers leading firewall and antivirus technology from an industry leader: Symantec Embedded Security.

Q: How do I buy Symantec Embedded Security?

A: Symantec Embedded Security (HP Part Number EL390AA) is available direct from HP, or your local and online resellers. Once purchased, HP will mail you a letter with information on how to download the latest versions of the Symantec Embedded Security and updates for the antivirus and firewall components.

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 provides Sygate Firewall software on all new t57x0 series thin clients with Windows XPe SP2 preinstalled. HP provides Windows XPe SP2 as a Web deliverable for existing t57x0 series thin clients, which provides end-users with restricted firewall control and administrators with full agent access privileges to the agent software.

Q: How is the 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 then any application could use it. A stateful firewall is more secure. HP Sygate Security Agent is a much more feature-rich software package that 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: The HP Sygate Security Agent uses a "whitelist" approach. In a whitelist environment, only network traffic for known, listed programs is allowed. A blacklist environment allows all traffic except what is known to be harmful. HP knows every program it installs on its thin clients; therefore, you only update additions you make to HP thin clients.

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 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 up-front 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 only known services and network activities are allowed by default. This minimizes the effectiveness of trojans, viruses, and worms that use unknown, unlisted programs. • It is easy to switch a default whitelist firewall to a blacklist firewall. • Installing a whitelist firewall takes more up-front time, because you must determine the list of what to allow through the firewall 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 frustrating to users because they have 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 prevent worm attacks such as Blaster and Sasser; however, only HP Sygate Security Agent has the ability to help stop propagation to other systems due to the whitelist approach which allows only known, listed programs to access the network.

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: Encompasses several scanning processes to perform a brief, general scan. It usually takes 20 seconds or less to accurately scan your devices ports, protocols, services, and possible Trojans. It records the results in the Agent Security Log.
- Stealth Scan: Uses specialized stealthing techniques that 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: Scans all of a 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: 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 malicious hackers can exploit.
- 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: Scans a user's device and 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. Double-click the Sygate icon to launch the HP Sygate Security Agent GUI.
2. Select **Tools > Test Your System Security** to automatically launch Internet Explorer and links to SOS at **http://scan.sygate.com.**
3. From the Sygate site, select the tests you want to perform.

Q: Which inbound and outbound ports has HP allowed?

A: The following table provides detailed information about ports:

Inbound/outbound port table

Application	TCP ports allowed	UDP ports allowed
Remote ports		
NT Kernel & System (ntoskrnl.exe)	1723	53, 67, 68, 123, 137, 138
NDIS User Mode I/O Driver (ndisuio.sys)		53, 67, 68, 123, 137, 138
TCP/IP Protocol Driver (tcpip.sys)		53, 67, 68, 123, 137, 138
IPv6 Driver (tcpip6.sys)		53, 67, 68, 123, 137, 138
NWLINK2 IPX Protocol Driver (nwlnkipx.sys)		53, 67, 68, 123, 137, 138
Internet Explorer (iexplore.exe)	20, 21, 22, 80, 443, 8080, 8000	
Windows Media Player (wmplayer.exe)	20, 21, 22, 80, 443, 8080, 8000	
FTP Application (ftp.exe)	20, 21, 22, 80, 443, 8080, 8000	
Remote Desktop Application (mstsc.exe)	1380, 3360 - 4020	1024 - 4900

Inbound/outbound port table		
Application	**TCP ports allowed**	**UDP ports allowed**
Remote Desktop Clip Board Monitor (rdpclip.exe)		1000 - 2000
Windows Messenger (msmsgs.exe)	1863, 6901, 8080, 8000, 80, 443, 6801	1900, 6801, 6901
Altiris (aclient.exe, aclntusr.exe)	All	All
All		402
Citrix Metaframe (wfica32.exe, pn.exe)	2598, 1494. 80, 8080, 8000, 443, 2512, 2513	1604, 1494
TeemNT (teemnt.exe)	23, 515	
Generic Host Process for Win32 Services (svchost.exe)	389, 1025 - 1030	53, 123, 389
Microsoft Management Console (mmc.exe)	389, 1025 - 1030	
Windows NT Logon Application (winlogon.exe)	389, 1025 - 1030	
LSA Shell (lsass.exe)	1025 - 1030	53, 123, 389
Spooler Subsystem App (spoolsv.exe)	515	
SNMP Service (snmp.exe)		1029
Microsoft HTML Help Executable (hh.exe)	80	
XP Prep System Tool (xpeprep.exe)	21, 1000 - 5000	
Local ports		
All		402
Generic Host Process for Win32 Services (svchost.exe)	3360 - 4020	
Protocols		
ICMP (0, 3, 8)		
IGMP IP Type 2		

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

A: An administrator-only tool that 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 available on the HP Help and Support Web site 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 HP default Sygate security settings on a single thin client:

1. Log on as Administrator.
2. Right-click on the Sygate systray icon.
3. Select **Advanced Rules**.

To modify security settings on multiple units, download the HP Sygate Policy Editor from the HP Service and Support Web site and follow the included instructions.

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

A: No. By using the HP Sygate Policy Editor, you can configure a policy 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 you can create.

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 which 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,

1. Log in as Administrator.
2. Right-click the Sygate icon in the system tray.
3. Select **Logs**.

Q: How do I retrieve the log files remotely?

A: You can save log files only to the local default location. You cannot currently remotely store 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: Tracks any security-related events that may occur. DOS attacks and port scans are examples of these events.
- Traffic log: Tracks all network traffic into and out of the thin client. Ports, IP addresses, and applications are tracked here.
- System log: Tracks system events such as the Sygate loading errors or various system errors.
- Packet log: Provides a much more detailed version of the traffic log. This log is disabled by default and 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. Click on this message to open the log viewer, and then 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 causes a loss of functionality, you may need to change your default policy 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.

Q: How do I deploy modified policies with Altiris?

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

- See question "How do I modify the ports against the applications already specified by HP?" on page 8 to make policy updates.
- See question "Are there best practices for automating deployment?" on page 10 for instructions on deploying the updates.
- See question "How do I make IDS files persistent?" on page 10 for instructions on retaining policy updates across reboots.

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.

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 white paper at:

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00101105/c00101105.pdf

For more information

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

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

382993-003, 3/2006