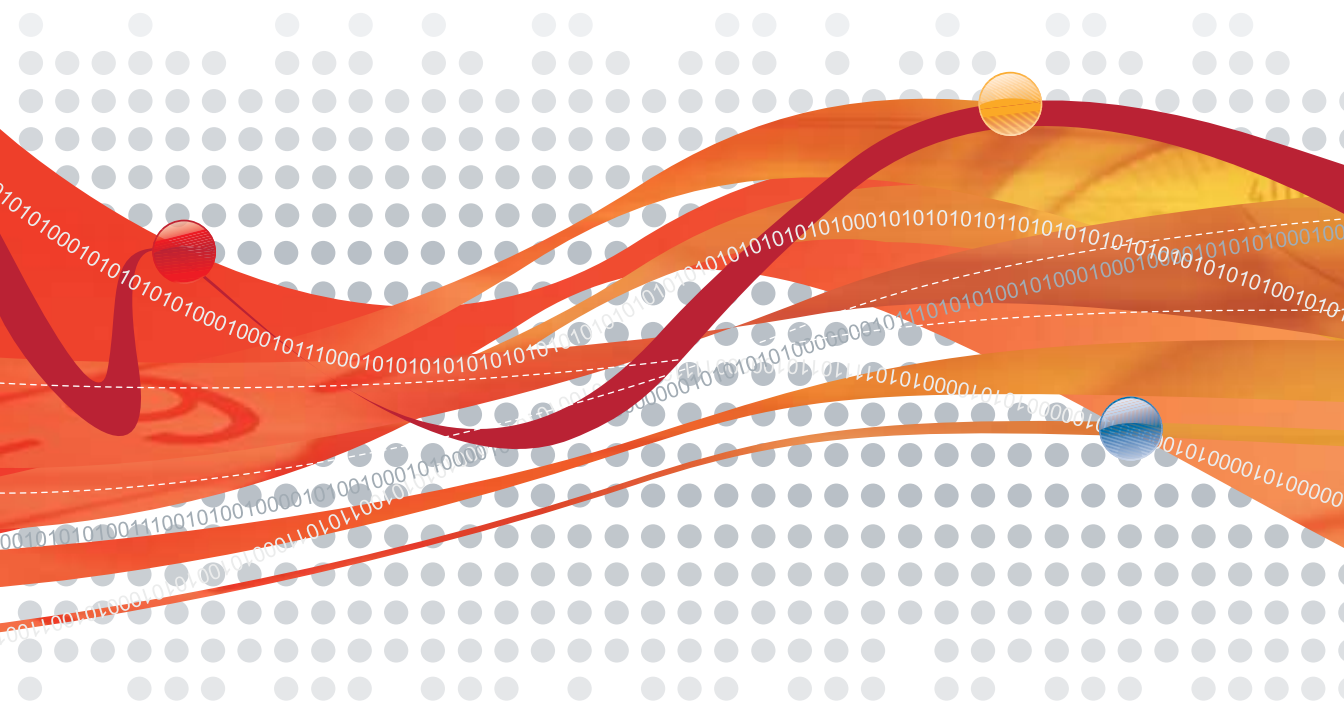
TREND MICRO™

InterScan™ Web Security Suite 3

Antivirus and Content Security at the Web Gateway

for Solaris™

Installation Guide



Web Security

Release Date: March 2009

Protected by U.S. Patent No. 5,951,698

The Installation Guide for Trend Micro™ InterScan™ Web Security Suite is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

For technical support, please refer to the Technical Support and Troubleshooting chapter for technical support information and contact details. Detailed information about how to use specific features within the software is available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents

Appendix E: Maintenance and Technical Support

Index

Preface

Welcome to the *Trend Micro™ InterScan Web Security Suite 3.1 Installation Guide*. This guide helps you to get "up and running" by introducing InterScan Web Security Suite (IWSS), assisting with deployment, installation, migration (if necessary), initial configuration, troubleshooting, performance tuning, and main post-installation configuration tasks. It also includes instructions on testing your installation using a harmless test virus, troubleshooting, and accessing Support.

This preface discusses the following topics:

Audience

The IWSS documentation is written for system administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of networks schemas, including details related to the following:

- HTTP and FTP protocols
- Database configuration

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

InterScan Web Security Suite Documentation

In addition to the *Trend Micro™ InterScan Web Security Suite 3.1 Installation Guide*, the documentation set includes the following:

- **Administrator's Guide**—this guide provides detailed information about all InterScan Web Security Suite configuration options. Topics include how to update your software to keep protection current against the latest risks, how to configure and use policies to support your security objectives, and using logs and reports.
- **Readme file**—the Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and release history.

  The latest versions of the Installation Guide, Administrator's Guide, and readme file are available in electronic form at:

  `http://www.trendmicro.com/download/`

- **Online help**—Helps you configure all features through the user interface. You can access the online help by opening the Web console and then clicking the help icon.

  The purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online help is accessible from the InterScan Web Security Suite management console.

- **Knowledge Base**—the Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  http://esupport.trendmicro.com/support

- **TrendEdge**—a program for Trend Micro employees, partners, and other interested parties that provides information on unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics.

  http://trendedge.trendmicro.com

The Administrator's Guide and readme are available on the InterScan Web Security Suite CD and at http://www.trendmicro.com/download.

Document Conventions

To help you locate and interpret information easily, the InterScan Web Security Suite documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Pre-installation Planning

This chapter explains the following:

Server Requirements

Operating System

- Sun Solaris 9 with Entire Distribution
- Sun Solaris 10 with Entire Distribution

Note: Trend Micro recommends applying the latest patch for your operating system.

Hardware Requirements

Minimum Requirements

- CPU: Dual Sun™ Ultra SPARC™ III processor 900MHz
- Memory: 2GB RAM
- Disk space:
  - 2GB free disk space for program files
  - 20GB free disk space for data storage. However, more disk space might be needed depending on the amount of logs needed to store
  - Swap space: 8GB free disk space for swap files. Swap space must be four times the amount of physical memory.

Recommended Requirements

- CPU: Sun™ Ultra SPARC™ T1 v9 processor 1.0 GHz or above
- Memory: 4GB RAM or more
- Disk space:
  - 2GB free disk space for program files
  - 40GB free disk space or more for data storage. However, more disk space might be needed depending on the amount of logs needed to store
  - Swap space: A maximum of 16GB free disk space for swap files. Swap space must be four times the amount of physical memory.

Note: Please see your local support representative to obtain the IWSS 3.1 Solaris Sizing Guide for details on the appropriate hardware for your environment.

IWSS does not support Zone (Container) and LDoms.

Web Browser

To access the HTTP-based Web console, using any of the browsers in table Table 1-1.

TABLE 1-1. Supported Web Browsers for Administrator Web Console Access

Browser	Windows			UNIX
	2003	XP SP2	Vista	Solaris
IE 6.0	X	X		
IE 7.0	X	X	X	
Firefox 2.0		X	X	X
Firefox 3.0		X	X	

TABLE 1-2. Supported Web Browsers for End User Internet Access

Application	Windows			Mac
	2003	XP SP2	Vista	OS X
IE 6.0	X	X		
IE 7.0	X	X	X	
Firefox 2.0		X	X	
Firefox 3.0		X	X	
Safari 2.0				X
Safari 3.0				X

Service Ports

The following ports are related to main services of IWSS3.1 Solaris. Please ensure that these ports are not in-use before install IWSS3.1 Solaris.

TABLE 1-3. Required Service Ports

Port Number	Description
8080	HTTP daemon for HTTP proxy mode
21	FTP daemon
1812	IWSS Web console
161	SNMP service
5432	PostgreSQL database (if you want to install PostgreSQL server v7.4.18 that comes with the IWSS setup package)

Note: The IWSS installation script checks the availability of these service ports before installation and displays a warning message if any of these ports are already used by another service.

Instant Messaging Applications

The following table lists the Instant Messaging (IM) applications IWSS supports:

TABLE 1-4. Supported Instant Messaging Applications

Application	Windows			Mac
	2003	XP SP2	Vista	OS X
ICQ	X	X	X	
Windows Live Messenger	X	X	X	
Google Talk	X	X	X	X

Other Requirements

- **Database requirements:**
  - PostgreSQL v7.4.18 (included)
  - When using multiple IWSS servers in a server farm configuration, Trend Micro recommends that you use separate server (possibly clustered) for PostgreSQL
- **Internet Content Adaptation Protocol (ICAP):**
  - NetApp™ NetCache™ release 6.0.1
  - Blue Coat Systems™ SGOS v5 (latest version)
  - Cisco ICAP servers: CE version 5.3
  - Any cache server that is ICAP 1.0 compliant
- **Directory Servers:**

  To configure policies based on Lightweight Directory Access Protocol (LDAP) users and groups, IWSS can integrate with the following LDAP directories:
  - Microsoft Active Directory 2000 and 2003
  - Linux OpenLDAP Directory 2.2.17 and 2.3.39
  - Sun™ Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)

Further Requirements

- Administrator or Domain Administrator access to the server machine
- IWSS clients must be able to access the HTTP port of the IWSS server that is selected during the install
- IWSS server must be able to communicate via the client communication port selected during the install to all IWSS clients
- IWSS server and IWSS clients must be able to perform ICMP echo / reply sequences - either using the DNS name or IP address depending on the server selected during the install

Information Needed to Install IWSS

You can either purchase IWSS or download a 30-day trial version of IWSS. The 30-day trial versions provides all the functionality of IWSS.

The IWSS setup program prompts you for required information, depending on the options chosen during installation.

Type of Proxy Configuration

The most common proxy configuration is to install IWSS as a forward proxy to protect clients from risks they might download from the Internet. Clients will have to modify their Internet connection settings to use the IWSS server as its proxy, unless you enable transparency. However, enabling transparency limits the user identification method to IP address and/or hostname and may make some FTP links inaccessible.

Another installation scenario is to configure IWSS as a reverse proxy, to protect a Web server from having malicious content uploaded to it. For more information, see *Planning the HTTP Flow* on page 1-12 and *Planning FTP Flows* on page 1-26.

Control Manager Server Information

If you plan to register IWSS with an existing Control Manager server on the network, you need to know the server's host name or IP address and its logon name. IWSS supports Control Manager 3.5 and Control Manager 5.0.

Database Type and Location

IWSS uses the PostgreSQL database for report logs, policies, rules and configuration settings. Install an instance of PostgreSQL unless you already have an existing instance.

SNMP Notifications

IWSS sends notifications in response to many security risk detections, policy violations or program events. The setup program prompts for the email address to

send notifications, and an SMTP server that allows message relay from the IWSS server.

Web Console Password

Access to the IWSS Web console is controlled through a password (the default is **adminIWSS85**).

Proxy for Internet Updates

If you have a proxy between IWSS and the Internet, enter the proxy's host name or IP address, port and an account.

Activation Codes

Activating the three IWSS modules (core program, URL Filtering, and Applet and ActiveX Scanning) requires three separate activation codes. IWSS usually comes with registration keys for the modules purchased. During product registration, the Registration Keys are exchanged for Activation Codes that "unlock" the program. You can register and obtain activation codes before installing by visiting Trend Micro's online registration Web site at:

`http://olr.trendmicro.com.`

Fresh Install or Migration

To install IWSS as a fresh install or to migrate from IWSS 2.2 to the current version of IWSS, run the `./install_iwss.sh` script. See Chapter 3, *Installing IWSS* or Chapter 4, *Migrating to IWSS 3.1*.

Planning Network Traffic Protection

To enforce the network traffic protection using IWSS, an additional solution (hardware, software or configuration) must be introduced that redirects the HTTP and/or FTP traffic to IWSS. Those solution include:

- See *Reconfiguring Client Settings* on page 1-8
- See *Using a Layer 4 Switch* on page 1-9
- See *Using an ICAP-enabled Proxy* on page 1-10

Reconfiguring Client Settings

HTTP clients (browser or proxy servers) can be configured to contact IWSS as a proxy. This configuration ensures that the FTP-over-HTTP traffic is forwarded to IWSS. The HTTP scanning service must be installed in the HTTP Proxy mode to process this traffic.

Set the following parameters in the [http] section of the pni file:

- `transparency= no` Disables transparent mode
- `self_proxy= (yes|no)` Depends on the traffic delivery requirements

FTP clients must contact IWSS instead of the destination server, and use a modified handshake to supply the FTP server address. The FTP scanning module must be installed and configured in standalone mode (`proxy_mode=standalone`) to process this traffic.

TABLE A-5. Reconfiguring the Client Settings

Advantage	Limitation
No additional hardware required	Administrator have to control settings for all computers. (Guest computers can have difficulties.)

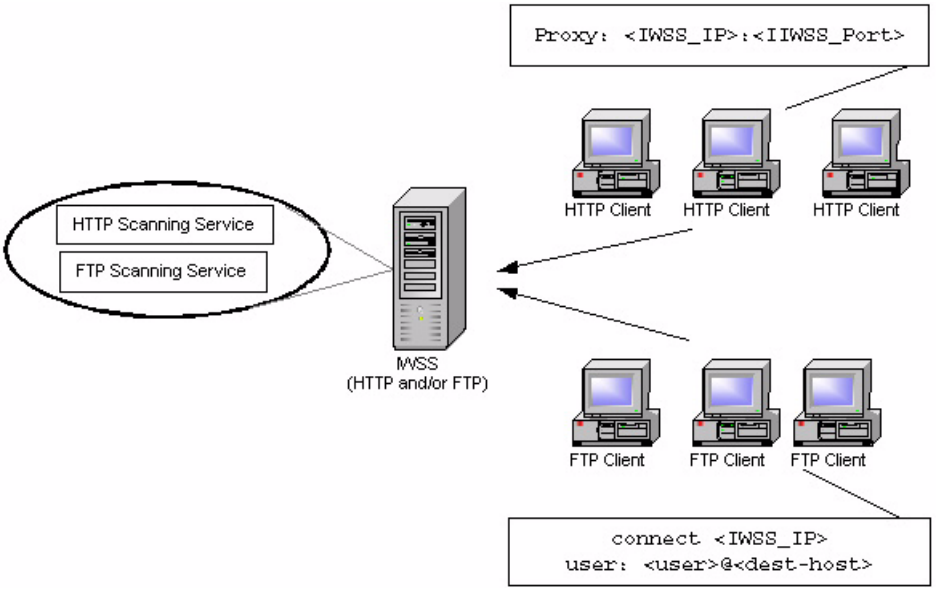


FIGURE A-1 Reconfiguring the Client Settings

Using a Layer 4 Switch

A Layer 4 switch can be used to redirect HTTP traffic to IWSS. The HTTP Scanning Service must be installed in the HTTP Proxy mode.

Set the following parameters in the [http] section of the pni file:

- `transparency=simple` enables simple transparent mode
- `self_proxy yes|no` based on traffic delivery requirements

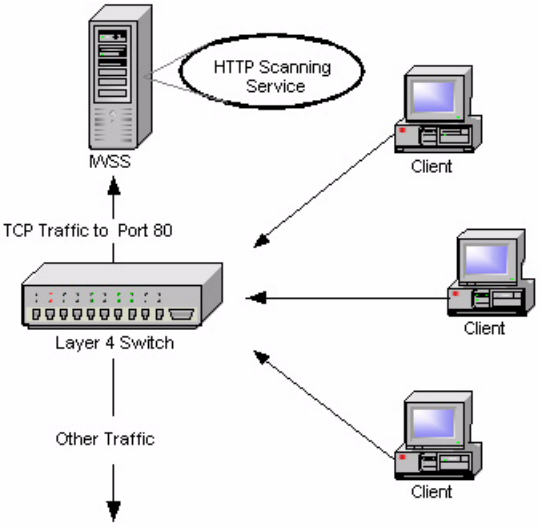


FIGURE A-2 Using a Layer 4 Switch

TABLE A-6. Using a Layer 4 Switch

Advantages	Limitations
Transparent to clients	Traffic interception must be port based (not protocol based) for one port. If the non-standard port is used for HTTP, it bypasses the switch.
Simple to establish	The switch-based redirection cannot be used for the FTP traffic.
	No LDAP support

Using an ICAP-enabled Proxy

Internet Content Adaptation Protocol (ICAP) is designed to forward HTTP response/request to third-party processors and collect the result. The component that

sends the ICAP request is called the ICAP-client. A component that processes the request is called an ICAP-server.

When IWSS is configured in ICAP mode, it processes requests from any ICAP-compliant client. Officially, Trend supports the following ICAP implementations: NetCache, Blue Coat, and Cisco Content Engines (CE).

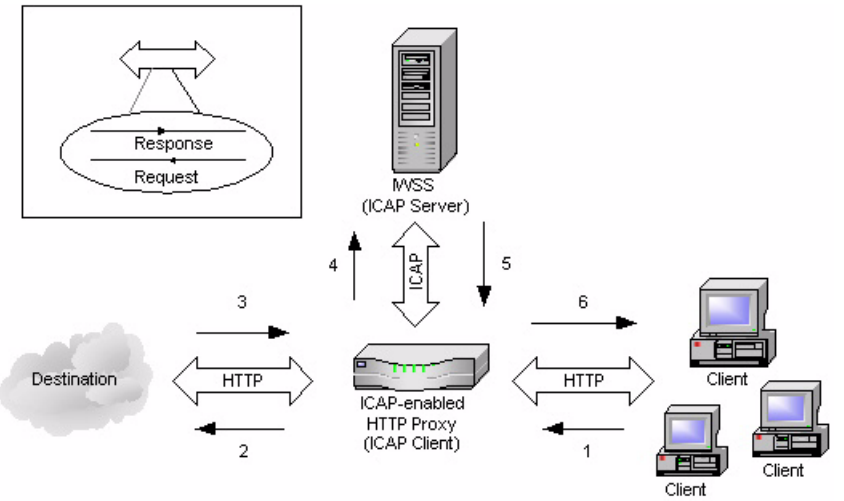


FIGURE A-3 Using an ICAP-enabled Proxy

TABLE A-7. Using am ICAP-enabled Proxy

Advantages	Limitations
ICAP allows scanning of only new and necessary content.	Up front coast of ICAP resources
Reduced, selective scanning enhances performance	Adds extra step in IWSS installation process
Increased resource efficiency reduces the number of IWSS server hardware needed	Requires management.

Planning HTTP and FTP Service Flows

Each HTTP and FTP configuration has implications for configuring IWSS, configuring the network, and for network security.

Create a flow plan for the HTTP and FTP services by doing the following:

- Understand each IWSS services purpose and function
- Determine each service's valid data sources. For example, does the HTTP service receive requests directly from the HTTP browsers, or indirectly through an ICAP proxy device?
- Determine which ports to use for the service. For instance, by default, the HTTP service uses port 8080, and the FTP service uses port 21. However, if another application or service is using port 8080, the administrator must configure the HTTP service to use a different port.
- Determine each services valid data destinations. For example, does the HTTP service send validated requests directly to the Web site? Or, does the HTTP service send the validated request to an upstream HTTP proxy?
- Add in any service-specific considerations. For instance, the HTTP service flow might include an ICAP device, but the FTP service flow does not.

Using the information gathered above, administrators determine which one of the possible flows to use for the installation.

Planning the HTTP Flow

The first step when planning HTTP flow for IWSS is choosing the type of handler:

- HTTP Proxy
- ICAP device

The flow involving an ICAP device is very different from those that do not involve ICAP devices.

There are five main possible flows:

For Forward Proxy Settings:

- **Standalone mode**—Use this flow when ICAP devices are not being used with IWSS, and IWSS connects directly to the Internet. This is the default flow created during installation.

- **Dependent mode**—Use this flow when ICAP devices are not being used with IWSS, and IWSS cannot connect directly to the Internet, but must instead connect through another HTTP proxy. This is can be accomplished in two ways:
  - Proxy-ahead mode
  - Proxy-behind mode (not recommended)
  - Double-proxy mode
- **Transparent proxy mode** - Use this mode when clients computers are not configured to use the IWSS server as their default gateway, but still need to connect to the Internet through IWSS

For reverse proxy settings:

- **Reverse proxy mode—**Use this flow to protect a Web server with a proxy server by placing the HTTP proxy between the Internet and the Web server. (Used by ISPs and ASPs to protect the upload traffic against viruses and by organizations with complex Web sites that need a centralized point of access control.)

For ICAP proxy settings:

- **ICAP protocol mode**—Use the ICAP protocol flow to use ICAP devices with IWSS

Each configuration has implications for configuring IWSS, configuring the network, and for network security.

HTTP Proxy in Standalone Mode

The simplest configuration is to install IWSS in stand-alone mode, with no upstream proxy. In this case, IWSS acts as a proxy server for the clients. Advantages of this configuration are its relative simplicity and that there is no need for a separate proxy server. A drawback of a forward proxy in stand-alone mode is that each client must configure the InterScan Web Security Suite device as their proxy server in their browser's Internet connection settings. This requires cooperation from your network users, and also makes it possible for users to exempt themselves from your organization's security policies by re-configuring their Internet connection settings.

Note: If you configure IWSS to work in stand-alone mode, each client on your network needs to configure Internet connection settings to use the IWSS device and port (default 8080) as their proxy server.

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP service.
2. The HTTP service validates the request, if the URL is not blocked. If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction. If the URL is valid, the HTTP service attempts to connect to the applicable Web server.
3. The contacted Web site returns a response from the Web server to the HTTP service.
4. The HTTP service scans the content for unwanted data and returns the appropriate response to the client.

TABLE A-8. HTTP Proxy in Standalone Mode

Advantage	Limitation
Simple to install and manage	Slow connection reaches maximum allowed connections limit.

Stand-alone Mode with Multiple Servers

Multiple IWSS servers can be installed to balance your network traffic and scanning load. In this installation example, a Layer 4 switch receives clients requests and then forwards them to the IWSS servers.

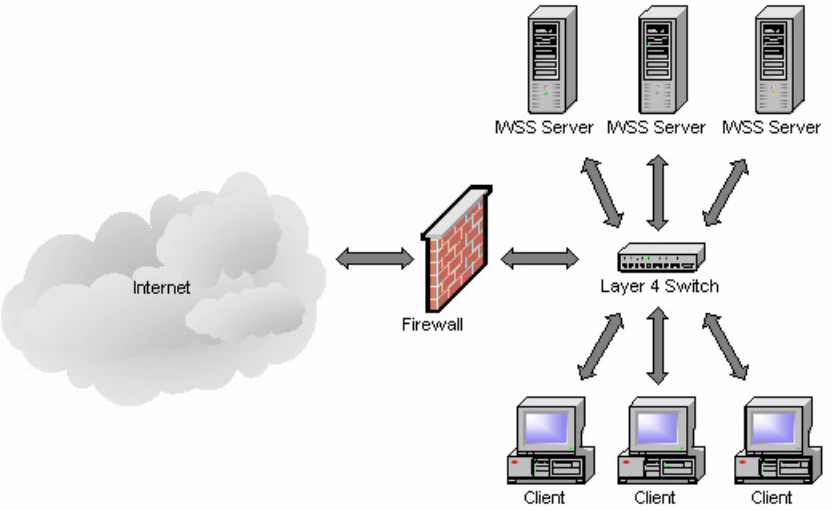


FIGURE A-4 Use a Layer 4 switch to load balance between IWSS servers for multiple HTTP stand-alone servers

HTTP Proxy in Dependent Mode (Proxy Ahead)

For HTTP browsers to use this flow, configure the browsers to proxy through the IWSS server, by default at port 8080.

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP service.
2. The HTTP service validates the request.
   - If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to an upstream HTTP proxy server.
3. The upstream proxy server performs its processing, then forwards the request to the Web site on the Internet

4. The contacted Web site returns a response (ideally a Web page) to the HTTP proxy server.
5. The HTTP proxy server performs its processing on the returned data, then forwards the response data to the IWSS HTTP service.
6. The HTTP service scans the content for unwanted data and returns an appropriate response to the HTTP client.

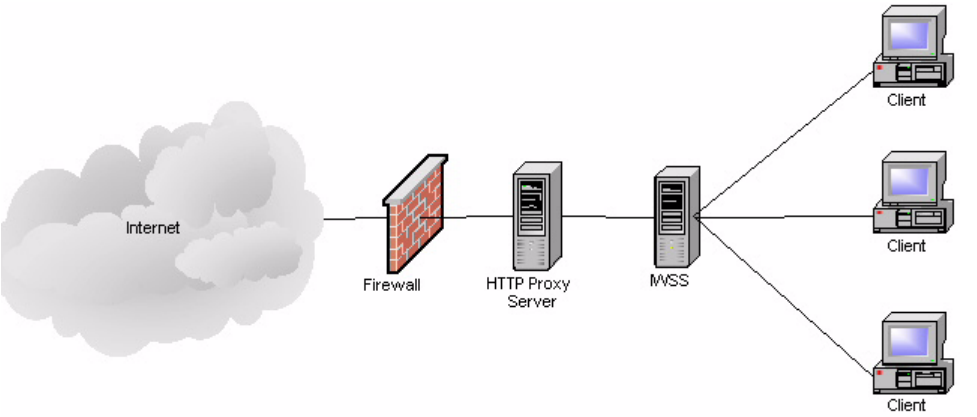


FIGURE A-5 HTTP Proxy in Dependent Mode (Proxy Ahead)

TABLE A-9. HTTP Proxy in Dependent Mode (Proxy Ahead)

Advantages	Limitations
Proxy server controls timing and content availability behavior	IWSS has to scan every response-even if cached.
It is more secure-configuration changes will affect cached objects.	
IWSS does not wait for download of already cached objects.	

HTTP Proxy in Dependent Mode (Proxy Behind)

The proxy behind flow consists of a caching proxy placed between the HTTP client and the IWSS server without using ICAP. Organizations typically use this flow to increase performance, as with ICAP.

WARNING! *Two security trade-offs exist for this potential performance enhancement:*
1. If the cache contains data with a virus, for which there was no pattern when the data hit the cache, the IWSS HTTP service is powerless to prevent the spread of the virus.
2. 2.Similarly, if a policy regarding valid content changes, or unauthorized users request data that exists in the cache (for authorized users), the HTTP service is powerless to prevent subsequent unauthorized access to this data.

Instead of using the proxy-behind flow, Trend Micro recommends that administrators use an ICAP caching device. This solution provides the performance enhancements of caching without the security issues of proxy-behind topology.

Web page requests follow this sequence:

1. The Web client sends a request to HTTP proxy server.
2. The proxy server forwards the request to IWSS.
3. IWSS validates the request using URL Filtering/Blocking.
   - If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to the Web server on the internet.
4. The contacted Web server returns a response (ideally a Web page) to IWSS.
5. IWSS performs its processing on the returned data (virus, spyware, ActiveX scanning), then forwards the appropriate response/data to Proxy server.
6. The Proxy server caches the data (if cacheable), then delivers the response/data to the HTTP client.

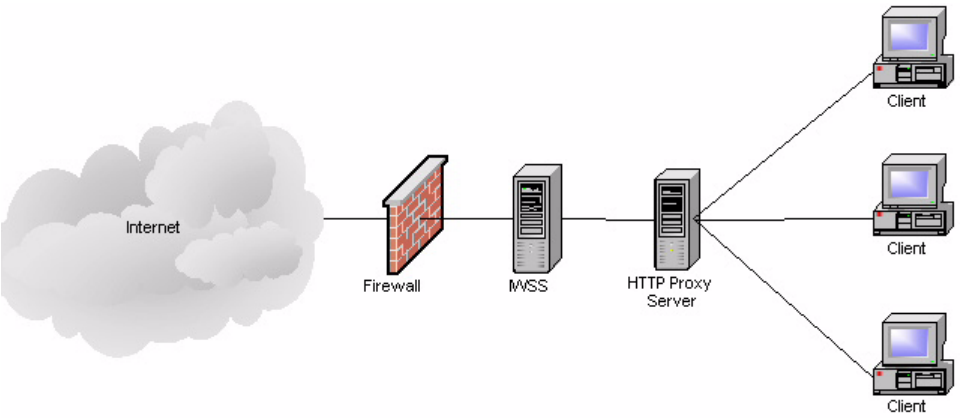


FIGURE A-6 HTTP Proxy in Dependent Mode (Proxy Behind)

TABLE A-10. HTTP Proxy in Dependent Mode (Proxy Behind)

Advantages	Limitations
No configuration changes required on the clients	Configuration changes on IWSS affect cached objects
Cached objects are downloaded by clients directly from the Proxy server, which minimizes delays	

HTTP Double Proxy in Dependent Mode

Double proxy configuration requires two caching proxies. The first proxy is placed between the HTTP client and the IWSS server, and other one is placed between the IWSS server and the Internet. This is typically used to get the advantages of the two configurations of Dependent Mode: Proxy-ahead and Proxy-behind.

Web page request follows this sequence:

1. The Web client sends a request to first proxy server.
2. The first proxy server forwards the request to IWSS.

3. IWSS validates the request using URL Filtering/Blocking.
   - If the URL is invalid (blocked) the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to the second proxy server.
4. The second proxy server performs its processing, then forwards the request to the Web server on the internet.
5. The contacted Web server returns a response (ideally a Web page) to second proxy server.
6. The second proxy server caches the data (if cacheable), then deliver the response/data to IWSS.
7. IWSS performs its processing on the returned data (Virus, Spyware, ActiveX scanning), then forwards the appropriate response/data to first proxy server.
8. The first proxy server caches the data (if cacheable), then delivers the response/data to the HTTP client.

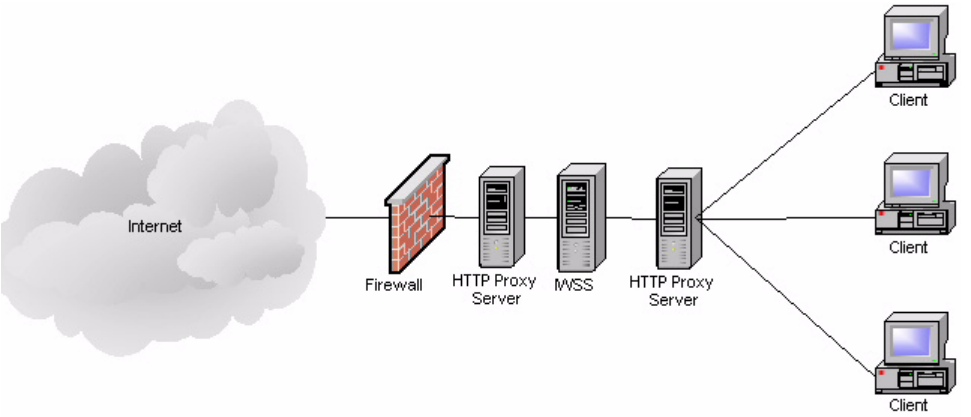


FIGURE A-7 HTTP Double Proxy in Dependent Mode

TABLE A-11. HTTP Double Proxy in Dependent Mode

Advantages	Limitations
Proxy server controls timing and content availability behavior	Costs more-- additional proxy server is needed
It is more secure-configuration changes will affect cached objects	
IWSS does not wait for download of already cached objects	
No configuration change required on the clients	

HTTP Proxy in Transparent Mode

Transparency is the functionality whereby client users do not need to change their Internet connection's proxy settings to work in conjunction with IWSS. Transparency is accomplished with a Layer 4 switch that redirects HTTP packets to a proxy server, which then forwards the packets to the requested server.

IWSS supports "simple" type transparency. Simple transparency is supported by most Layer 4 switches. While it is compatible with a wide variety of network hardware from different manufacturers, configuring simple transparency does impose several limitations:

- When using simple transparency, the User Identification method to define policies is limited to IP address and/or host name; configuring policies based on LDAP is not possible.
- FTP over HTTP is not available; thus, links to ftp:// URLs may not work if your firewall settings do not allow FTP connections. Alternatively, links to ftp:// URLs may work, but the files will not be scanned.
- Simple transparency is not compatible with some older Web browsers when their HTTP requests don't include information about the host.
- HTTP requests for servers that use a port other than the HTTP default port 80 are redirected to IWSS. This means SSL (HTTPS) requests are typically fulfilled, but the content is not scanned.
- Do not use any source NAT (IP masquerade) downstream of IWSS, since IWSS needs to know the IP address of the client to clean.

- A DNS server is needed for DCS to resolve the client machine name from its IP address in order to perform a cleanup.

The benefit of enabling transparency is that clients' HTTP requests can be processed and scanned by IWSS without any client configuration changes. This is more convenient for your end users, and prevents clients from exempting themselves from security policies by simply changing their Internet connection settings.

HTTP Reverse Proxy in Dependent Mode

In reverse proxy mode, IWSS protects a Web server with the proxy server. The HTTP proxy is placed between the Internet and the Web server. This is useful when the Web server accepts file uploads from clients, or to reduce the load of each Web server by balancing the load among multiple Web servers. ASPs/ISPs use IWSS as an HTTP proxy to protect the upload traffic against viruses, and organizations with complex Web sites need it as a centralized point of access control.

This flow is especially useful for Web sites involved in e-commerce transactions, distributed applications, which exchange data across the Internet, or other situations where clients upload files to the Web server from remote locations.

In reverse proxy mode, the HTTP proxy acts as the Web server to the client systems. The proxy receives all requests and transfers them to the real Web server. Consequently, all HTTP traffic goes through the HTTP proxy, enabling the proxy to scan to content and block any infected transactions.

Note: Administrators should be aware of the following:
1. The URL-filtering feature makes no sense in this configuration; only anti-virus scanning and URL-blocking are useful.
2. In reverse proxy mode, the Web server's access log is useless. To analyze the connections for the Web site, you must use the proxy's access log.
3. Ideally, the reverse proxy server should be placed behind a firewall, but in many cases, the proxy is connected directly to the Internet, where it is more vulnerable to direct attacks. When a reverse proxy is configured without a firewall, administrators should take all appropriate precautions in securing the operating system hosting IWSS

Web page requests follow this sequence:

1. Clients initiate Web request.

2. The request is received by InterScan Web Security Suite, configured to listen on port 80.
3. InterScan Web Security Suite scans the content, then forwards it to an actual Web server.
4. The Web server delivers the requested page back to IWSS.
5. InterScan Web Security Suite rewrites the page headers, and sends on the request.
6. The modified page returns to the requestor.

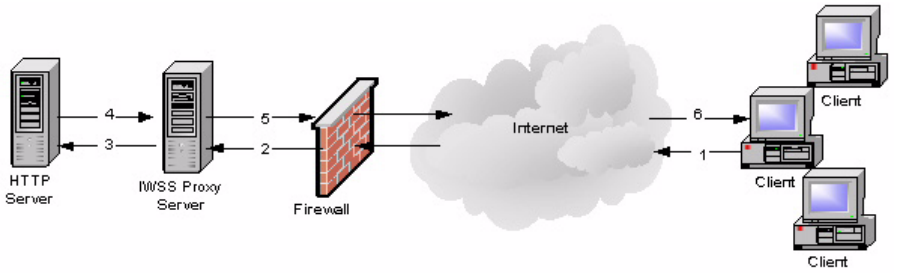


FIGURE A-8 HTTP Reverse Proxy in Dependent Mode

TABLE A-12. HTTP Reverse Proxy in Dependent Mode

Advantages	Limitations
IWSS scans all objects only once-before they are cached	New engine, pattern, and configurations will not affect cached objects.
	Access logging feature of IWSS is compromised.

HTTP Proxy in ICAP Mode (Single and Multiple IWSS Servers)

This section discusses the flow of a typical HTTP GET request using both an ICAP device and IWSS servers. In these flows, IWSS interacts with the ICAP device, in response to ICAP rules. This is very different from other flows where IWSS receives

URL requests form HTTP clients. To use these flows for HTTP browsers, configure the browsers to use the ICAP device as the HTTP proxy.

Using ICAP devices can enhance performance in two ways:

- **Caching good data**–If the data is clean, the ICAP device caches the data. Subsequent requests require only four steps, not eight. (ICAP must still ask IWSS to check the policies to validate that the users making the subsequent requests can browse the data, has not exceeded his or her quota, etc.)
- **Clustered IWSS servers**—When multiple IWSS servers are used, the ICAP device load balances the requests between the servers. This is vital for enterprise environments where the demand for scanning incoming pages can overwhelm a single IWSS server. With ICAP, the ICAP device performs load balancing, and receives maximum performance from the available IWSS servers.

Note: Non-ICAP environments can receive similar benefits by using multiple IWSS servers. However, the administrator must configure different users to proxy through the available IWSS servers and estimate how many and which clients to assign to each.

When IWSS is configured in ICAP mode, it processes requests from any ICAP-compliant client. Trend Micro supports the following ICAP client implementations:

- NetCache
- Blue Coat
- Cisco Content Engines

Although IWSS performs the same filtering of URLs and scanning of data for unwanted content, the ICAP flow is so different from the other flows that it requires a completely different communications protocol. Administrators indicate which protocol (ICAP or non-ICAP) to use during post-installation configuration.

The following figures show the HTTP flow with single and multiple IWSS servers. (Both images assume the requested data in not in the ICAP device's cache.) The ICAP service determines which IWSS server receives the request in a multi-server environment.

Web page requests follow this sequence:

1. An HTTP client makes a request for a URL, sending the request to the ICAP caching proxy device.
2. The ICAP device, based on its configuration, determines that the request must be forwarded to an IWSS server. If multiple servers are available, it alternates in round-robin fashion for load balancing.
3. The IWSS server validates the URL.
   - If the URL is not blocked, IWSS sends the response to the ICAP device.
   - If the URL is invalid (blocked), IWSS directs the ICAP device to send an appropriate response to the HTTP client and the transaction is complete.
4. If the URL is valid, the ICAP server requests the page from the Web site on the Internet.
5. The Web site on the Internet returns the requested page (or some other appropriate response).
6. If the page is returned, the ICAP device, based on its configuration, determines that an IWSS server must scan the data. Again, if multiple servers are available, it alternates in round-robin fashion for load balancing.
7. The IWSS server scans the results and returns an appropriate response to the ICAP device, based on whether the data is clean or contains unwanted content.
8. If the data is clean, the ICAP device returns said data to the HTTP client, and the ICAP device retains a copy of the data to satisfy future requests. If the data contains unwanted content, the ICAP device returns an appropriate error message (dictated by IWSS) to the HTTP client, and the ICAP device does not retain a copy for future requests.

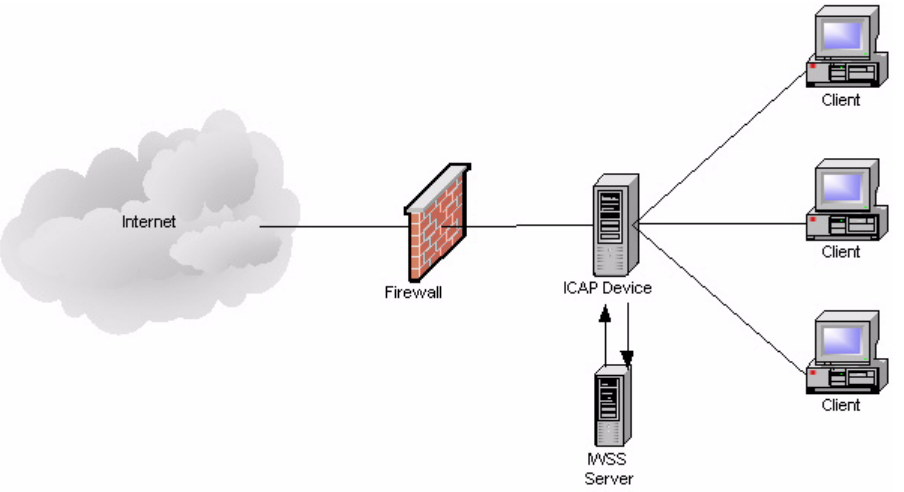


FIGURE A-9 HTTP Proxy in ICAP Mode (Single IWSS Server)

IWSS ICAP Mode with Multiple Servers

If there is already a content cache server on your network, then Trend Micro recommends installing the ICAP HTTP handler. The following diagram shows the installation topology for IWSS ICAP with multiple servers. For multiple IWSS ICAP servers to work properly, their corresponding pattern, scan engine version, and intscan.ini files must be identical, and all servers should connect to the same database.

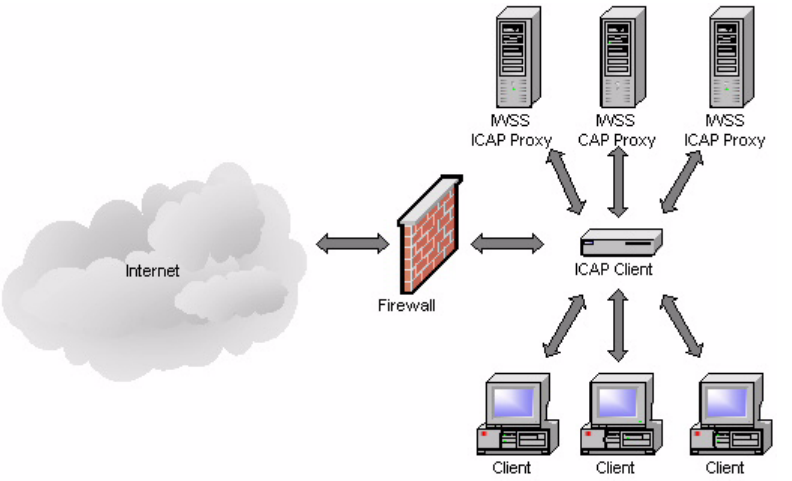


FIGURE A-10 HTTP Proxy in ICAP Mode (Multiple IWSS Servers)

TABLE A-13. HTTP Proxy in ICAP Mode

Advantages	Limitations
No configuration changes required on the clients	User identification on IWSS is not supported; thus, limited reporting
Cached objects are downloaded by clients directly from the Proxy server, which minimizes delays, and improves performance	Configuration changes on IWSS affect cached objects
Load-balancing possible after some configuration to the clients	

Planning FTP Flows

There are two possible FTP flows: standalone and dependent. They are similar to the stand-alone and dependent-mode flows for HTTP service. Each requires a different configuration and has its own implications including:

- **Stand-alone**—the IWSS server acts as an FTP proxy server between the requesting client and the remote site, brokering all transactions

- **Dependent**—IWSS works in conjunction with another FTP proxy server within a LAN

FTP Proxy in Standalone Mode

To scan all FTP traffic in and out of the LAN, set up the FTP scanning module so that it "brokers" all such connections. In this case, clients FTP to the IWSS server, supply the logon credentials to the target site, and then allow the IWSS FTP server to make the connection. The remote site transfers the files to IWSS FTP. Before delivering the files to the requesting clients, the IWSS FTP server scans the files for viruses and other security risks

The implications for the FTP standalone flow are:

- IWSS must have access to the target FTP servers
- There is one less step in the flow, compared to the FTP proxy mode

To configure FTP clients to use this flow:

- Set the IWSS server as a FTP proxy
- Set the user name to be `username@targetftp-server`, instead of the normal username

---

Note: IWSS FTP works with most firewalls, usually requiring only a modification to the firewall to open a port for the FTP proxy.

FTP requests follow this sequence:

1. The FTP client sends a request to the IWSS FTP service.
2. The IWSS FTP service validates the request (for example, the file type is not blocked). If the request is valid, the IWSS FTP service attempts to connect to the appropriate FTP server on the Internet. If the connection succeeds, the IWSS FTP service sends the request to the target FTP server.
3. The FTP server on the Internet responds to the request, ideally with the requested file.
4. The IWSS FTP service scans the returned data for unwanted content. If it finds any unwanted content, it returns an appropriate message to the FTP client. Otherwise, it returns the requested data to the FTP client.

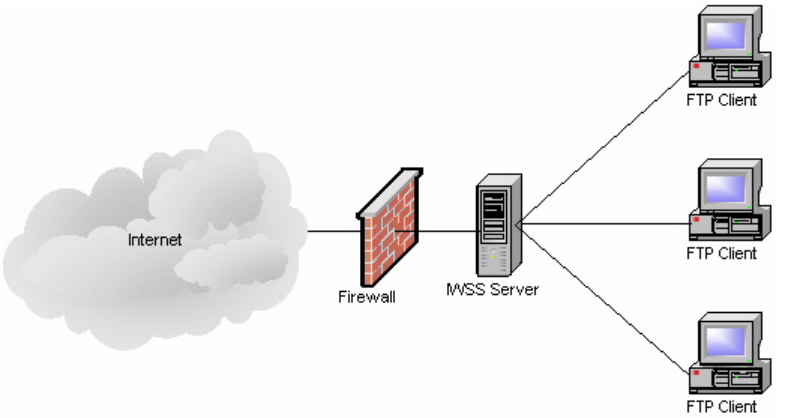


FIGURE A-11 FTP Proxy in Standalone Mode

FTP Proxy in Dependent Mode

You can also install IWSS FTP on a dedicated machine between an upstream proxy and the requesting clients. Use this setup adds other FTP features (for example, access blocking, logging, and filtering) to supplement the existing FTP proxy.

IWSS's FTP-proxy mode, shown in Figure A-12, is analogous to the dependent-mode flow of the HTTP service. Because it carries a performance penalty of an extra hop and extra processing by the other FTP proxy server, only use this mode if your organization does not allow the IWSS Server to access the Internet directly.

If the other FTP proxy server uses a store-and-forward technique, the performance penalty is more noticeable on large files because the other FTP proxy first downloads the file and passes it on to the IWSS FTP service. Additionally, the other FTP proxy must have sufficient free disk space to hold all transfers in progress.

Unlike the HTTP dependent-mode service, which has the possible benefit of cached requests, most FTP proxy servers do not cache requests.

FTP Dependent Mode also protects FTP servers from upload and download threats.

FTP requests follow this sequence:

1. The FTP client sends a request to the IWSS FTP service.

2. The IWSS FTP service validates the request (for example, the file type is not blocked). If the request is valid, the IWSS FTP service relays it to the other FTP proxy or the FTP server being protected by IWSS.
3. The FTP server on the Internet responds to the request, ideally with the requested file.
4. The IWSS FTP service scans the returned data for unwanted content. If it finds any unwanted content, it returns an appropriate message to the FTP client. Otherwise, it returns the requested data to the FTP client.

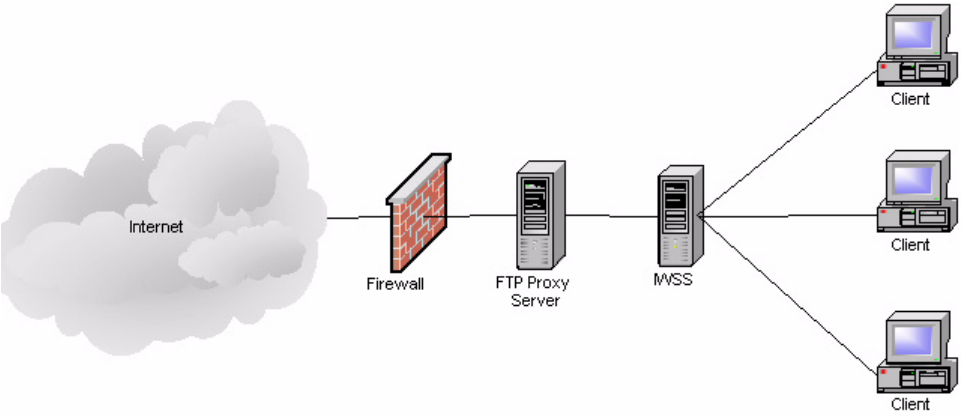


FIGURE A-12 FTP Proxy in Dependent Mode

Chapter 2

Deployment

This chapter explains the following:

Operating Mode

Unlike previous versions, InterScan Web Security Suite 3.1 uses one operating mode—**TPC (Threads per Connection) mode**—which runs 4 processes, each with 500 threads (for a total of 2000 threads that IWSS can handle. The number of processes and threads per process can be configured to fit the hardware and network environment. See *Determining the Correct Process/Thread Configuration* on page B-5 for more details.

Identifying Your Server Placement

The first step is to identify the existing server where IWSS server should be installed. The second step is to identify the deployment options that exist, and eliminate those that do not fit the requirement.

Today's enterprise network topologies typically fall into one of two categories:

- Two firewalls with a Demilitarized Zone (DMZ)
- One firewall without a DMZ.

The ideal location for the IWSS server depends upon the topology in use.

Two Firewalls with DMZ

Given today's security concerns, many organizations have implemented a topology consisting of two firewalls (one external and one internal). These firewalls divide the network into two main areas:

- **The DMZ**—The DMZ is located between the external and internal firewalls. Hosts that reside in this area can accept connections from servers that are external to the organization's network. The configuration of the external firewall lets packets from external computers only reach servers inside the DMZ.
- **Corporate LAN**—These segments are located behind the internal firewall. The configuration of the internal firewall passes traffic to machines on the corporate LAN only when the traffic originates from computers inside the DMZ.

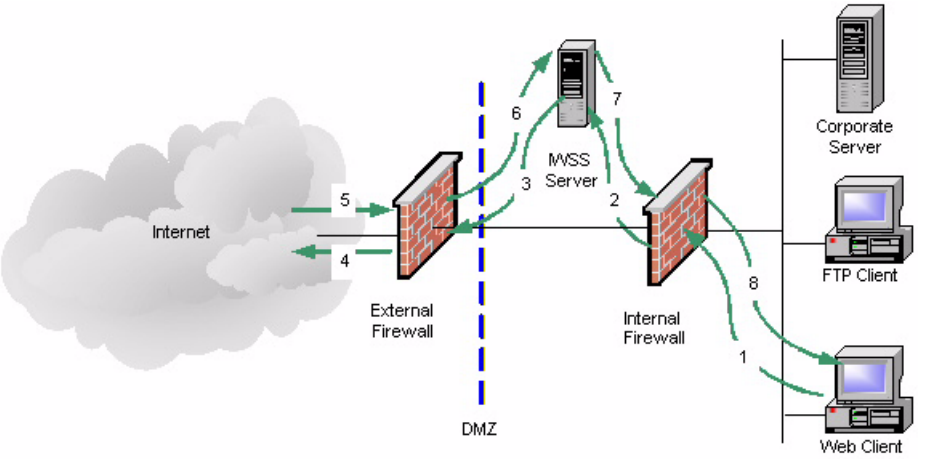


FIGURE 2-1 Two Firewalls with DMZ

This topology requires that all data inbound from the external servers (such as those on the Internet) first pass through a server in the DMZ. It also requires that certain types of data (for example HTTP and FTP packets), outbound from internal segments, pass through a server in the DMZ. This forces the use of proxies such as IWSS.

One Firewall with No DMZ

Some organizations have a firewall, but no DMZ. When using the “no DMZ” topology place the IWSS server behind the firewall.

- Because the IWSS server is not isolated from the corporate LAN, there is one less hop between external machines and machines on the corporate LAN. As shown in the diagram, this results in two less steps for processing a request, one outbound and one inbound.
- The firewall configuration allows connections to machines on the corporate LAN. For security, the firewall must limit the types of data that can reach machines on the LAN. For example, the firewall might allow HTTP data from the Internet to reach only the IWSS server.

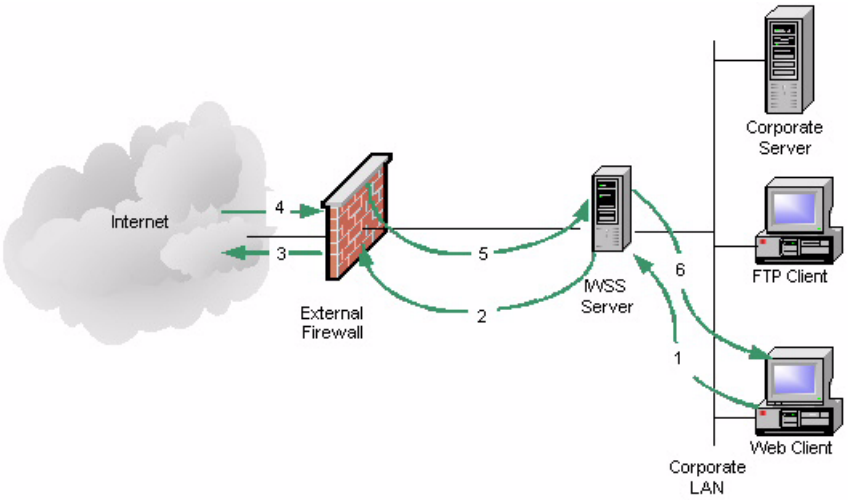


FIGURE 2-2 One Firewall with DMZ

Planning Network Protection and HTTP & FTP Service Flows

Network Traffic

To enforce the network traffic protection using IWSS, an additional solution (hardware, software or configuration) must be introduced that redirects the HTTP and/or FTP traffic to IWSS. Those solution include the following:

- Reconfiguring client settings
- Using a Layer 4 switch
- Using an ICAP-enabled proxy

See Appendix A, *Deployment Integration* starting on page A-1 for complete details.

HTTP and FTP Service Flows

Each HTTP and FTP configuration has implications for configuring IWSS, configuring the network, and for network security.

Create a flow plan for the HTTP and FTP services by doing the following:

- Understand each IWSS services purpose and function
- Determine each service's valid data sources. For example, does the HTTP service receive requests directly from the HTTP browsers, or indirectly through an ICAP proxy device?
- Determine which ports to use for the service. For instance, by default, the HTTP service uses port 8080, and the FTP service uses port 21. However, if another application or service is using port 8080, the administrator must configure the HTTP service to use a different port.
- Determine each services valid data destinations. For example, does the HTTP service send validated requests directly to the Web site? Or, does the HTTP service send the validated request to an upstream HTTP proxy?
- Add in any service-specific considerations. For instance, the HTTP service flow might include an ICAP device, but the FTP service flow does not.

Using the information gathered above, administrators determine which one of the possible flows to use for the installation.

Chapter 3

Installing IWSS

This chapter explains the following:

Component Installation

Note: Trend Micro recommends installing IWSS (IWSS) on a dedicated server.

During installation, the following components are automatically installed:

- **Main Program**—Management console and the basic library files necessary for IWSS.
- **HTTP Scanning**—Service necessary for HTTP scanning (either ICAP or HTTP proxy) and URL blocking.
- **FTP Scanning**—Service necessary for FTP scanning.
- **URL Filtering**—Service necessary for URL filtering (not enabled by default). Requires a separate activation code.
- **Applets and ActiveX Scanning**—Service necessary for scanning Java applets and ActiveX controls. Requires a separate activation code.
- **IntelliTunnel Security**—Services to block communication provided by certain Instant Message (IM) protocols and certain authentication connection protocols.
- **SNMP Notifications**—Service to send SNMP traps to SNMP-compliant network management software.
- **Control Manager Agent for IWSS**—Files necessary for the Control Manager agent. You need to install the agent if you are using Control Manager (Trend Micro's central management console).

Note: URL Filtering and Applets and ActiveX Scanning each require a separate activation code.

Pre-Installation Notes

Ensure that your DNS server is able to resolve the IWSS hostname to its IP address by doing one of the following:

- Add an A-record for the IWSS server on your DNS server
- Add the appropriate entry to the `/etc/hosts` file.

  The entry would be in the following format:

  ```
  {IP Address} {Hostname}
  ```

  For example:

  ```
  10.1.1.1  iwsssrv
  ```

Obtaining IWSS

You can install IWSS from the Trend Micro Enterprise Solutions CD or download the installation files from the Web. The Solutions CD is available for purchase and contains the installation file and all documentation.

To install from the Trend Micro Enterprise Solutions CD:

1. Insert the CD-ROM disc into the CD-ROM drive of the server where you want to install IWSS.
2. Choose **InterScan Web Security Suite** from the **Choose a product** drop-down list and then click **Go**.
3. Run the install script from the product folder on the Enterprise Solutions CD.

To download an evaluation version:

1. Go to the Trend Micro Web page:

   `www.trendmicro.com`.
2. From the **Product & Services** tab, select **Enterprise** from the drop-down list.
3. From the **Complete Product List** drop-down list, select **InterScan Web Security Suite**.
4. From the **InterScan Web Security Suite** page, click the **Download Evaluation Copy** link.
5. From the **Download InterScan Web Security Suite** page, complete all the required fields, accept the license agreement, and then click **Submit Form**.

A page opens thanking you for downloading an evaluation version of IWSS. This page states that you will receive an email from Trend Micro containing the links necessary to download the 30-day free trial versions of IWSS.

6. Download the IWSS product to a temporary directory on the server where you want IWSS to run, and then extract the files.

Installing IWSS

Trend Micro recommends that you install IWSS on a dedicated server. To install IWSS, you must log on to the target server as **root**.

The section describes the following installation scenarios:

Note: An activation code is required to enable scanning and product updates (see the *Administrator's Guide*).

Installing IWSS 3.1 and PostgreSQL

To install a fresh copy of IWSS and PostgreSQL:

1. Log on the server as "`root`" and access the folder where the installation tar package is located.

   Note: Before running the install script, make sure the current directory and its parent directories are granted read privilege to all users.

2. Extract the installer components by running the following:

   ```
   gunzip IWSS3.1Sol.tar.gz
   ```

   ```
   tar -xvf IWSS3.1Sol.tar
   ```

3. From the directory containing the IWSS installation files, type `./install_iwss.sh` and then press **Enter**.
4. The license agreement page appears. Accept the license agreement to continue installation.

   The install script performs system check on memory and swap space. Trend Micro recommends a minimum physical memory of 1GB for installation and a swap space that is four times the amount of physical memory. If physical

memory is less than 1GB, you will need at least 4GB of swap space. The maximum swap space required is 16GB.

Note: If your server does not meet the minimum memory or swap space requirement, you can still install IWSS. However, normal IWSS operation may be affected after installation due to resource limitations.

5. Specify the installation location (the default is `/opt/trend/iwss`). Installation automatically creates `iscan` user and group settings and extract the packages.

Note: For compatibility, IWSS 3.1 installation script creates three symbolic links as follows:
1. `/usr/iwss` pointing to `<IWSS>/bin`
2. `/etc/iscan` pointing to `<IWSS>/data`
3. `/var/iwss` pointing to `<IWSS>/data`

Make sure these symbolic links can be created successfully. If these folders already exist and are mounted to the file system, IWSS will not be able to delete the folders and create the corresponding links as expected.

To avoid such issue, umount them before installation. You can mount them to the file system after installation if needed.

6. The installation script checks the service ports required for IWSS services.

For example, port numbers 8080, 21, 161, and 1812. If any one of these ports are already used by another service, a warning message displays. Make sure the port(s) is free for use by IWSS before you type "`y`" to continue.

Note: If another application is using port 5432, a warning message will display. Make sure this port number is not already in use before you continue to install the PostgreSQL included in the IWSS setup package.

By default, the installation script installs PostgreSQL v7.4.18 automatically and creates the "`iwss31`" database with "`sa`" as the username.

7. If you choose to register IWSS to the Control Manager server during installation, specify the required settings.

   By default, 80 is used for HTTP connection or 443 for HTTPS connection.

   If you skip Control Manager registration (the default action), you can still use the IWSS Web console to register to Control Manager after installation.

   Note: After installation is complete, the system starts IWSS services and the screen displays the IWSS Web console URL and the default administrator login information (username and password).

8. Press **Enter** to exit.

Installing IWSS 3.1 with an Existing PostgreSQL Server

You can choose to use an existing local or remote PostgreSQL server. Specify the server and database information (such as hostname or IP address and the port number, etc.). If a database with the name "`iwss31`" exists, you can choose to:

- Connect to the existing iwss31 database and share database information with other IWSS server(s)
- Delete the existing database and create a new one
- Configure the PostgreSQL database information and try again
- Terminate the installation process

Installing IWSS 3.1 on an Existing IWSS Server

If a previous version of IWSS is already installed on the server, you are prompted to migrate or perform a fresh install (uninstalling the old IWSS version and PostgreSQL). Type **f** at the prompt to start a fresh install.

Refer to *Migrating to IWSS 3.1* on page 4-1 for more information on migration.

```
Detected a previous installation of InterScan Web Security Suite (version
2.2).
Do you want to migrate (enter m) or perform a fresh install (enter f)?
(m/f): [m] f
```

Installing IWSS 3.1 in a Server Farm

Follow the steps in *Installing IWSS 3.1 and PostgreSQL* on page 3-5 to install a fresh copy of IWSS 3.1 on the first server. Trend Micro recommends installing PostgreSQL on a dedicated server for a server farm.

To install IWSS 3.1 on subsequent servers, type "**y**" at the prompt to use an existing PostgreSQL server and configure the settings when prompted.

Post-Installation Notes

After you finish installing, open the IWSS Web console and change the administrator password to ensure the security of your system (see the *Administrator's Guide*).

Note the following:

- Trend Micro recommends that you update your scan engine and virus pattern files immediately after installing, registering and activating the product.
- Trend Micro only supports listening port 80 for IWSS in reverse proxy mode, as well as for the protected server. When configuring IWSS as a reverse proxy, specify port 80 in the **HTTP listening port** field, and in the **Port** field for the protected server. The IWSS listening port for reverse proxy is hardcoded to 80.

Uninstalling IWSS 3.1

You can uninstall IWSS 3.1 using the uninstall script or manually. The uninstallation process will not remove the PostgreSQL database. You may manually delete the database if required.

To uninstall IWSS using the uninstall script:

1. Log on the IWSS server as "root" and open a command window.
2. Type `./uninstall_iwss.sh`.

   The system will stop all IWSS services.
3. When the prompt "`Do you want to stop the PostgreSQL database and disable its auto-start?`" displays, type "`y`" to stop and disable auto-start for the database or type "`n`."

   After the uninstallation is complete, the message "`All IWSS 3.1 components except the default installed PostgreSQL database have been successfully uninstalled.`" displays.

To manually uninstall IWSS 3.1:

1. Log on the IWSS server as "`root`" and type one of the following command to stop all IWSS services.

   ```
   /etc/rc2.d/S99IWSS stop
   ```

   or

   ```
   /opt/trend/iwss/bin/rcIwss stop
   ```

Note: You can also stop each IWSS component using the `stop` command in the directory `/opt/trend/iwss/bin`. For example, ./`S99ISMetricMgmtd stop`.

2. Type the following commands to delete IWSS files and directories.

```
rm -rf /opt/trend/iwss
rm -rf /var/iwss
rm -rf /usr/iwss
rm -rf /etc/iscan
```

3. Type the following commands to delete IWSS start/stop scripts.

```
rm -rf /etc/rc0.d/ K09IWSS
rm -rf /etc/rc2.d/ S99IWSS
```

4. Type the following commands to delete the `iscan` user and group information.

```
userdel iscan
groupdel iscan
```

Chapter 4

Migrating to IWSS 3.1

This chapter explains the following:

About Migration

You can migrate your IWSS 2.2 release to version 3.1 using the migration script. Migration procedure and screen prompts are similar to the installation process. The migration script will automatically detect existing IWSS 2.2 and PostgreSQL installed on your server.

Log Migration Notes

IWSS automatically detects the existence of IWSS 2.2 on your computer and saves your configuration settings. However, while customized directories are saved during the migration, the contents of these directories are not. The contents of the following directories will not be migrated:

- **Reporting and System logs**
- **Scheduled reports**
- **Quarantine log**

Operating Mode Migration Notes

In previous versions, IWSS ran in different operating modes (thread and process modes). IWSS 3.1 for Solaris uses one operating mode—**TPC mode (Threads per Connection)**. During migration, the version 2.2 operating mode (either thread or process mode) will be automatically changed to TPC mode, which is not configurable through the user interface.

Database Migration Notes

When migrating IWSS 2.2 to IWSS 3.1 on Solaris 10 and the migration process goes to the “Backup Solaris 2.2 Policy Backup” step, the system may display an error message to indicate that database connection failed and prompts you to exit installation.

This issue is caused by the Solaris 10 operating system. Please refer to the following URLs for details:

- `http://archives.postgresql.org/pgsql-general/2004-09/msg00987.php`
- `http://bugs.opensolaris.org/view_bug.do?bug_id=4944187`

To continue the migration process:

1. Add "`dns`" to the file `/etc/nsswitch.conf`.
2. Disable the name service cache daemon (nscd) as follows:

```
// Check nscd status:
bash-3.00 # svcs name-service-cache
STATE          STIME    FMRI
online         Dec_05   svc:/system/name-service-cache:default

// Disable nscd
bash-3.00 # svcadm disable system/name-service-cache

// Check nscd status again:
bash-3.00# svcs name-service-cache
STATE          STIME    FMRI
disabled       13:14:44 svc:/system/name-service-cache:default"
```

Backing Up IWSS 2.2 Information

The migration script automatically backs up the policy tables and local configuration information in IWSS 2.2 before migration. You can retrieve these backup files from the directory `/opt/trend/backup/iwss22`.

Trend Micro recommends manually creating a backup copy of IWSS 2.2 configuration, policies, and logs before migration, which allows you to roll back to IWSS 2.2 if an error occurs during program update or data migration.

Saving Customized Settings

Backing Up Your InterScan Web Security Suite 2.2 Settings

Note: The backup process make take several minutes depending on the amount of data (such as old logs, reports, quarantine files, and so on) available on IWSS 2.2. Trend Micro recommends that you remove data that you do not want to include in the backup files.

You can use this backup to manually restore your production IWSS settings if you want to return to using IWSS 2.2.

1. Stop all IWSS 2.2 services. Type `find /etc/rc3.d/ -name S99IS* -exec {} stop \;` or the following commands in the `/etc/rc3.d` directory:

   ```
   S99IScanHttpd stop
   S99ISftp stop
   S99ISmaild stop
   S99ISproxy stop
   S99ISlogtodb stop
   S99ISagent stop
   S99ISdatabase stop
   ```

2. Back up all configuration files from IWSS 2.2 by typing the following commands:

   ```
   tar -cvf  /home/iscan.tar  /etc/iscan/
   tar -cvf  /home/IWSS.tar  /opt/trend/IWSS
   ```

3. Back up settings and data in the database.

   If you installed PostreSQL that comes with the IWSS 2.2 setup package on the IWSS 2.2 machine, type the following command to back up information from the database:

   ```
   tar -cvf  /home/pgdata.tar  /var/iwss/pgdata
   ```

Note: If you installed IWSS 2.2 with an existing remote database, you do not need to back up the database information as it will not be replaced during the migration process. You can reuse information in the existing database after the migration.

Migration Requirements

Make sure you have the migration script `install_iwss.sh` before you continue.

Migrating to IWSS 3.1

This section describes how to migrate to IWSS 3.1 from one of the following:

- Single IWSS server with PostgreSQL v7.4.1 or other specified version
- IWSS server farm

Note: You can only upgrade to IWSS version 3.1 from IWSS version 2.2. If you want to upgrade to version 3.1 from version 2.x, you must first upgrade to version 2.2, then upgrade again to version 3.1, or perform a fresh install.

Single Server Migration

Procedure for single server migration is similar for an IWSS 2.2 server with the default PostgreSQL v7.4.1 or other specified PostgreSQL version installed.

Note: Before you start the migration process, Trend Micro recommends you back up IWSS 2.2 policy tables and configuration information. See to *Backing Up IWSS 2.2 Information* on page 4-3.

To migrate a single server to IWSS 3.1:

1. Log on the IWSS server as "`root`" and access the folder where the migration script file is located.

Note: Before running the migration script, make sure the current directory and its parent directories are granted read privilege to all users.

2. From the directory containing the IWSS installation files, type `./install_iwss.sh` and then press **Enter**.
3. The license agreement page appears. Type "y" to accept the license agreement to continue.
4. The install script performs a check on system memory and swap space. Trend Micro recommends a minimum physical memory of 1GB and a swap space that is four times the amount of physical memory. If physical memory is less than 1GB, you will need at least 4GB of swap space.

Note: If your server does not meet the minimum memory or swap space requirement, you can still install IWSS. However, normal IWSS operation may be affected after installation due to resource limitations.

5. The migration script automatically detects existing IWSS 2.2 installed on the server. Press **Enter** or type "m" to migrate to IWSS 3.1.

WARNING! *If you type* **f** *and press* **Enter***, the migration script uninstalls IWSS 2.2 before installing IWSS 3.1. All existing IWSS 2.2 data will be erased.*

```
Detected a previous installation of InterScan Web Security Suite (version
2.2).
Do you want to migrate (enter m) or perform a fresh install (enter f)?
(m/f): [m]
```

6. A message displays prompting you to perform data backup manually. If you have already backed up IWSS 2.2 information, press **Enter** to continue.

```
The migration script will automatically back up IWSS 2.2 policy tables and
configuration information before migration.

Trend Micro recommends you create a backup copy of IWSS 2.2 configuration,
logs, and policy tables manually. This allows you to roll back to IWSS 2.2
in case an error occurs during program upgrade or data migration. Please
refer to the Installation Guide for manual backup procedure.

Press [Enter] to continue ...
```

The migration script tests the connection to the old IWSS 2.2 database and prompt you to specify the database name for IWSS 3.1 (the default is "`iwss31`"). After you press **Enter**, the migration script automatically backs up IWSS 2.2 information to the folder `/opt/trend/backup/iwss22` and starts the migration process.

The migration process uninstalls IWSS 2.2 and PostgreSQL v7.4.1 from the server before installing IWSS 3.1 and PostgreSQL v7.4.18. Old policy and configuration settings will be applied after the PostgreSQL service is started.

Note: If you have installed PostgreSQL v7.4.1 that comes with the IWSS 2.2 setup program, the migration process automatically backs up the old database and restores it after PostgreSQL v7.4.18 is installed.

If you use an existing PostgreSQL server with IWSS 2.2 installation, the migration process will not install PostgreSQL v7.4.18. In this case, both the IWSS 2.2 database and IWSS 3.1 database will be in the old PostgreSQL server.

If your IWSS 2.2 server was registered to Control Manager before migration, the registration information will be retained and a message displays prompting you to use existing information to register IWSS 3.1. Otherwise, you are prompted to specify Control Manager registration settings. If you skip this step during migration, you can still use the IWSS Web console to register to Control Manager after migration.

After IWSS migration is complete, the screen displays the IWSS Web console URL and the default administrator login information (user name and password).

7. Press **Enter** to exit.

Server Farm Migration

If you deploy IWSS 2.2 in a server farm with a master IWSS server, one or more IWSS slave servers, and a shared PostgreSQL server, you can still migrate IWSS 2.2 to IWSS 3.1.

Use the migration script to migrate the IWSS server with the "iwss" database to IWSS 3.1 first and then run the migration script on other IWSS servers. The

migration procedure is similar to single server migration except for the database options on a slave server.

To migrate a server farm to IWSS 3.1:

1. Run the migration script on the IWSS server where the database "`iwss`" is located to perform the migration first.

   Follow the steps described in *Single Server Migration* on page 4-5.

2. Run the migration script on the other IWSS servers.

   Follow the steps described in *Single Server Migration* on page 4-5. The migration script detects an existing IWSS 3.1 database (which is created during the master server migration). The the screen displays the following database options:

```
Enter database name for IWSS 3.1 in PostgreSQL: [iwss31]
The database: iwss31 already exists.

You can choose to:
 1) Connect to this existing 3.1 database
 2) Drop it and create a new one with the same name
 3) Enter another database name and try again
 4) Quit installation and try later
Please type your selection (1/2/3/4): [1]
```

   - **Connect to this existing 3.1 database—**Select this option to connect and use the existing IWSS 3.1 database. Trend Micro recommends you select this option during migration on a slave server
   - **Drop it and create a new one with the same name—**Select this option to create the database again. The database will have the same settings since IWSS 2.2 configuration and policy settings will be applied again.
   - **Enter another database name and try again—**Select this option to create a separate database for the slave server. Select this option only if you want to change the deployment mode for the slave server to single server deployment.
   - **Quit installation and try later—**Select this option to exit from the migration process. The slave server is still operational with IWSS 2.2 configuration and policy settings.

3. After the migration process is complete on the master and slave servers, access the IWSS Web console to configure the server role again.

Restoring IWSS 2.2

1. Execute `./uninstall_iwss.sh` in the IWSS 3.1 installation package.

   This command automatically removes IWSS 3.1 from the system.

2. Use the ghost image to restore the entire machine, or install IWSS 2.2 and manually restore the old configurations and data as described in the following steps.

   Note: If you are re-installing IWSS 2.2 and restoring the settings, make sure you use the same deployment mode and installation path as before the IWSS 3.1 migration.

3. Stop all IWSS 2.2 processes after installation. Type `find /etc/rc3.d/ -name S99IS* -exec {} stop \;` or the following commands in the `/etc/rc3.d` directory:

   ```
   S99IScanHttpd stop
   S99ISftp stop
   S99ISmaild stop
   S99ISproxy stop
   S99ISlogtodb stop
   S99ISagent stop
   S99ISdatabase stop
   ```

4. Restore data that you have previously backed up before the migration. Type the following commands:

   ```
   tar -xvf /home/iscan.tar /etc/iscan
   tar -xvf /home/IWSS.tar /opt/trend/IWSS
   ```

5. Restore data and settings in the PostgreSQL database.

   If you installed PostgreSQL that comes with IWSS 2.2 setup packet on the same IWSS 2.2 server, type the following command:

   ```
   tar -xvf /home/pgdata.tar /var/iwss/pgdata
   ```

If you are using an existing database, connect to the remote PostgreSQL server to obtain the information.

6. Start all IWSS 2.2 services. Type `find /etc/rc3.d/ -name S99IS* -exec {} start \;` or the following commands in the `/etc/rc3.d` directory:

```
S99IScanHttpd start
S99ISftp start
S99ISmaild start
S99ISdatabase start
S99ISproxy start
S99ISlogtodb start
S99ISagent start
```

Chapter 5

ICAP Configuration

This chapter explains the following:

After Installing IWSS ICAP

Perform these post-install configuration steps only if you have installed IWSS ICAP on your system.

After installing the IWSS ICAP program files, do the following:

1. *Setting up an ICAP 1.0-compliant Cache Server* on page 5-2
2. *Enabling "X-Virus-ID" and "X-Infection-Found" Headers* on page 5-9

Setting up an ICAP 1.0-compliant Cache Server

Configure an ICAP client to communicate with the ICAP server.

- *To set up ICAP for NetCache Appliance:* on page 5-2
- *To set up ICAP for the Blue Coat Port 80 Security Appliance:* on page 5-4
- *To set up ICAP for Cisco CE ICAP servers:* on page 5-7

Setting up ICAP for NetCache Appliances

To set up ICAP for NetCache Appliance:

1. Log on to the NetCache console by opening `http://{SERVER-IP}:3132` in a browser window.
2. Click the **Setup** tab, and then click **ICAP** > **ICAP 1.0** in the left menu.
3. Click the **General** tab, and then select **Enable ICAP Version 1.0**. Click **Commit Changes**.

   Note: An error message `"icap: This service is not licensed."` appears if you have not provided the required ICAP license key for NetCache.

4. Enter an ICAP license key:
   a. Click the **Setup** tab, and then click **System > Licenses** in the left menu. The **System Licenses** screen appears.
   b. Type **IWFLPWA** under the **ICAP license** section.
   c. Click **Commit Changes**.

5. Select the **Service Farms** tab on the **ICAP 1.0** screen, and then click **New Service Farm** to add ICAP servers. Then, assign the service farm name in the **Service Farm Name** field.
   - For response mode, select **RESPMOD_PRECACHE** in the **Vectoring Point** field
   - For request mode, select **REQMOD_PRECACHE** in the **Vectoring Point** field

   Select **Service Farm Enable**.
6. In the **Load Balancing** field, choose the proper algorithm that you use for load balancing (if you have more than one ICAP server in the service farm). Clear **Bypass on Failure**.

Note: Disable **Bypass on Failure** if the priority is more on virus propagation within your network. Otherwise, enable **Bypass on Failure** to guarantee an unblocked connection to the Internet.

---

7. Under the **Consistency** field, choose **strong** from the drop-down menu and leave the **lbw Threshold** field empty.
8. Under the **Services** text box (for response mode), type:
   `icap://{ICAP-SERVER-IP}:1344/resp on,`
   where `ICAP-SERVER-IP` is the IP address of IWSS ICAP for response mode.

   Under the **Services** text box (for request mode), type
   `icap://{ICAP-SERVER-IP}:1344/REQ-Service on,`
   where `ICAP-SERVER-IP` is the IP address of IWSS ICAP for request mode.

   For multiple IWSS ICAP server services, type the additional entries in step 7. For example:

   For response mode,
   - `icap://{ICAP-SERVER1-IP}:1344/resp on`
   - `icap://{ICAP-SERVER2-IP}:1344/resp on`

   Click **Commit Changes**.

   For request mode,
   - `icap://{ICAP-SERVER1-IP}:1344/REQ-Service on`
   - `icap://{ICAP-SERVER2-IP}:1344/REQ-Service on`

   Click **Commit Changes**.

Note: For multiple ICAP servers within a service farm with **strong** consistency selected, make sure that all ICAP servers have identical `intscan.ini` and other configuration files and the same virus pattern. The service farm will not work properly if the ICAP servers have different configurations.

9. Click the **Access Control Lists** tab, and then select **Enable Access Control Lists**. Type `icap (Service Farm name of the ICAP Server) any` in **HTTP ACL**. Click **Commit Changes**.

   To configure scanning FTP over HTTP traffic, go to FTP > Configuration > **Access Control Lists**, and then add `"icap (service farm name)" any` into the **FTP ACL** field.

Setting up ICAP for Blue Coat Port 80 Security Appliance

To set up ICAP for the Blue Coat Port 80 Security Appliance:

Log on to the management console by typing http://{SERVER-IP}:8081 in the address bar of your Web browser (specifying port 8081 as the default management port). For example, if the IP address configured during the first-time installation is 123.123.123.12, enter the URL http://123.123.123.12:8081 in the Web browser.

1. Select **Management**. Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Services** tab.
3. Click **New**. The **Add ICAP Service** screen appears.
4. In the **ICAP service name** field, type an alphanumeric name. Click **Ok**.
5. Highlight the new ICAP service name and click **Edit**. The **Edit ICAP Service name** screen appears.
6. Type or select the following information:
   a. ICAP version number (that is, 1.0)
   b. The service URL, which includes the virus-scanning server host name or IP address, and the ICAP port number. The default ICAP port number is 1344.
      - Response mode:
      `icap://{ICAP-SERVER-IP}:1344`
      - Request mode:
      `icap://{ICAP-SERVER-IP}:1344/REQ-Service`

where `ICAP-SERVER-IP` is the IP address of IWSS ICAP.

c. The maximum number of connections (ranges from 1-65535). The default value is 5.

d. The connection timeout, which is the number of seconds the Blue Coat Port 80 Security Appliance waits for replies from the virus-scanning server. The range is an interval from 60 to 65535. The default timeout is 70 seconds.

e. Choose the type of method supported (response or request modes).

f. Use the default preview size (bytes) of zero (0).

g. Click **Sense settings** to retrieve settings from the ICAP server (recommended).

h. To register the ICAP service for health checks, click **Register** under the **Health Check Options** section.

7. Click **Ok**, and then click **Apply**.

Note: You can edit the configured ICAP services. To edit a server configuration again, select the service and click **Edit**. The examples used for configuring ICAP for Blue Coat is based on version 2.1.07. The settings may vary depending on the version of Blue Coat.

---

8. Add response or request mode policy.

The Visual Policy Manager requires the Java 2 Runtime Environment Standard Edition v.1.3.1 or later (also known as the Java Runtime or JRE) from Sun™ Microsystems, Inc. If you already installed JRE on your workstation, the Security Gateway opens a separate browser window and starts the Visual Policy Manager. The first time you start the policy editor, it displays an empty policy.

If you have not installed JRE on your workstation, a security-warning window appears. Click **Yes** to continue. Follow the instructions to install the JRE.

To add the response mode policy:

a. Select **Management**. Type the logon user name and password if prompted.

b. Click **Policy** in the left menu, and then click the **Visual Policy Manager** tab.

c. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.

d. On the menu bar, click **Edit > Add Web Content Policy**. The **Add New Policy Table** screen appears.

e. Type the policy name under the **Select policy table name** field. Click **OK**.

f. Under the **Action** column, right-click **Bypass ICAP Response Service** and click **Set**. The **Add Object** screen appears. Click **New** and select **Use ICAP Response Service**. The **Add ICAP Service Action** screen appears.

g. Choose the ICAP service name under the **ICAP Service/Cluster Names** field. Enable **Deny the request** under the **On communication error with ICAP service** section. Click **OK**, and then click **OK** again.

h. Click **Install Policies**.

To add the request mode policy:

a. Select **Management**. Type the logon user name and password if prompted.

b. Select **Policy** in the left menu, and then click the **Visual Policy Manager** tab.

c. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.

d. On the menu bar, click **Edit > Add Web Access Policy**. The **Add New Policy Table** screen appears.

e. Type the policy name under the **Select policy table name** field. Click **OK**.

f. Under the **Action** column, right-click **Deny** and click **Set**. The **Add Object** screen appears. Click **New** and select **Use ICAP Request Service**. The **Add ICAP Service Action** screen appears.

g. Choose the ICAP service name under the **ICAP Service/Cluster Names** field. Enable **Deny the request** under the **On communication error with ICAP service** section. Click **OK**, and then click **OK** again.

h. Click **Install Policies**.

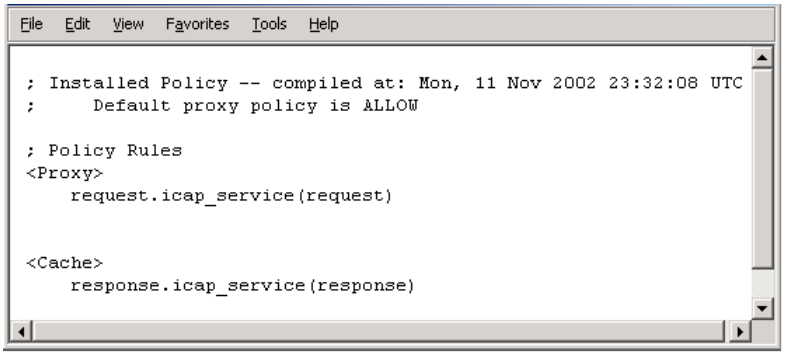


FIGURE 5-1 Configure both the request and response mode ICAP services. To check the current policy, go to the "Policy" screen, click the "Policy Files" tab, and then click "Current Policy".

Setting up ICAP for Cisco CE ICAP Servers

To set up ICAP for Cisco CE ICAP servers:

IWSS supports Cisco ICAP servers (CE version 5.1.3, b15). All ICAP settings are performed through a command line interface (CLI); there is no user interface associated with the Cisco ICAP implementation.

1. Open the Cisco CE console.
2. Type `config` to enter the configuration mode.
3. Type `ICAP` to display a list of all ICAP-related commands.
4. Create a response modification service, by typing

   ```
   icap service RESPMOD SERVICE NAME
   ```

   This takes you into the ICAP service configuration menu. Display a list of all available commands. Type the following commands:

   `server icap://ICAP SERVER IP:1344/resp` (to assign a server type)

   `vector-point respmod-precache` (to assign the proper vector point type)

   `error-handling return-error` (to assign the proper error-handling type)

   `enable` (to enable the ICAP multiple server configuration)

5. Type `exit`.
6. Create a request modification service, by typing

   ```
   icap service REQUESTMOD SERVICE NAME
   ```

   This command takes you into the ICAP service configuration menu. Display a list of all available commands. Issue the following commands:

   `server icap://ICAP SERVER IP:1344/REQ-Service` (to assign a server type)

   `vector-point reqmod-precache` (to assign the proper vector point type)

   `error-handling return-error` (to assign the proper error-handling type)

   `enable` (to enable the ICAP multiple server configuration)
7. Type `exit`.
8. For additional configuration steps, type the following:

   `icap append-x-headers x-client-ip` (to enable X-client headers for reports)

   `icap append-x-headers x-server-ip` (to enable X-server headers for reports)

   `icap rescan-cache ISTag-change` (to enable ISTAG rescan for updates)

   `icap bypass streaming-media` (to exclude streaming media from ICAP scanning)

   `icap apply all` (to apply all settings and activate ICAP type)

   `show icap` (to display current ICAP configuration at root CLI menu)

Configuring Virus-scanning Server Clusters

For the Blue Coat Port 80 Security Appliance to work with multiple virus-scanning servers, you must configure a cluster in the Security Gateway (add the cluster, and then add the relevant ICAP services to the cluster).

To configure a cluster using the management console:

1. Select **Management**. Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Clusters** tab.
3. Click **New**. The **Add ICAP Cluster** screen appears.
4. In the **ICAP cluster name** field, type an alphanumeric name. Click **Ok**.

5. Highlight the new ICAP cluster name and click **Edit**. The **Edit ICAP Cluster name** screen appears.
6. Click **New** to add an ICAP service to the cluster. The **Add ICAP Cluster Entry** screen appears. The pick list contains a list of any services available to add to the cluster. Choose a service and click **Ok**.
7. Highlight the ICAP cluster entry and click **Edit**. The **Edit ICAP Cluster Entry name** screen appears. In the **ICAP cluster entry weight** field, assign a weight from 0-255. Click **Ok**, click **Ok** again, and then click **Apply**.

Deleting a Cluster Configuration or Entry

You can delete the configuration for an entire virus-scanning server cluster, or you can delete individual entries from a cluster.

Note: Do not delete a cluster used in a Blue Coat Port 80 Security Appliance policy if a policy rule uses a cluster name.

To delete a cluster configuration using the management console:

1. Select **Management**. Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Clusters** tab.
3. Click the cluster you want to delete. Click **Delete**, and then click **Ok** to confirm.

Enabling “X-Virus-ID” and “X-Infection-Found” Headers

IWSS can return 2 optional headers from the ICAP server whenever a virus is found: the “X-Virus-ID” and the “X-Infection-Found” headers. Neither of these headers are returned by default for performance reasons, since many ICAP clients do not use these headers. They must be enabled in the IWSS management console.

- “X-Virus-ID” contains one line of US-ASCII text with a name of the virus or risk encountered. For example:

  ```
  X-Virus-ID: EICAR Test String
  ```

- “X-Infection-Found” returns a numeric code for the type of infection, the resolution, and the risk description.

For more details on the parameter values, see:

`http://www.i-cap.org/spec/draft-stecher-icap-subid-00.txt`

To enable the X-Virus-ID header:

1. From the main menu, click **HTTP > Configuration > Proxy Scan Settings**.
2. On the **Proxy Settings** page, select **Enable 'X-Virus ID' ICAP header** and/or **Enable 'X-Infection-Found' ICAP header**.

Using SSL with Damage Cleanup Services

To redirect clients to Damage Cleanup Service (DCS) to clean up malicious code when you are using the HTTPS-enabled Web management console, access to the secure port that IWSS uses (typically 8443) must be enabled. Otherwise, redirection to DCS will not be successful, since the redirection request will be blocked.

To allow access to secure port 8443:

1. Click **HTTP > Configuration > Access Control Settings**, and make the **HTTPS Ports** tab active.
2. Under the Action drop-down list, select **Allow.**
3. Select the **Port** radio button.
4. In the **Port** field, enter the port number used for HTTPS traffic (typically 8443).
5. Click **Add** and then **Save**.

FIGURE 5-2 Allow access to the secure port (typically 8443) if using DCS and the HTTPS management console

Appendix A

Deployment Integration

This appendix explains the following:

IWSS in a Distributed Environment

IWSS is designed to be part of a distributed system and can establish a number of network connections based on the configuration settings.

The administrator must ensure the following:

- None of the required channels are blocked
- All channels have enough throughput
- Servers use a supported version of the software
- Servers have enough performance

Connection Requirements and Properties

Table 1-1 below gives the required connections and their properties.

TABLE 1-1. Required Connections and Properties

Connecting Component	Traffic: Type and Volume	If the Connection is lost
Clients	Should be measured on the real network	No protection
Database server	**Type:** TCP **Volume:** • **Low**—if access logging is disabled • **Medium**—if access logging is enabled	Cached data is used for already started services. Services will not start.
LDAP server (if configured)	**Type:** LDAP **Volume:** Medium	Cached data is used for already started services. Services will not start.
Trend Micro Active Update Server	**Type:** HTTP and HTTPS **Volume:** 10-50 Mb/day	IWSS components cannot be updated in time.
Trend Micro Dynamic Categorization server (if configured)	**Type:** HTTP **Volume:** Depends on the specific access	Requested resources are not categorized properly. URLs prohibited by policy settings can be accessible.

TABLE 1-1. Required Connections and Properties (Continued)

Connecting Component	Traffic: Type and Volume	If the Connection is lost
Trend Micro DCS server (if configured)	**Type:** HTTP **Volume:** Depends on the number of infected machines	No cleaning is performed for infected machines.

Throughput and Availability Requirements

The administrator must determine the IWSS availability requirements.

- Is IWSS downtime acceptable?
- If so, what is the proper action (bypass or stop) to enforce when IWSS is down?
- If a failover configuration with multiple IWSS instances is used, do the LDAP server and the database server have the same level of failover?

Integration with LDAP

Support Referral Chasing for Multiple LDAP Servers

IWSS has an LDAP module that allows communication with multiple LDAP servers with the ability to establish multi-domain tree- and forest-like environments.

If the configured main LDAP server from the IWSS Web console **HTTP > Configuration > User Identification** page cannot resolve client credentials, and the "referral chasing" is enabled (providing that the referral server(s) is configured), IWSS attempts to query for the requested User/Group object with the configured Primary Referral Server. If the queried object is still not found, a configured Secondary Referral will be queried. In order to do that, it must keep the credentials of the administrative account for all LDAP servers in the `[LDAP-Setting]` section of the intscan.ini file.

The Windows Active Directory (AD) Global Catalog enables LDAP clients, such as IWSS, to query objects native to the domain being queried, and those residing in remote domains, as long as the AD server being queried and the remote AD server has Global Catalog enabled. The Global Catalog server accepts the LDAP requests on port 3268 and allows querying the user credentials, full name and membership in

the global and universal groups across all other domains in the forest. The use of the Global Catalog is handy when creating IWSS LDAP policies for a parent group with user(s)/group(s) member(s) residing on remote domains that are part of many sub-domain levels.

To use this feature, the IWSS administrator should configure the main LDAP server that IWSS uses from the Web console **HTTP > Configuration > User Identification** page to communicate with a designated Global Catalog-enabled Active Directory server using port 3268, instead of using the default LDAP communication port 389.

Note: Global Catalog is available only in Microsoft Active Directory. The advantage of using the Global Catalog port includes better performance for LDAP object lookup, and allows object lookup that resides in many sub-levels of the Active Directory tree (beyond three). However, in order for IWSS to utilize the Global Catalog, the AD being requested for an object needs to have the Global Catalog enabled along with the AD where the queried user/group object reside. IWSS supports the use of the Global Catalog port only to be configured as the main LDAP server, and not part of the IWSS referral chasing servers.

Tip: Trend Micro recommends allowing IWSS to query the root Active Directory server with the Global Catalog enabled, and using Universal group types to do group nesting when applying policies. This can be seen by the Global Catalog and will be visible throughout the Active Directory. For more information, see Microsoft support (`http://support.microsoft.com/kb/231273`).

Guest Account

When LDAP support is enabled, IWSS works in the authenticated proxy mode. It requires authentication for every client. This rule can cause problems for guest/mobile computers, whose users are not registered in the local LDAP server.

To resolve this issue, the HTTP scanning service in the HTTP proxy mode supports an additional listening point that can be used as a proxy server specification for the guest computers.

The following configuration in the Web console HTTP > Configuration > Proxy Scan Settings control this behavior:

- Enable guest account—enables this feature
- Port number—port number on which to listen

IWSS bypasses the LDAP-based user identification and applies the special (Guest) policies to every computer accessing it over this port.

Damage Cleanup Services Integration

While IWSS can detect and block worms and spyware at the HTTP and FTP gateway, it can also work in conjunction with Trend Micro Damage Cleanup Services to clean infected clients. Damage Cleanup Services (DCS) is a comprehensive service that helps assess and clean system damage without installing software on client computers in a network. It performs the following activities:

- Removes registry entries created by worms and Trojans
- Removes memory resident worms, Trojans, and spyware/grayware
- Repairs system file configurations modified by malware

After IWSS is registered with one or more DCS servers, IWSS issues a cleanup request if it detects one of the following trigger conditions:

- Client PC attempts to access a URL classified as “Spyware,” “Disease Vector,” or “Virus Accomplice” by the Phish pattern file, or
- Client PC uploads a virus classified as a worm

Note: If malware attempts to contact a remote server using a protocol other than HTTP, IWSS will not detect it, thus will not trigger a cleanup.

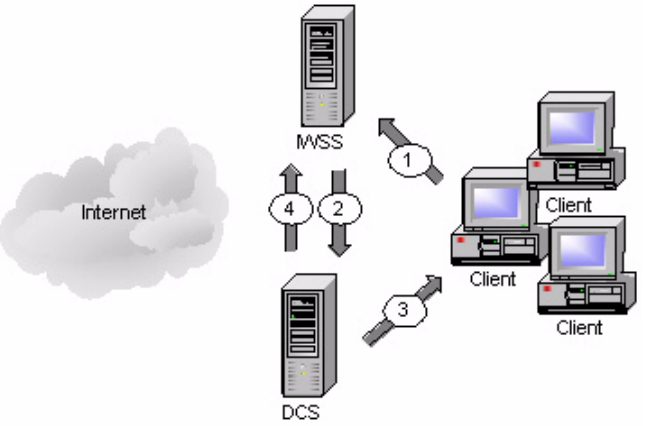


FIGURE A-1 How IWSS requests DCS to perform a client cleanup

When IWSS registers to a DCS server, infected client cleanups are handled in the following manner:

1. IWSS detects the client attempting to access a URL listed in the PhishTrap pattern file or upload a worm.
2. IWSS requests the DCS server to clean up the infected client.
3. DCS attempts to connect to the infected client and clean it through remote procedures.
4. DCS reports the outcome of its cleaning attempt to IWSS for logging.

When it receives a cleanup request from IWSS, DCS attempts to connect to the infected client and repair the system damage. The outcome of the cleaning attempt, either successful or unsuccessful, is reported back to the IWSS server for logging. If the cleanup attempt is not successful, then the client is redirected to a Web page hosted on the DCS server and an ActiveX control again attempts to clean the infected computer, with the permission of the computer's user.

Note: If you are using DCS in conjunction with a HTTPS-enabled IWSS Web management console, IWSS must be configured to allow access to the secure port (typically 8443). If access to the secure port is blocked, IWSS will be unable to redirect clients to DCS for clean-up requests. For more information, see *Using SSL with Damage Cleanup Services* starting on page 5-11.

Integration with Cisco Router

You can integrate IWSS on a network that uses a Cisco router at the gateway without changing the browser settings of the client machines.

To resolve the issue, integrate IWSS on the network through transparent proxy configuration by setting up the Policy-based Routing (PBR) on the Cisco router with the following policies:

Policy 1 Conditions:

- If the packet is from the IWSS server
- If the packet is for port 80/tcp and/or 443/tcp

Action: Routes the packet to the Internet.

Policy 2 Conditions:

- If the packet is from the local area network (other than the IWSS server)
- If the packet is for port 80/tcp and/or 443/tcp
- If the packet is not from the IWSS server

Action: Forwards the packet to the IWSS proxy port

For information on configuring policy-based routing, refer to the *Cisco Online Configuration Guide*.

Note: In IWSS 3.1, set IWSS to **transparent proxy** when implementing this setup. For additional information, see *Planning the HTTP Flow* starting on page 1-12.

Protecting an HTTP or FTP Server

If you are protecting the HTTP server, install IWSS and use the reverse proxy configuration.

From the Web console click **HTTP > Configuration > Proxy Scan Settings** and select **Reverse proxy**.

- Protected server—specifies the IP address of the protected HTTP server
- Port—specifies the TCP port of the protected HTTP server

Note: To simplify the deployment of the reverse-proxy configuration in an HTTP/HTTPS environment, IWSS can listen for the incoming (HTTPS) connection on a port specified by Port number under Enable SSL Port, and forward this traffic without scanning to port 443 of the protected server if Enable SSL Port is checked

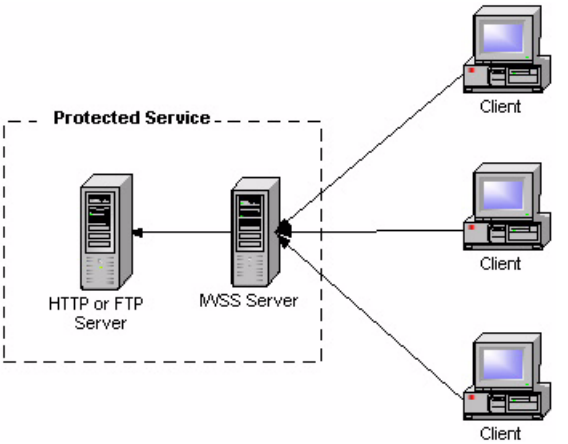


FIGURE A-2 Protecting a Dedicated Server

If you are protecting the FTP server, install IWSS and configure it to use an FTP proxy. From the Web console, click **FTP > Configuration > General** and select **Use FTP proxy**.

- Proxy server—specifies the IP address of the protected FTP server

- Port—specifies the TCP port of the protected server

Appendix B

Tuning and Troubleshooting

This appendix explains the following:

IWSS Performance Tuning

If you are experiencing issues with slow browsing performance, consider the following modifications and the InterScan Web Security Suite (IWSS) remote rating service.

URL Filtering

IWSS utilizes the Trend Micro URL Filtering Engine to perform URL categorization and reputation rating based on the data supplied by the Trend Micro Web Reputation feature. Trend Micro recommends using the default setting of a weekly update check to ensure that your installation has the most current URL Filtering Engine.

IWSS can control URL access based on Web Reputation feedback, the optional URL Filtering module, or a combination of both. The combination of Web Reputation and the URL Filtering module is a multi-layered, multi-threat protection solution provided by IWSS.

The optional URL Filtering module grants or denies Web access based on the category to which a URL belongs. Web Reputation grants or denies Web access based on whether the requested URL is a phishing or pharming threat, has hacking potential, or has a reputation score that deems it untrustworthy. Both the optional URL Filtering module and Web Reputation are controlled by the specifications you make in policies.

For further details, see Chapter 4 in the Administrator’s Guide.

LDAP Performance Tuning

When running IWSS to use the user/group name via proxy authorization identification method (LDAP), HTTP proxy performance becomes dependent upon the responsiveness of the LDAP directory server. In a worst case scenario, every HTTP request would require an LDAP query to authenticate the user's credentials, and another to retrieve group membership information for that user. These queries introduce latency in terms of the transmit/receive delay between IWSS and the LDAP server, and add load to the LDAP server itself.

LDAP Internal Caches

To reduce the amount of LDAP queries required, IWSS provides several internal caches:

- User group membership cache: This cache can store the group membership information for several hundred users. By default, entries in this cache will be valid for 48 hours, or until the cache fills (at which point entries are replaced, starting with the oldest). The time to live (TTL) for entries in this cache can be configured via the setting “user_groups_central_cache_interval” in the [user-identification] section of intscan.ini configuration file.
- Client IP to User ID cache: This cache associates a client IP address with a user who recently authenticated from that same IP address. Any request originating from the same IP address as a previously authenticated request will be attributed to that user, provided the new request is issued within a configurable window of time (15 minutes by default for HTTP, 90 minutes for ICAP) from that authentication. The caveat is that client IP addresses seen by IWSS must be unique to a user within that time period, thus this cache is not useful in environments where there is a proxy server or source NAT between the clients and IWSS, or where DHCP frequently reassigns client IPs. To enable or disable this cache, change the “enable_ip_user_cache” setting in the [user-identification] section of intscan.ini. To change the TTL of this cache, change the “ip_user_central_cache_interval” (unit is hours). For example, to create a TTL of 30 minutes, then enter “0.5”.
- User authentication cache: This avoids re-authenticating multiple HTTP requests passed over a persistent connection. When users pass the credential validation over a persistent connection, IWSS adds an entry (two important keys in one cache entry are the client’s IP address and the client’s username) in the user authentication cache so the subsequent requests over a keep-alive connection will not authenticate again. The client IP address and client’s username serve as two forward references, or links, to the “client IP to user ID cache” and “user group membership cache,” respectively. IWSS will thus still be able to retrieve the user’s connection information from both the IP-user and user-group caches.

When deploying IWSS with LDAP integration, it is important to consider the additional load that authenticating HTTP requests will place on the LDAP directory server. In an environment that cannot effectively use the client IP to user ID cache, the directory server will need to be able to handle queries at the same rate as IWSS receives HTTP requests.

Disable Verbose Logging When LDAP Enabled

Trend Micro recommends turning off verbose logging in the intscan.ini file, under the [http] section, “verbose” parameter) when LDAP is enabled for server performance reasons. Verbose logging is primarily used by software developers to identify abnormal application behavior and troubleshooting. In a production deployment, verbose logging is usually unnecessary.

If verbose logging is enabled and LDAP is also enabled, IWSS will log user authentication information and group membership information in the HTTP log in the `\Log` folder. Logs may contain hundreds of lines per user and therefore significantly consume disk space, depending on the amount of internal traffic and the number of groups a user is associated with. Verbose logging keeps the service busy with issuing I/O operations to the operating system. This may prevent the service from responding to HTTP requests in a timely fashion, hence latency may occur. In an extreme bursting HTTP traffic environment, it’s possible to observe significant delays when IWSS starts up in verbose mode.

System Parameters Tuning

Note: If you installed IWSS on Solaris 10, you do not need to perform this tuning procedure.

When you installed IWSS on Solaris 9, you can tune the semaphore and shared memory parameters to ensure consistent and stable IWSS performance under heavy network load. Add the following lines to the `/etc/system` file:

```
set shmsys:shminfo_shmmax=0x2000000
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256
set semsys:seminfo_semmap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semmsl=50
set semsys:seminfo_semopm=30
set semsys:seminfo_semmnu=100
```

Save the file and restart the operating system to make the changes take effect.

Determining the Correct Process/Thread Configuration

IWSS http daemon could be tuned to achieve better performance suited to your environment. The hybrid mode daemon uses a combination of threads and processes to balance the work load, understanding the peak time concurrent connections in the environment will help tune it.

The total no of threads (`max_tpc_proc * max_threads_per_proc`) run by the daemon should be higher than the peak connections the IWSS instance is expected to handle, For example, if you normally have 2000 peak concurrent sessions, you should increase the default `max_tpc_proc` to make up for the difference (`max_tpc_proc = 5, max_threads_per_proc = 500`).

Increasing Threads Vs Processes

- IIWSS performs best when the number of threads in a single process (`max_threads_per_proc`) is not more than 500.
- If your environment is not memory constrained, Trend Micro recommends increasing the `max_tpc_proc` and keep the `max_threads_per_proc` as close to 250 as possible.
- Each additional thread needs about 160-500K of memory to run.

Note: Changing `max_tpc_proc` or `max_threads_per_proc` requires you to restart all IWSS daemon processes for the change to take effect.

Troubleshooting

Troubleshooting Tips

- **Issue:** IWSS could not connect to the database specified in the Database Connection Settings page. The IWSS management console displays the following error message:

  ```
  JDBC-ODBC BRIDGE: [unixODBC]Could not connect to the server;
  Could not connect to remote socket.
  ```

  Solution:

  - Please check the ODBC connection and/or database server and try again.

- **Issue:** The IWSS management console displays an authentication error message.

  ```
  JDBC-ODBC BRIDGE: [unixODBC]FATAL: Password authentication
  failed for user.
  ```

  Solution:

  - Verify the user credential for the PostgreSQL Server and also ensure that the database settings are correct (**Administration > IWSS Configuration > Database | Database Setting**). If the problem persists, ensure that the permissions in the `etc/iscan/odbc.ini` file are correct.

Before Contacting Technical Support

When contacting Technical Support with your issues, having specific information can streamline the process:

Installation Problem

Collect the following information about your installation problem before contacting Trend Micro technical support to expedite the process.

1. IWSS version and build number
2. Screenshot of the exact error that appears during installation
3. The stage of the installation / un-installation where the problem occurs
4. The `/etc/iscan/log/install.log` installation log file

General Feature Problem

If you have problems with IWSS, collect the following information to give to Trend Micro support:

1. The system file(s) that describes the current state of IWSS.

   To compile these files, access the Web console and choose **Administration > Support** and then click **Generate System Information File**. This button is an extension of the case diagnostic tool (CDT), allowing you to package the current machine "state" at a click of a button.

   The system file(s) that IWSS generates from clicking the **Generate System Information File** button are packaged into a single file with the following format:

   `Info_YYYYMMDD_999999.tar.gz`

   Where `YYYY` is the current year, `MM` is the current month, and `DD` is the current day that the package file was generated. `999999` is the Unix time code.

   The system file(s) contains the following information:

   - **IWSS information**—Includes IWSS product version, engine version and build number, current pattern file (if available), and IWSS hot fixes and service pack information. Product and integration settings are also part of this information
   - **IWSS/system logs**—Includes IWSS logs and debug logs, logs generated by syslogd daemon (if system logs are enabled), and core dump file
   - **System/network information**—Includes the hardware configuration, operating system, build, system resource status, other application installed, and network information
   - **CDT-compliant configuration/plug-ins information**—Includes information about changes made to CDT as a result of IWSS adding a new component, such as a TMCM or MCP agent.

2. Core files are first created in the first directory listed below, and then moved to the second directory listed:
   - /etc/iscan/iwss/
   - /etc/iscan/iwss/UserDumps

Use these files when working with Trend Micro technical support to help diagnose the cause of your problem. To view the files yourself, use a program like GDB, the GNU Project debugger.

3. Log file for the day the issue occurred
   - All log files the day the issue occurred (logs are stored in `/etc/iscan/log` by default)
   - Make sure `verbose=1` is set in the [ftp], [http], and [notification] sections of the `intscan.ini` file
   - Make sure `log_trans=yes` is set under the [ftp] and [http] sections of the `intscan.ini` file
4. From the Web console, take a screen shot of the **Summary** > **Scanning** tab page.
5. Record the IWSS version number.
6. URL samples (if applicable)
7. Get a packet capture of the failing transaction using ethereal or tcpdump (if possible)

Appendix C

Additional IWSS Testing

In appendix explains the following:

Testing Upload Scanning

Trend Micro recommends that you test virus scanning of Web-based mail attachments.

To test virus scanning of Web-based mail attachments:

1. Open the IWSS console and click **HTTP > Scan Policies** in the main menu. Clear **Enable virus scanning**, and then click **Save**.
2. Download the test virus from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`
3. Save the test virus on your local machine.
4. Re-open the IWSS console, under **HTTP > Scan Policies** in the main menu, select **Enable virus scanning**, and then click **Save**.
5. Send a message with one of the test viruses as an attachment by using any Internet mail service. A message similar to the following should display in your browser.

FIGURE C-1 This warning screen shows the detection of an EICAR test virus.

Testing FTP Scanning

The following procedure contains instructions to test FTP virus scanning in stand-alone mode.

To test virus scanning of FTP traffic:

1. Download the test virus from the following page:

`http://www.eicar.org/anti_virus_test_file.htm`

2. Access the FTP server through IWSS working as the FTP proxy.
   For example, assume the following IP addresses: IWSS FTP proxy server (`10.2.10.2`), FTP server (`10.2.10.10`).
   Open a command line prompt and type the following:

   `ftp 10.2.10.2`

3. Log on as `user@host`. For example, if your FTP account name is `anonymous` and the IP address of the FTP server is `10.2.10.10`; then, log on as `anonymous@10.2.10.10`
4. Upload the test virus (for example, eicar_com.zip) by typing the command

   `put eicar_com.zip`

5. If you have configured the IWSS FTP proxy correctly, IWSS displays a message similar to the following.

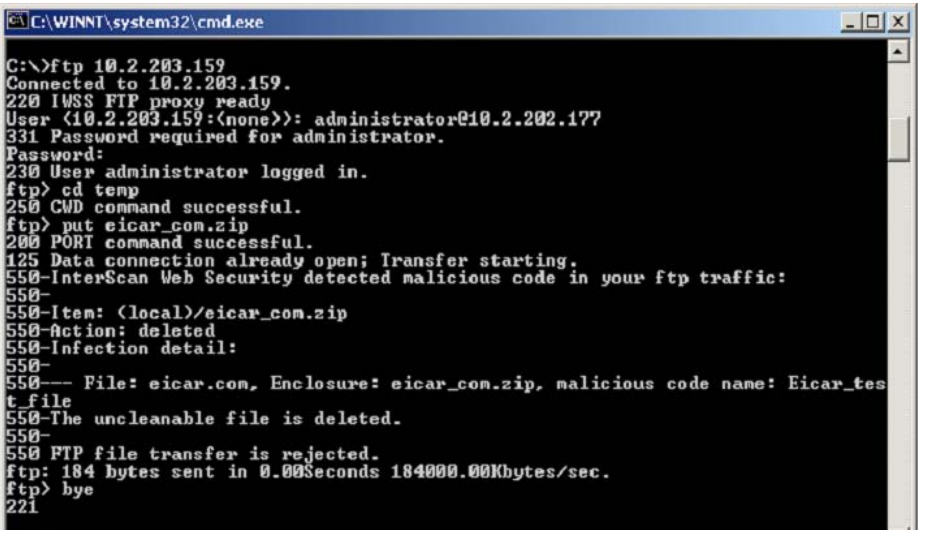


FIGURE C-2 This is a warning message that shows the detection of a virus in eicar_com.zip.

Testing URL Blocking

Before testing URL blocking, require your users to set the Web client's HTTP proxy to point to IWSS.

- For stand-alone mode, set the Web client's HTTP proxy to point to IWSS (for example, open Internet Explorer and click **Tools > Internet Options > Connections > LAN Settings > Use a proxy server**).
- For upstream proxy, set the Web client's HTTP proxy to point to IWSS (for example, open Internet Explorer and click **Tools > Internet Options > Connections > LAN Settings > Use a proxy server**). Open the IWSS console and click **HTTP > Configuration > Proxy Scan** in the left menu and enable **Dependent mode**. Type the proxy address and the port number.

To test URL blocking:

1. Open the IWSS console and click **HTTP > URL Access Control > URL Blocking** in the main menu and select **Enable URL blocking**.
2. In the **Match** field, type the full Web address, URL keyword, or exact-match string.
3. Click **Block**, and then click **Save**.
4. Open a Web browser and try to access the blocked Web site, a URL containing the string, or the exact-match string. A message similar to the following displays in the browser.

FIGURE C-3 A sample warning message for a blocked URL site.

Testing Download Scanning

To test virus scanning when downloading using HTTP or FTP over HTTP, attempt to download the test virus from the following Web site:

`http://www.eicar.org/anti_virus_test_file.htm`

FIGURE C-4 The above virus-warning screen displays if the system is set up properly.

If a client attempts to download an infected file, IWSS blocks other clients' access to that site for four hours by default. When other clients subsequently attempt to access the same URL that contained the virus, the user will see a URL blocking message instead of the virus-warning message.

Configure the default block time (in hours) by changing the parameter `infected_url_block_length` under the `[Scan-configuration]` section of the `intscan.ini` file.

Testing URL Filtering

Trend Micro recommends that you use the default setting to test URL filtering.

To test URL Filtering:

1. Click **HTTP > URL Filtering > Settings**.
2. From the **Approved URL List** tab, review the Web site categories that are classified as "Approved URL List."
3. From the main menu, click **HTTP > URL Filtering > Policies**.
4. Select **Enable URL filtering** and then click **Save**.

5. Click **URL Filtering Global Policy** and verify that the appropriate categories are blocked during work and leisure time.
6. Open a browser and access any site (for this example, `www.urlfilteredsite.com`), which is specified in a prohibited category.

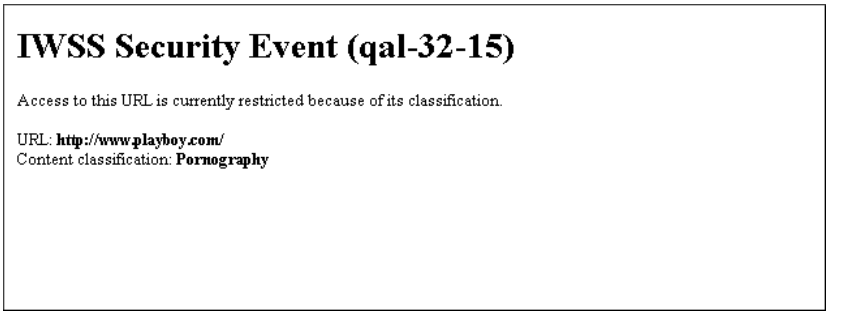


FIGURE C-5 The following message appears if the URL filtering is set up properly.

Testing Spyware Scanning

Perform the following procedure to test for spyware scanning.

To test Spyware scanning:

1. Open the IWSS console and click **Summary**.
2. Click the **Scanning** tab.
3. Enable spyware and other grayware categories for scanning by clicking **HTTP scanning**.
4. Click **HTTP > Scan Policy.**
5. Click the **Spyware/Grayware** tab and select the types of spyware/grayware which should be scanned.
6. Click the **Action** tab.
7. Under the **Uncleanable files** field, select the action setting (Delete, Quarantine, or Pass).

8. Click **Save**.
9. After a successful spyware detection, a sample message appears:

FIGURE C-6 A sample message after detecting a spyware with action "Delete" setting.

Testing PhishTrap

Perform the following procedure to test PhishTrap.

To test Phishtrap scanning:

1. Open the IWSS console and click **HTTP > URL Access Control > URL Blocking.**
2. Select **Enable URL blocking**.
3. Click the **Via Pattern File (PhishTrap)** tab.
4. Under **Block the following PhishTrap categories**, select all four categories (Phishing, Spyware, Virus accomplice, Disease vector).
5. Click **Save**.

6. After a successful phishing site detection, a sample message appears:

FIGURE C-7 A sample message after detecting a phishing site.

Testing Java Applet and ActiveX Scanning

Java applets and ActiveX controls are used on many Web pages to display interactive content or applications. One way to test your installation is to temporarily configure the global policy to block all applets and ActiveX controls, and then attempt to open Web pages that use them (to verify that the applet or object is blocked).

To test Java applet and ActiveX scanning:

1. Click **HTTP > Applets and ActiveX > Policies** from the main menu.
2. If necessary, select **Enable Applet/ActiveX security** and click **Save**.
3. Click **Applet/ActiveX Security Global Policy**.
4. On the **Java Applet Security Rules** tab, click **Block all Java applets** and click **Save**.
5. On the **ActiveX Security Rules** tab, click **Block all cabinet files** and **Block all PE format files** and click **Save**.
6. Open a Web browser and attempt to navigate to Web sites that use Java applets and ActiveX controls, for example, for stock price tickers or games. IWSS will block the mobile code from downloading and running in your browser.

Note: Blocking all Java applets and ActiveX controls may be too restrictive for your environment since it will prevent many legitimate Web sites from functioning properly. After testing, Trend Micro recommends going back to the **Applets and**

ActiveX Policy: Edit Global Policy screen to change the settings back to the default or your own less-restrictive configuration.

Testing IntelliTunnel Security

To test IntelliTunnel security:

1. Download the latest MSN Messenger from `http://get.live.com/messenger/overview`
2. Install MSN Messenger.
3. Enable IntelliTunnel in IWSS.
   a. Click **HTTP** > **IntelliTunnel**.
   b. Create a new policy or open an existing one.
   c. Select **MSN Messenger**.
   d. Click **Save**.
   e. Select the policy and then click **Deploy Policies**.
4. Configure proxy settings in Internet Explorer.
   a. Open Internet Explorer.
   b. Click **Tools** > **Internet Options**.
   c. Click the **Connections** tab.
   d. Click **LAN Settings**.
   e. Select **Use a proxy for your LAN**. These settings will not apply to dial-up or VPN connections.
   f. Enter the IWSS IP address in the **Address** field.
   g. Enter the IWSS HTTP listening port in the **Port** field. This value must match **HTTP** > **Configuration** > **Proxy Scan Settings** > **HTTP Listening Port** in IWSS.
   h. Click **OK** and then **OK** again.
   i. Close Internet Explorer.
5. Login to MSN Messenger.

An error message should appear stating that you were not able to sign into Windows Live Messenger at this time.

6. Disable IntelliTunnel.
   a. Click **HTTP > IntelliTunnel**.
   b. Open the policy.
   c. De-select **MSN Messenger**.
   d. Click **Save**.
   e. Select the policy and then click **Deploy Policies**.
7. Login to MSN Messenger.

   MSN Messenger should now work.

Note: MSN Messenger uses the proxy configuration in Internet Explorer, so this test should be valid without requiring any modifications to firewalls, network, etc. Other IM applications may not honor the proxy configuration in Internet Explorer and only fall back to port 80 if the standard port is blocked.

Appendix D

Post-Installation Tasks and Reference

This appendix explains the following:

Hardening Your OS

There are steps you can take before and after your OS installation to harden your OS.

Note: The recommendations in this guide may not fit everyone's needs. Carefully consider your unique environment and situation before implementing these recommendations.

OS Pre-installation Procedures for Hardening

Create your own policy before installing a Solaris system. The following questions act as a guide to help you create your policy:

- What is the server's primary function?
- Which services and external access ports are required for the majority of uses?
- Who needs access to accounts and to the server?
- What local applications do you need?

Trend Micro recommends that you:

- Start the installation process without a network connection. It is unlikely that your system can be attacked during the installation process if it is not connected to the network.
- Install the latest supported version of your operating system.
- Reconnect only when you are sure that you have taken all the necessary precautions to secure your server.

OS Installation Procedures for Hardening

Most operating system distributions provide the option of a customized installation. However, Trend Micro recommends that you only install the packages that you need and deactivate all the packages that you do not need.

Trend Micro recommends that you partition your hard disk during the installation process. Trend Micro cannot provide partition-sizing requirements because the correct sizing will depend both on your environment and on your plans for the server. Use the following recommendations as a guide:

- Create a dedicated partition for all log files to prevent a Denial of Service (DoS) attack.

Note: By default, IWSS installs the log file into the `/etc/iscan` directory. You need to move the log file location once you have completed the installation.

- If you install a mail host on the server, create a dedicated partition for the mailboxes
- Create a dedicated swap partition that is approximately four times the size of your RAM
- Most UNIX systems have moved to the hierarchical (FHS[2]) filesystem. Check that your partition sizing conforms to this standard.
- The installation process prompts you a password. Take the usual precautions when selecting a password. For example, include digits, meta, and capital characters.
- Create an unprivileged user account to use as your default login.

Additional Post-OS Installation Procedures

Trend Micro recommends that you conduct the following post-installation tasks after completing the installation process:

1. Fortify your system using recommended updates and security patches for all of the installed packages.

   You can download security patches from the following source:

   http://sunsolve.sun.com/show.do?target=patchpage

2. Move your system into single-user mode (run level s in Solaris) when installing patches to minimize the risk of conflicts between running processes and the packages that you are upgrading.
3. Remove all unassigned users from `/etc/passwd` (`/etc/shadow`) and from the groups file.

Appendix E

Maintenance and Technical Support

This appendix explains the following:

Product Maintenance

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to your product. To find out whether there are any patches available, visit the following URL:

`http://www.trendmicro.com/download/`

The Update Center screen displays. Select your product from the links on this screen:

Clicking the link for InterScan Web Security Suite takes you to the Update Center page for IWSS. Scroll down to review the patches that are available.

Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the installation instructions in the readme.

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Note: If the Maintenance Agreement expires, your License Agreement will not.

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will be alerted of the pending discontinuation. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

`https://olr.trendmicro.com/registration/`

Renewing Your Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If your Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

To purchase renewal maintenance, contact the same vendor from whom you purchased the product. A Maintenance Agreement, extending your protection for a year, will be sent by post to the primary company contact listed in your company's Registration Profile.

To view or modify your company's Registration Profile, log on to the account at the Trend Micro online registration Web site:

`https://olr.trendmicro.com/registration`

You are prompted to enter a logon ID and password.

To view your Registration Profile, type the logon ID and password created when you first registered your product with Trend Micro (as a new customer), and then click **Log on**.

Contacting Technical Support

To contact Trend Micro Technical Support, visit the following URL:

`http://kb.trendmicro.com`

Then, click the link for one of the following regions:

- Asia/Pacific
- Australia and New Zealand
- Europe
- Latin America
- United States and Canada

Follow the instructions for contacting support in your region.

In the United States, Trend Micro representatives can be reached via phone, fax, or email. Our Web site and email addresses follow:

`http://www.trendmicro.com`

`support@trendmicro.com`

For regional contact information and the specific technical support numbers for all the regional and worldwide offices, open the IWSS management console and choosing **Support** from the menu in the management console's banner.

General US phone and fax numbers follow:

```
Voice: +1 (408) 257-1500 (main)
```

```
Fax: +1 (408) 257-2003
```

Our US headquarters is located in the heart of Silicon Valley:

```
Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
```

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The “virus doctors” at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging risks. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support.

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.

Also available in Knowledge Base are product FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

`http://kb.trendmicro.com`

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

Known Issues

Known issues are features in your IWSS software that may temporarily require a workaround. Known issues are typically documented in section 7 of the Readme document you received with your product. Readme files for Trend Micro products, along with the latest copies of the product manuals, can also be found in the Trend Micro Update Center:

`http://www.trendmicro.com/download/`

Known issues can be found in the technical support Knowledge Base:

`http://kb.trendmicro.com`

Trend Micro recommends that you always check the Readme file for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

`http://subwiz.trendmicro.com/SubWiz`

Click the "Submit a suspicious file/undetected virus" link. The following screen displays.

You are prompted to supply the following information:

- **Email**: Your email address where you would like to receive a response from the antivirus team.
- **Product**: The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Number of Infected Seats**: The number of users in your organization that are infected.
- **Upload File**: Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word "virus" as the password—then select the protected zip file in the **Upload File** field.
- **Description**: Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any risks it may contain and return the cleaned file to you, usually within 48 hours.

Note: Submissions made via the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you click **Next**, an acknowledgement screen displays. This screen also displays a case number for the problem you submitted. Make note of the case number for tracking purposes.

If you prefer to communicate by email, send a query to the following address:

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAV, or 877-873-6328

Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

`http://www.trendmicro.com/vinfo/`

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of risks expected to trigger in the current week, and describes the 10 most prevalent risks around the globe for the current week
- View a Virus Map of the top 10 risks around the globe
- Consult the Virus Encyclopedia, a compilation of known risks including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the risk, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
    - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other risks
    - The Trend Micro *Safe Computing Guide*
    - A description of risk ratings to help you understand the damage potential for a risk rated Very Low or Low vs. Medium or High risk
    - A glossary of virus and other security risk terminology
- Download comprehensive industry white papers

- Subscribe, free, to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters
- Read about TrendLabs, Trend Micro's global antivirus research and support center

To open Security Information:

1. Open the IWSS management console.
2. Click **Security Info** from the drop-down menu at the top-right panel of the screen. The **Security Information** screen displays.

About Trend Micro

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway–gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of risks to information, by offering centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point, before they ever reach the desktop.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

`http://www.trendmicro.com`

Index