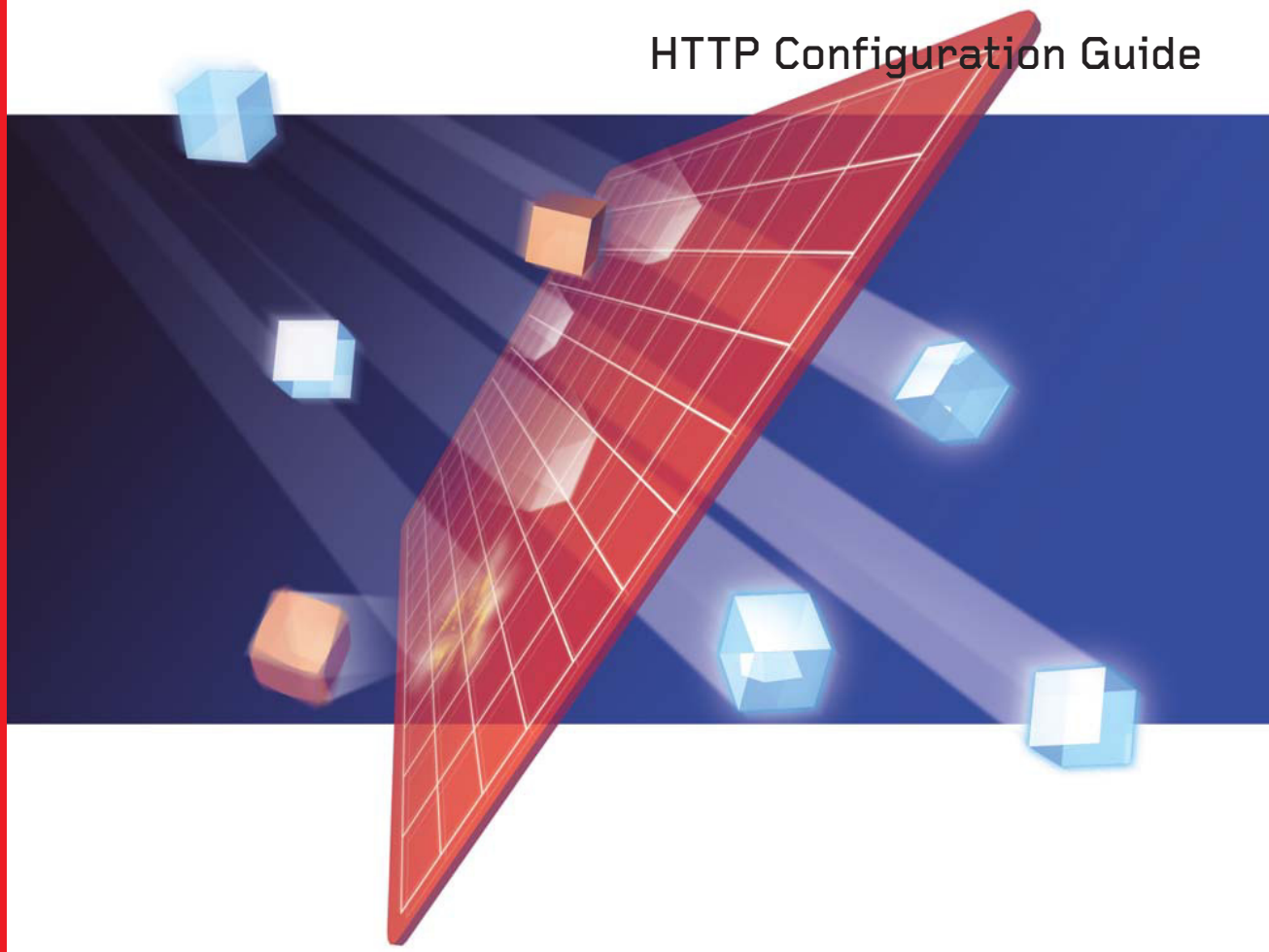
TREND MICRO™
InterScan™ VirusWall™ 6

Integrated virus and spam protection for your Internet gateway

for Linux™

HTTP Configuration Guide



TREND MICRO™

Should we need to make changes to this document and to the products described herein, we shall however inform you of such changes when they have occurred. Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

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

Document Part No. IVEM62711/60419

Release Date: July 2006

Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698; and 6,119,165

The *Trend Micro InterScan VirusWall 6 for Linux HTTP Configuration Guide* provides detailed information about how to use the HTTP-related features of the software. Read it before using the software.

Additional information about how to use specific features within the software is available in the online help for this product and in the online Knowledge Base at the Trend Micro Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any other 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

Chapter 3: Configuring HTTP Anti-Phishing Settings

Chapter 4: Configuring HTTP Anti-Spyware/Grayware Settings

Chapter 5: HTTP URL Blocking and Filtering

Chapter 1

Preparing InterScan VirusWall to Protect HTTP Traffic

This chapter includes the following topics:

How InterScan VirusWall Scans HTTP Traffic

With InterScan VirusWall you can monitor HTTP traffic to maintain security at your network gateway. You can enable or disable the scanning of HTTP traffic during installation or at any time later, through the Summary page of the Web console.

HTTP services include:

- Scanning for viruses and security risks in uploads and downloads
- Phishing site detection
- Spyware and other grayware detection
- URL blocking
- URL filtering
- Configuration of HTTP server mode and listening port

The Web (HTTP) tab on the InterScan VirusWall Summary screen provides statistics about the number of infected files, spyware, grayware, and phishing incidents that the InterScan VirusWall HTTP scanning function (HTTP VirusWall) has detected in uploaded and downloaded files. The Summary screen also lists the number of URLs that HTTP VirusWall has blocked and filtered.

Enabling or Disabling HTTP Scanning Services

You can enable or disable HTTP scanning services in two ways:

1. During installation, in the Preconfiguration screen. (See the *InterScan VirusWall 6 Getting Started Guide* for installation instructions.)
2. On the Summary screen, Web (HTTP) tab. Select or clear the **Enable HTTP Traffic** check box shown in figure 1-1, “Summary screen, Web (HTTP) tab, showing enabled check box,” on page 1-3.

When you enable HTTP scanning services, the following default settings apply to the HTTP scan types:

TABLE 1-1. HTTP scan types and their default settings

HTTP Scan Type	Default Setting
Virus/malware scanning	Enabled
Anti-phishing	Enabled
Anti-spyware	Enabled
URL blocking	Enabled
URL filtering	Disabled

HTTP scanning statistics for virus/malware detection, spyware/grayware detection, URL blocking/anti-phishing, and URL filtering appear in the HTTP Summary table.

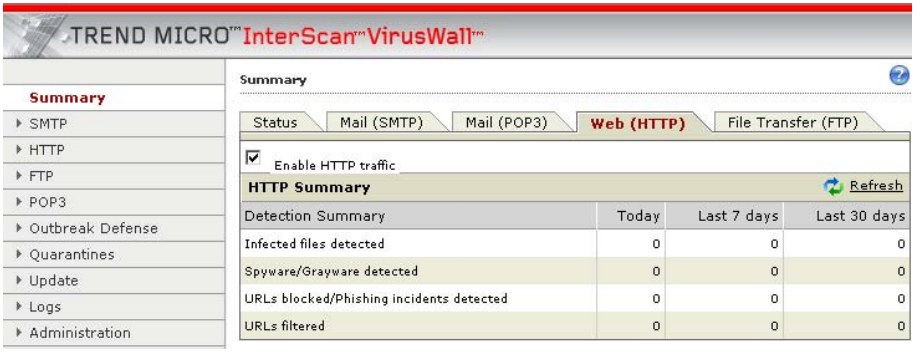


FIGURE 1-1. Summary screen, Web (HTTP) tab, showing enabled check box

Configuring InterScan VirusWall to Scan HTTP Traffic

The HTTP scanning feature of InterScan VirusWall for Linux (HTTP VirusWall) offers the InterScan VirusWall administrator a great deal of flexibility in configuring how the program will behave.

Note: Before InterScan VirusWall can scan HTTP traffic, it must have information about how to work with the HTTP servers in your network.

InterScan VirusWall scans the HTTP traffic flow to detect viruses and other security risks in uploads and downloads. HTTP VirusWall is highly configurable. For example, you can set the types of files to block at the HTTP gateway and how InterScan VirusWall scans compressed and large files to prevent performance issues and browser timeouts.

First set up HTTP VirusWall to work with your HTTP server before you begin set up URL filtering and blocking and begin configuring how HTTP VirusWall will scan for viruses and other malware, Phishing attempts, and spyware/grayware.

Consult the *Trend Micro InterScan VirusWall 6 for Linux Getting Started Guide* (the printed manual) for guidance on deploying InterScan VirusWall in your network topology.

Four Deployment Modes

InterScan VirusWall can protect your users and network resources from HTTP-borne risks in one of these modes:

- **Standalone mode.**—As a forward proxy
- **Dependent mode**.—As a secondary proxy
- **Reverse proxy mode.—**As a reverse proxy in reverse mode
- **Transparent proxy.**—As a transparent proxy when an L4 switch is installed

In all configurations, InterScan VirusWall resides between the clients and a Web server.

Standalone Mode

The standalone mode configuration protects clients from receiving malicious HTTP-borne risks from a server. This is the most common configuration, and the typical use case is to protect Web users on your network from receiving malicious Internet downloads. In the standalone proxy topology shown in figure 1-2, “HTTP VirusWall deployed in standalone mode,” on page 1-5.

Administrators typically install InterScan VirusWall and the clients that it protects within the same LAN.

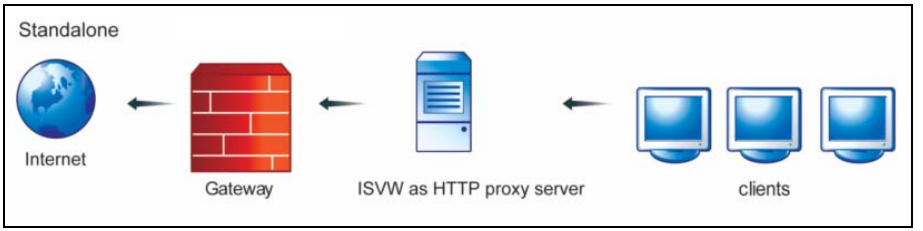


FIGURE 1-2. HTTP VirusWall deployed in standalone mode

Dependent Mode

Dependent mode is similar to standalone mode, except that InterScan VirusWall is dependent upon an upstream proxy to access the HTTP server. Dependent mode protects clients from receiving malicious HTTP-borne risks from a server.

The typical use case is to protect Web users on your network from receiving malicious Internet downloads. In dependent mode, InterScan VirusWall and the clients that it protects are typically installed within the same LAN, and InterScan

VirusWall depends on an upstream proxy to access the HTTP server. Figure 1-3 shows a typical topology for dependent mode.

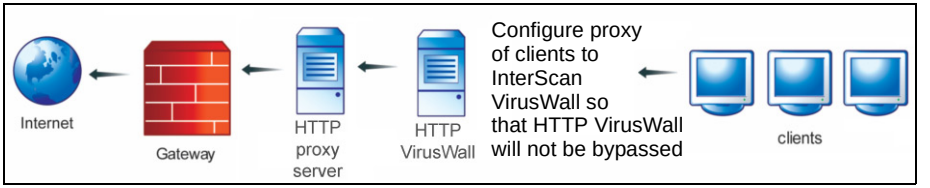


FIGURE 1-3. HTTP VirusWall deployed in dependent mode

Reverse Mode

The Reverse mode configuration places InterScan VirusWall between a Web server and the clients of that server. This configuration is less common, and administrators typically used it to protect Web servers from having malicious content uploaded to them. In the reverse mode proxy topology, InterScan VirusWall is typically installed close to the Web server that it protects.

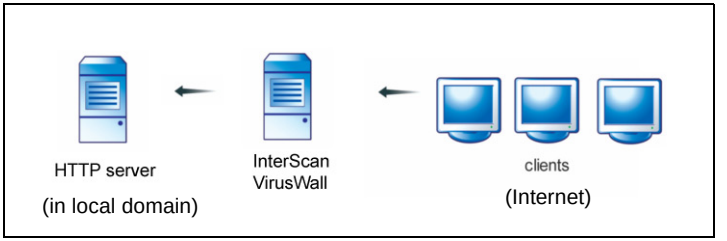


FIGURE 1-4. InterScan VirusWall in a reverse mode deployment

Configuring the HTTP Proxy Settings

Before InterScan VirusWall can monitor HTTP traffic, you need to specify the configuration settings of the HTTP server. Figure 1-5, “HTTP Configuration screen,” on page 1-7 shows the settings that you can choose from.

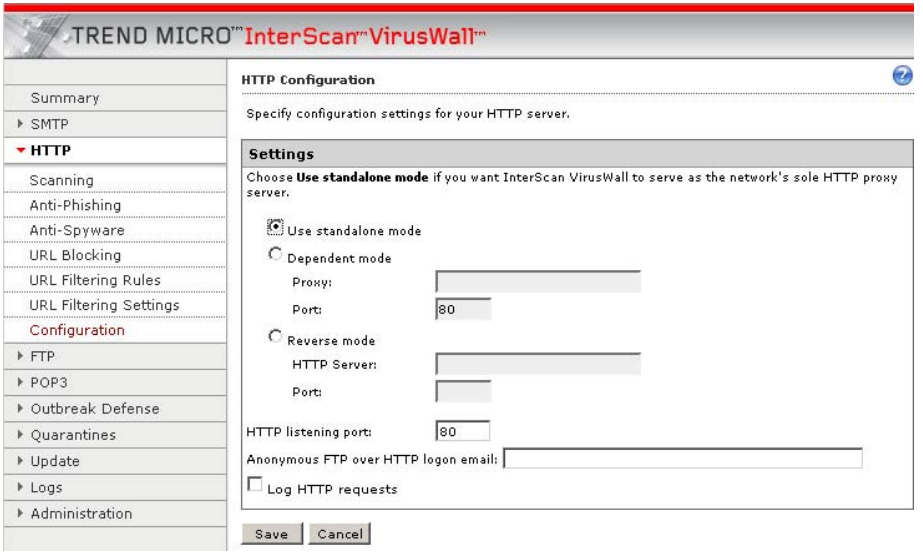


FIGURE 1-5. HTTP Configuration screen

Setting Deployment Mode

The first task in configuring HTTP VirusWall to work in your network environment is to select which deployment mode you have chosen (standalone, dependent, or reverse). See the topology section of the *Trend Micro InterScan VirusWall Getting Started Guide* for guidance on deploying InterScan VirusWall.

Note: To have InterScan VirusWall serve as the only HTTP proxy server on your network, choose standalone mode.

To configure settings based on your deployment:

1. Click **HTTP** > **Configuration**. The HTTP Configuration screen appears.
2. Select one of the three main options:
   - Use standalone mode
   - Dependent mode
   - Reverse mode
3. If you have selected dependent mode:
   a. Type the IP address or name of your HTTP proxy server in the **Proxy** field.
   b. Type the port number of your HTTP proxy server in the **Port** field.
4. If you have selected Reverse mode:
   a. Type the IP address or domain name of the HTTP server to protect.
   b. Type the port number of your HTTP server.
5. Click **Save.**

Other HTTP Configuration Information

After you have selected your deployment mode, give HTTP VirusWall the rest of the information that it needs to work within your network and then choose your HTTP logging option.

To complete HTTP settings after selecting deployment mode:

1. In the **HTTP listening port** field, type the listening port on which HTTP VirusWall will listen to your HTTP traffic or accept the default value of 8080.
2. In order for your users to access FTP servers using anonymous FTP over HTTP, type a legitimate email address in **Anonymous FTP over HTTP logon email**. (For more information about this rarely used function, see *About Anonymous FTP over HTTP Logon Email* on page 1-9.)
3. You can analyze HTTP traffic using InterScan VirusWall. To record all HTTP requests in a log for later analysis, select **Log HTTP requests**. By default, this function is disabled.

Tip: For more information about querying HTTP logs and other kinds of logs, see the Logs section of the *Trend Micro InterScan VirusWall 6 Getting Started Guide.*

About Anonymous FTP over HTTP Logon Email

The purpose of the field called **Anonymous FTP over HTTP logon email** may not be readily apparent. Most anonymous FTP servers do not require a password for anonymous login sessions. However, some require not only a password, but that the password consist of a legitimate, well-formed email address to a functioning Internet domain. In FTP over HTTP, the proxy server acts as an HTTP proxy on the client side but acts as an FTP client on the server side. If a client intends to log on anonymously, you need to have this email address. The configuration decides what email address to use as the password in anonymous logon.

Setting the Proxy on Client Browsers

In addition to configuring HTTP VirusWall in the HTTP Configuration screen of the Web console, ensure that all clients in your network are using the correct proxy so that HTTP VirusWall can scan traffic going to and from each client machine.

If you deploy InterScan VirusWall in standalone mode, there is no change to the existing proxy, as HTTP VirusWall simply takes the place of your HTTP proxy.

If you connect InterScan VirusWall directly to the HTTP proxy (that is, if you deploy it in dependent mode), ensure that the proxy settings of all clients in your network refer to InterScan VirusWall, which is between the client browsers and the original HTTP proxy.

If your network is running Microsoft™ Windows™ machines, you can deploy these proxy settings automatically by using Windows Domain Controller. Consult your Microsoft documentation for instructions on deploying proxy settings automatically.

Chapter 2

Configuring HTTP Virus Scans

This chapter includes the following topics:

Overview

InterScan VirusWall scans the HTTP traffic flow to detect viruses and other security risks in uploads and downloads. HTTP scanning is highly configurable. For example, you can configure the types of files to block at the HTTP gateway and how InterScan VirusWall scans compressed and large files to prevent performance issues and browser timeouts.

As an administrator, you can configure HTTP Scanning for viruses and other malware when you select **HTTP > Scanning**.

Enabling HTTP Virus Scanning

Enabling HTTP scanning services during installation or on the InterScan VirusWall Summary screen, Web (HTTP) tab enables scanning of HTTP traffic that flows through InterScan VirusWall. This setting by default enables HTTP virus scanning.

HTTP VirusWall gives you the flexibility to individually disable the scanning of URL filtering, URL blocking, and three kinds of security threats. This section addresses only the scanning of HTTP traffic for viruses/malware.

To enable or disable HTTP virus scanning:

1. On the left-side menu, select **HTTP > Scanning**. The HTTP Scanning screen appears, displaying the Target tab.
2. At the top of the Target tab contents, select or deselect the **Enable HTTP Scanning** check box.
3. Click **Save** at the bottom of the screen.

Specifying Targets for HTTP Virus Scanning

The Target tab of the HTTP Scanning screen contains several sections:

- Block Selected File Types
- Files to Scan (if not blocked)
- Compressed File Handling
- MIME Type Exceptions
- Large File Handling

For discussions of the above sections, see the corresponding headings below.

File Types to Block

InterScan VirusWall can block selected files by file type. Follow the procedure below to select file types to block from all HTTP traffic.

To block files by type:

1. On the left-side menu, select **HTTP > Scanning**. The HTTP Scanning screen appears, displaying the Target tab.
2. In the Block Selected File Types section, select the check box next to each file type to block. (See Table 2-1, “File formats to be blocked, by file type in the Web console,” on page 2-4, for a detailed list of file types represented by each grouping in this section.)
3. If you do not see the file type that you wish to block in list, select the **Other file types** check box and type the file extensions of the file types that you wish to block. Type the extensions of the other file types to block without an asterisk or a period, and separate multiple entries with a semicolon, as shown below:

   ```
   rar;vid;wav
   ```

4. Click **Save** at the bottom of the screen.

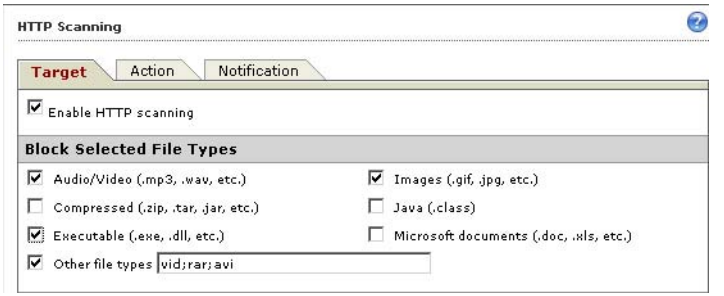


FIGURE 2-1. HTTP Scanning screen, Block Selected File Types section

Table 2-1 below lists file types represented by the categories in the Block Selected File Types section of the Target tab.

TABLE 2-1. File formats to be blocked, by file type in the Web console

File Type	Description
Compressed:	
mscomp	MSCOMP
cpio	By default, cpio creates binary format archives, so that they are compatible with older cpio programs. When it is extracting files from archives, cpio automatically recognizes which kind of archive it is readingand can read archives created on machines with a different byte-order.
lha	An archiver that was written in Japan in the 1980s.Dozens of archivers are based on its source code.
ar, arj	A popular file compression/archival tool, available for UNIX/Linux, DOS/ Windows, and other operating systems. Files compressed in this manner typically have .arj or .ar extensions.
tar	A file packaging tool included with UNIX/Linux for the purpose of assembling a collection of files into one combined file for easier archiving.
rar	A file format created by Eugene Roshal for his WinRar / Rar / Unrar programs. MIME type: application/x-rar-compressed

TABLE 2-1. File formats to be blocked, by file type in the Web console (Continued)

File Type	Description
gzip	Gnu zip
zip	PK Zip
mscab	Microsoft Cabinet file
Audio/Video:	
av	audio
wav	Microsoft RIFF
midi	MIDI (Musical Instrument Digital Interface)
mp3	MP3
voc	Creative Voice Format
Executable:	
com	COM file / DOS COM
exec	executable
exe	DOS executable
lnk	Windows NT/95 shortcut
binhex	Binhex (BINary HEXadecimal): A method for converting non-text files (non-ASCII) into ASCII. This is needed because Internet e-mail can only handle ASCII.
base64	MIME base64
Java:	
java	Java applet
Microsoft documents:	
msdoc	Microsoft Word document/DOS 4.0/5.0
msppt	Microsoft PowerPoint presentation
msexl	Microsoft Excel 95/97
mswri	Microsoft Windows Write
mscal	Microsoft Windows Calendar

TABLE 2-1. File formats to be blocked, by file type in the Web console (Continued)

File Type	Description
msmdb	Microsoft Access database
msproj	Microsoft Project
hlp	Microsoft Help file
rtf	Microsoft Rich Text Format
Images:	
icon	Microsoft Windows icon
pcx	PC Paintbrush
fli	Autodesk Animator (FLI)
bmp	Windows bitmap
jpeg	Joint Photographic Experts Group image file
tiff	Tagged Information Format File
ras	SUNRaster (RAS)
psd	Adobe Photoshop (PSD)
gif	Graphics Information Format

Specifying File Types to Scan

For traffic remaining after the above blocking criteria have taken effect, choose which files to scan. Choose from the following options:

- All scannable files
- IntelliScan: uses *true file type* identification
- Specified file extensions...

All Scannable Files

Some files, such as those that are password protected or corrupted, cannot be scanned. The All scannable files option scans all files other than those.

Before HTTP VirusWall scans a file, it checks its data type and determines whether to proceed with the scan. HTTP VirusWall does not scan files that are unscannable.

Instead, HTTP VirusWall performs a user-configurable action against the file. The default action for unscannable files is clean and block. You can set the action that HTTP VirusWall takes from the HTTP > Scanning screen, Action tab.

Unscannable files consist of two kinds of files:

- Files that HTTP VirusWall judges to be safe. These kinds of files cannot harbor viruses, Trojans, worms, or spyware or other grayware.
- Files that HTTP VirusWall cannot scan for technical reasons, such as:
  - Encrypted and password-protected files
  - Files that exceed the configured scanning restrictions
  - Files with an unsupported data type

IntelliScan

Most antivirus solutions today offer you two options in determining which files to scan for potential threats. Such products either scan all files (the safest approach) or only those files with certain file name extensions (considered the most vulnerable to infection). But recent developments involving files being "disguised" through having their extensions changed has made this latter option less effective.

IntelliScan is a Trend Micro technology that identifies a file's "true file type," regardless of the file name extension. IntelliScan uses a method of identifying which files to scan that is more efficient than the **All scannable files** option.

Note: IntelliScan examines the header of every file but, based on certain indicators, selects only files that it determines are susceptible to virus scanning.

Because IntelliScan scans only files that are particularly vulnerable to infection, using IntelliScan brings you the following benefits:

- **Performance optimization**.—IntelliScan uses fewer system resources than the **All scannable files** option.
- **Shorter scanning period.**—The scan time is shorter than the time needed by the **All scannable files** option.

Specified File Extensions

Scan only selected attachment types by file name extension. InterScan VirusWall scans only those file types that are explicitly specified in the associated popup window:

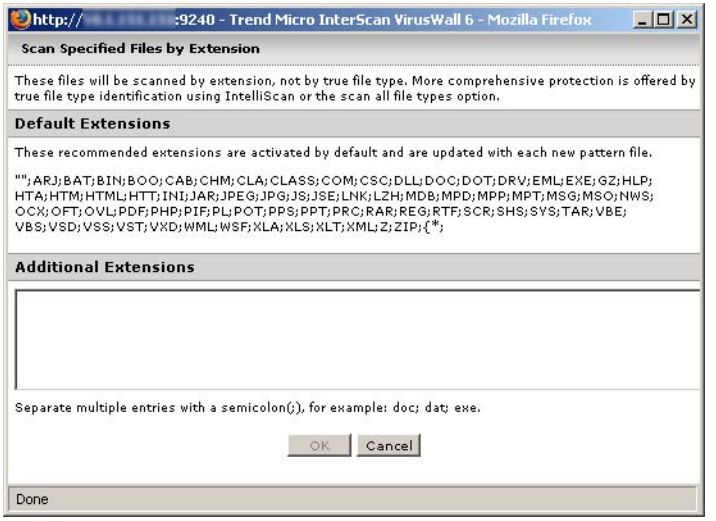


FIGURE 2-2. The Specified Files by Extension popup window

Selecting either of the first two options is straightforward. However, the third option involves a few more steps, as outlined below.

To select specified file extensions for scanning (incoming traffic):

1. From the left menu, select **HTTP > Scanning** and ensure that the **Target** tab is active.
2. Under **Files to Scan (if not blocked)**, select **Specified file extensions.**
3. Click the hyperlinked word extensions in **Specified file extensions.** The Specified Files by Extension popup window appears. The window lists the default extensions and displays an input field for additional extensions.
4. To add extensions to the default list, type them in the **Additional Extensions** field, separating multiple entries with a semicolon (;).

5. Click **OK** to save and click **OK** in the confirmation window to close the popup box.

   By default, InterScan VirusWall scans files with the following file name extensions:

```
"";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DLL;DOC;
DOT;DRV;EML;EXE;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;
JPG;JS;JSE;LNK;LZH;MDB;MPD;MPP;MPT;MSG;MSO;NWS;OCX;
OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RTF;SCR;
SHS;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;
XLT;XML;Z;ZIP;{*;
```

FIGURE 2-3. The file extensions of those files scanned by default when *Specified file extensions* is selected

Tip: Use the **Specified file extensions** option to modify the default scan list.

Configuring Processing of Compressed Files

Settings for handling compressed files are set in different places based on whether the traffic is incoming or outgoing.

To specify how to handle compressed files during HTTP scanning:

1. On the left side menu, select **HTTP > Scanning**. The HTTP scanning screen opens, displaying the Target tab.
2. Under **Compressed File Handling**, select your preferred option:
   - To scan all compressed attachments, select **Scan all compressed files**. This is the most secure setting, and it is the default.
   - To skip all compressed attachments, select **Do not scan compressed files**. HTTP VirusWall will not scan any compressed attachments.
   - To scan compressed attachments based on the number of files, the file size after decompression, the number of compression layers, and the

compression ratio, select **Do not scan compressed files if** and then specify the conditions under which compressed attachments should not be scanned.

- **Extracted file count exceeds**—the maximum number of files within the compressed attachment (0 means no limit).
- **Extracted file size exceeds**—the maximum file size after decompression. InterScan VirusWall scans only individual files within the limit.
- **Number of layers of compression exceeds**—the maximum number of compression layers.
- **Extracted file size/compressed file size ratio exceeds**—the maximum size ratio before and after compression. InterScan VirusWall scans only individual files within the limit.

3. Click **Save** at the bottom of the screen.

MIME Type Exceptions

In this section you can create a list of MIME types that you do not wish to scan.

MIME (Multipurpose Internet Mail Extensions) is a standard for multipart, multimedia electronic mail messages and World Wide Web hypertext documents. MIME provides the capability for transferring over the Internet nontextual data, such as graphics, audio, and fax. A MIME type describes the kind of data that a server is transmitting, for example video/QuickTime for certain kinds of video, or text/html for browser hypertext markup language content.

Separate multiple entries with a semicolon (;).

Table 2-2 lists file types that you can enter in the HTTP virus scanning MIME Type Exceptions field to prevent scanning of the corresponding MIME content types.

TABLE 2-2. File types, mapped to MIME types

File Type	MIME Content Type	File Type	MIME Content Type	File Type	MIME Content Type
afc	audio/aiff	av	video/avs-video	bin	application/x-binary
afc	audio/x-aiff	audiovideo	video/	binhex	application/binhex
ani	application/octetstream	base64	application/base64	binhex	application/binhex4
arc	application/octetstream	bin	application/mac-binary	binhex	application/macbinhex
arj	application/octetstream	bin	application/mac-binary	binhex	application/macbinhex40
asf	video/x-ms-asf	bin	application/octetstream	binhex	application/x-binhex40
bin	application/xmacbinary	bmp	image/bmp	bmp	image/x-windowsbmp
bw	image/x-sgi-bw	bzip2	application/x-bzi2	cgm	image/cgm
cmx	application/x-cmx	cmx	image/x-cmx	com	application/octetstream
core	application/octetstream	cpio	application/x-cpio	dcr	application/x-director
doc	application/wordperfect	dwg	application/acad	dwg	application/x-acad
dwg	drawing/x-dwg	dwg	image/vnd.dwg	dwg	image/x-dwg
eps	application/postscript	eps	image/x-eps	exec	application/octetstream
exec	application/x-msdownload	exe	application/octetstream	fh9	image/x-freehand
fli	video/x-fli	fm	application/vnd.framemaker	gif	image/gif
gzip	application/x-gzip	gzip	encoding/x-g	hpexe	application/octetstream
iff	audio/x-aiff	java	text/x-javasource	java	application/java-class
java	application/x-javaapplet	java	application/x-javavm	java	text/x-javasource

TABLE 2-2. File types, mapped to MIME types (Continued)

File Type	MIME Content Type	File Type	MIME Content Type	File Type	MIME Content Type
java	application/ java-class	java	application/ x-javaapplet	java	application/ x-javavm
jpeg	image/jpeg	jpeg	image/pjpeg	lha	application/x-lha
lisp	applica- tion/x-lisp	maud	audio/x-ma	ud	midi audio/midi
mif	application/x-mif	mng	video/x-mng	mp3	audio/mpeg
mp3	audio/mpeg3	mp3	audio/x-mpeg-3	mp3	video/mpeg
mp3	video/x-mpeg	mpeg	video/mpeg	mscab	application/ x-cainetwin32-x86
msdoc	application/ msword	msexl	application/excel	msexl	application/ x-msexcel
msexl	application/ x-excel	msexl	application/ vnd.ms-excel	msmdb	application/ x-msaccess
msppt	application/ mspowerpoint	msppt	application/ powerpoint	msppt	application/ vnd.mspowerpoint
msproj	application/ vnd.msproject	msproj	application/ x-msproject	msproj	application/ x-project
mswri	application/ mswrite	pcx	image/x-pcx	pdb	application/ x-pilot-pdb
pdf	application/pdf	pdf	application/x-pdf	pfb	application/x-font
pict	image/pict	pict	image/x-pict	picture	image
png	image/png	ppm	image/ x-portablepixmap	ps	application/ postscript
psd	application/ octetstream	qtm	video/quicktime	ra	audio/ vnd.mrealaudio
ra	audio/ xpnrealaudio	ra	audio/xrealaudio	rar	application/rar
ras	image/ x-cmuraster	ras	image/cmu-raster	risc	application/ octetstream
rmf	application/ vnd.m-realme- dia, g_audiovideo	rtf	application/rtf	rtf	application/x-rtf
rtf	text/rich text	scm	application/ vnd.lotusscreen- cam	scm	application/ x-lotusscreencam

TABLE 2-2. File types, mapped to MIME types (Continued)

File Type	MIME Content Type	File Type	MIME Content Type	File Type	MIME Content Type
scm	application/ x-screencam	scm	video/x-scm	sf	audio/x-sf
swf	application/ x-shock-wave-flash	tar	application/x-tar	tga	image/tga
tiff	image/tiff	tnef	applica-tion/ms-tnef	tnef	application/ vnd.mstnef
txt	text/plain	uuencode	text/x-uuencode	zip	application/zip
voc	audio/voc	voc	audio/x-voc	wav	audio/wav
wbc	application/ x-webshots	wmf	application/ x-msmetafile	wmf	image/x-wmf

Handling Large Files

In the Large File Handling section, configure how HTTP VirusWall will handle large files. The two major options are:

- Do not scan files larger than *x* KB/MB/GB
- Enable special handling when a files is larger than *x* bytes/KB/MB

The first option is self-explanatory. However if you choose the second option, there is one more decision to make: Would you like for HTTP VirusWall to scan each Web page gradually, while loading it—and stop the connection if a virus is found, or would you prefer to load each page first and then scan it.

In the Web console, these options appear as:

- Deferred scan: load part of the page before scan begins, and then stop the connection if a virus is found
- Scan-behind: load the page first, and then scan afterwards (highest risk of infection)

Tip: The default options is **Deferred scan** because, even though it may slightly slow the loading of each Web page, it is much safer than the second option.

Remember to click **Save** at the bottom of the screen to save all of your changes.

Specifying Action to Take upon Detection of a Virus

In the Action tab of the HTTP Scanning screen, specify the action to take on infected files. See figure 2-4, “The HTTP Scanning screen, Action tab,” on page 2-14 for the options to choose from.

FIGURE 2-4. The HTTP Scanning screen, Action tab

If you keep the default choice of Clean, select which action to take on any files that are uncleanable. Choose from the following options in the drop-down menu:

- Quarantine
- Block (the default)
- Pass (not recommended)

Click **Save** at the bottom of the screen to save your choice.

When InterScan VirusWall cannot successfully clean a file, it labels the file “uncleanable” and performs the user-configured action for uncleanable files. The default action is block. InterScan VirusWall records all virus events and associated courses of action in the log file.

Some common reasons why HTTP VirusWall cannot perform the clean action are as follows:

- The file contains a Trojan, worm, or other executable program. To stop an executable from executing, HTTP VirusWall must completely remove it.
- The file is a backup file that HTTP VirusWall previously created when attempting to clean the file.
- HTTP VirusWall does not support the compression format used to compress the file.
- An unexpected problem prevents HTTP VirusWall from cleaning, such as:
    - The temp directory that acts as a repository for files requiring cleaning is full
    - The file is locked or is currently executing
    - The file is corrupted
    - The file is password protected
    - The file is located in the recycle bin, Windows Temp folder, or browser temporary folder

Setting Notifications to Send upon Detection of a Virus

In the Notification tab of the HTTP Scanning screen you can select two kinds of notifications:

- The message to display in a user's browser when HTTP VirusWall has detected a virus/malware in a file that the user is attempting to transfer.
- The message to send to the administrator when such an incident has occurred.

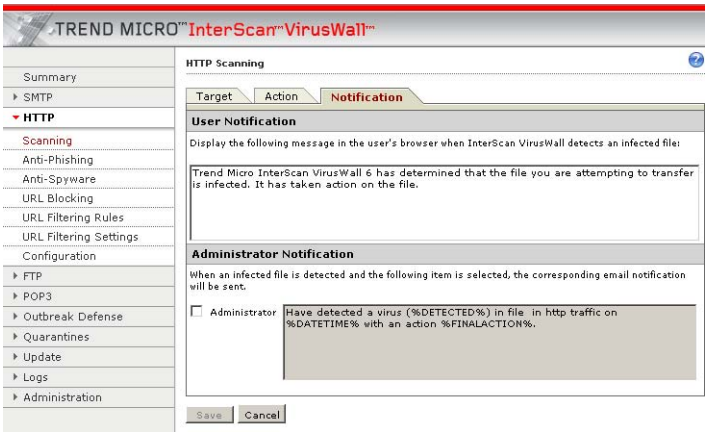


FIGURE 2-5. HTTP Scanning screen, Notification tab

Set the first kind of notification in the User Notification section. You can either accept the default message or customize it.

For the administrator notification, select the Administrator check box to activate the text field. The default message comes with three variables:

```
Have detected a virus (%DETECTED%) in file in http traffic on %DATETIME%
with an action %FINALACTION%.
```

FIGURE 2-6. HTTP Scanning screen, Notification tab, default Administrator notification message, showing the three variables/tokens used

However, several other tokens are available to choose from in customizing your message. Table 2-3 on page 2-17 lists all of the available tokens.

TABLE 2-3. HTTP scanning, administrator notification tokens and descriptions

Token	Description
%DETECTED%	The name of the detected virus or malware
%DATETIME%	The date and time of the detection
%FINALACTION%	Pass, Remove, Quarantine, or Clean
%CLIENT%	The client IP address
%URL%	The target URL
%PROTOCOL%	Always HTTP
%QUARANTINE_AREA%	The quarantine path for HTTP quarantined items
%MACHINE_NAME%	The host name of the InterScan VirusWall server
%FILTER_NAME%	Always FileVirusScan

Tip: Remember to click **Save** at the bottom of the screen to save your choices.

Chapter 3

Configuring HTTP Anti-Phishing Settings

This chapter includes the following topics:

Overview

Phishing is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site. In a typical scenario, an unsuspecting user gets an urgent (and authentic-looking) email message, telling him or her that there is a problem with their account that they must fix immediately or the company will close the account. The message typically includes the URL of a Web site that looks exactly like the Web site of the user's bank or credit card company.

The phishing message urges the user to log on to the bogus site and confirm his or her account information. The code behind the Web site, however, redirects any data entered at the site to a malicious hacker who steals the user name, password, credit card number, Social Security number, or whatever data that the victim entered.

Phish fraud is easy to perpetuate, hard for even computer-savvy users to detect, hard for law enforcement to track down, harder still to prosecute, and potentially quite lucrative for those criminals who practice it.

Setting HTTP Anti-Phishing Targets

Just as with every protocol, there are three tabs in the HTTP Anti-Phishing screen: Target, Action, and Notification.

Enabling HTTP Anti-Phishing

When you enable HTTP scanning either during installation or on the Summary screen, HTTP Anti-Phishing scanning is enabled by default.

Follow the procedure below to enable or disable HTTP Anti-Phishing independent of any other scan type.

To enable or disable HTTP Anti-phishing services:

1. Click **HTTP > Anti-Phishing.** The HTTP Anti-Phishing screen appears, displaying the Target tab.
2. Near the top of the Target tab, select (or deselect) the **Enable HTTP anti-phishing** check box.
3. Click **Save.**

Choosing Phish Categories to Block

After you have enabled HTTP Anti-Phishing services, the next step is to select what kinds of phish sites to block. You can choose from four categories, as shown in figure 3-1, “HTTP Anti-Phishing screen, Target tab, showing the default selections for phish categories to block,” on page 3-3:

FIGURE 3-1. HTTP Anti-Phishing screen, Target tab, showing the default selections for phish categories to block

All four phish categories are selected by default. To allow traffic of any category to flow through unblocked, deselect the check box next to it.

Specifying Action to Take upon Detection of a Phishing Site

There are only two options for action to take upon detection of phishing sites: block or allow, as shown in figure 3-2, “HTTP Anti-Phishing screen, Action tab,” on page 3-4.

FIGURE 3-2. HTTP Anti-Phishing screen, Action tab

The default setting is Block.

Setting Notifications to Send upon Detection of a Phishing Site

In the Notification tab of the HTTP Anti-Phishing screen, you can select two kinds of notifications:

- The message to display in a user's browser when HTTP VirusWall has detected a phish site that the user is attempting to access.
- The message to send to the administrator when such an incident has occurred.

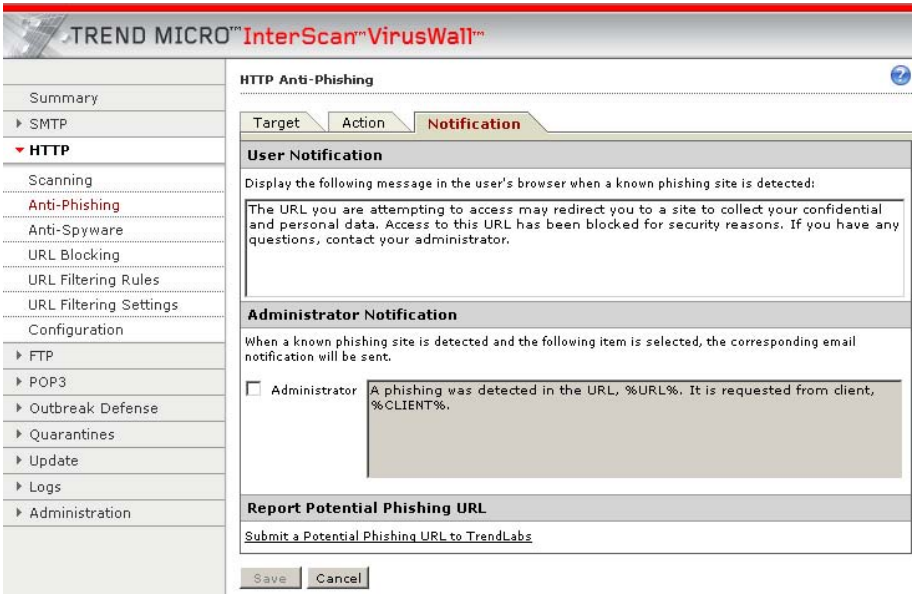


FIGURE 3-3. HTTP Anti-Phishing screen, Notification tab

User Notification

Set the first kind of notification in the User Notification section. You can either accept the default message or customize it.

Administrator Notification

For the administrator notification, select the Administrator check box to activate the text field. The default message comes with two variables:

> A phishing was detected in the URL, %URL%. It is requested from client, %CLIENT%.

FIGURE 3-4. HTTP Anti-Phishing screen, Notification tab, default Administrator notification message, showing the two tokens used

However, several other tokens are available to choose from in customizing your message. Table 3-1 on page 3-6 lists the additional tokens.

TABLE 3-1. HTTP anti-phishing, administrator notification tokens and descriptions

Token	Description
%FINALACTION%	The action taken when HTTP VirusWall detects a phishing site
%DATETIME%	The time that this URL access occurs
%CLIENT%	The client IP address
%URL%	The target URL
%PROTOCOL%	Always HTTP
%MACHINE_NAME%	The host name of the InterScan VirusWall server
%FILTER_NAME%	Always PhishTrap
%PHISHING_CATEGORY%	“Phishing”, “Spyware”, “Virus accomplice”, “Forged signature”, “Disease vector”, “Malicious applet”

Tip: Remember to click **Save** at the bottom of the screen to save your choices.

Report a Potential Phishing URL

The final section on the HTTP Anti-Phishing Notification tab consists of a hyperlink that you can click to send Trend Micro the URL of a Web site that you suspect is a phish site. The hyperlink is an email link that opens your email client to an email addressed to the anti-fraud section of Trend Micro 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 threats. The daily culmination of these efforts is 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 Irvine, CA, to mitigate virus outbreaks and provide urgent support.

TrendLabs' modern headquarters, in a major Metro Manila IT park, earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

To send TrendLabs the suspect URL, click the Submit a Potential Phishing URL to TrendLabs hyperlink and complete and send the email message, being sure to include the URL itself in the body of the message.

Chapter 4

Configuring HTTP Anti-Spyware/Grayware Settings

This chapter includes the following topics:

Spyware/Grayware Overview

Spyware/grayware comes in many forms and often appears to be a legitimate software program. Trend Micro tracks spyware/grayware and provides regular updates in a pattern file.

Some common types of grayware include:

Type of grayware	Typical Function
Spyware	gathers data, such as account user names and passwords, and transmits them to third parties
Adware	displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser
Dialers	changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Program	causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	helps hackers enter computers
Remote Access Tools	help hackers remotely access and control computers
Password Cracking Applications	helps hackers decipher account user names and passwords
Others	other types not covered above

Setting HTTP Anti-Spyware Targets

Just as with every protocol, there are three tabs in the HTTP Anti-Spyware screen: Target, Action, and Notification.

Enabling HTTP Spyware/Grayware Scanning

When you enable HTTP scanning services either during installation or on the Summary screen, HTTP anti-spyware/grayware scanning is enabled by default.

Follow the procedure below to enable or disable HTTP anti-spyware/grayware independent of any other scan type.

To enable or disable HTTP Anti-Spyware services:

1. Click **HTTP > Anti-Spyware.** The HTTP Anti-Spyware screen appears, displaying the Target tab.
2. Near the top of the Target tab, select (or deselect) the **Enable HTTP anti-spyware** check box.
3. Click **Save.**

Setting the Spyware/Grayware Scanning Exclusion List

Not all spyware or grayware is undesirable. For this reason InterScan VirusWall provides a feature by which you can create a list of spyware/grayware that you would like to exclude from scanning, as shown in figure 4-1, “HTTP Anti-Spyware screen, Target tab,” on page 4-4. You can target spyware/grayware for exclusion from scanning and cleaning in three different ways:

- By spyware/grayware program file name
- By spyware/grayware file extension
- By spyware grayware category

Use the Target tab of the HTTP Anti-Spyware screen to identify spyware/grayware for exclusion, by whichever of the above methods you use.

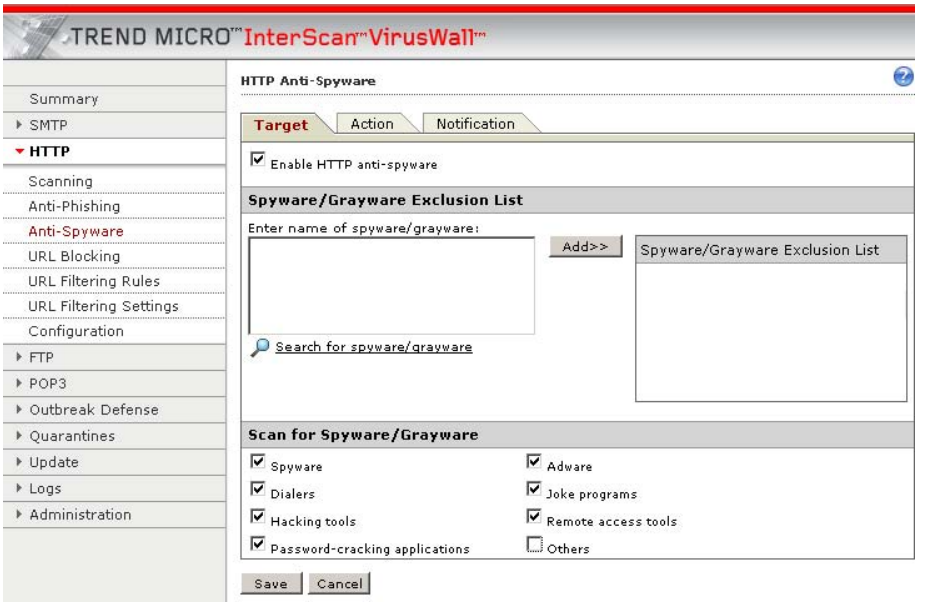


FIGURE 4-1. HTTP Anti-Spyware screen, Target tab

Excluding Spyware/Grayware by Program File Name

InterScan VirusWall can recognize only the program file of the spyware/grayware item listed in the spyware/grayware exclusion list.

If you know the name of the program file of the spyware/grayware that you wish to exclude from scanning, follow the procedures below to add items to or remove them from the HTTP spyware/grayware exclusion list.

To add a spyware/grayware item to the HTTP spyware/grayware exclusion list:

1. On the left-side menu, click **HTTP** > **Anti-Spyware.** The HTTP Anti-Spyware screen appears, displaying the Target tab.
2. In the Spyware/Grayware Exclusion List section, in the **Enter name of spyware/grayware** text box, type the name of the spyware or grayware program to exclude from scanning and click **Add**>> (Add>>). The spyware item that you typed moves over to the Spyware/Grayware Exclusion List box on the right.

Note: You can add more than one spyware/grayware item at a time by typing one item per line and then clicking **Add>>** (Add>>).

3. Click **Save.**

The procedure for removing an item from the spyware/grayware exclusion list is quite simple.

To remove a spyware/grayware item from the exclusion list:

1. On the left-side menu, click **HTTP > Anti-Spyware.** The HTTP Anti-Spyware screen appears, displaying the Target tab.
2. In the Spyware/Grayware Exclusion List section, click the trash can icon () next to the item in the Spyware/Grayware Exclusion List box on the right side of the screen. The item disappears.

Note: Although the item had disappeared from view, HTTP VirusWall will not remove it from the exclusion list until you click **Save** at the bottom of the screen.

3. Click **Save** at the bottom of the screen.

Excluding Spyware/Grayware by File Name Extension

You can target spyware/grayware for exclusion by entering extension names in the left-side text box in the Spyware/Grayware Exclusion List section. To enter extensions for exclusion, follow the same basic steps as for entering spyware/grayware program file names, except use the format `*.ext`, as shown in *To add a spyware/grayware item to the HTTP spyware/grayware exclusion list:* on page 4-4.

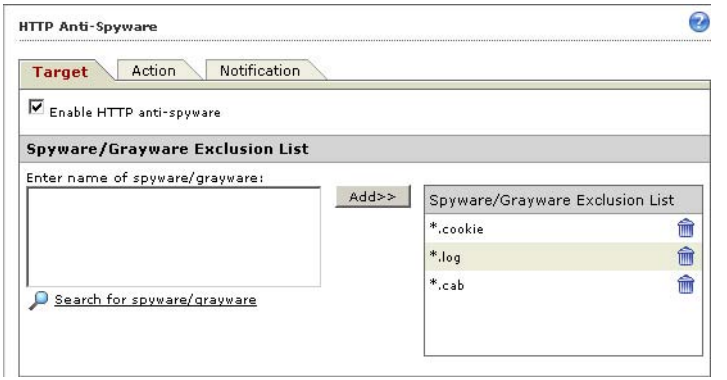


FIGURE 4-2. HTTP Anti-Spyware screen, Target tab, detail showing spyware/grayware entered by file extension

Excluding Spyware/Grayware by Category

In addition to excluding specific spyware/grayware from scanning, you can also configure HTTP VirusWall to scan only for specific categories of spyware/grayware.

To select specific categories of spyware/grayware to scan for:

1. On the left-side menu, click **HTTP > Anti-Spyware.** The HTTP Anti-Spyware screen appears, displaying the Target tab.
2. In the **Scan for Spyware/Grayware** section (lower half of the screen), select the check mark next to each category of spyware/grayware that you want to scan for, as shown in figure 4-3, “The HTTP Anti-Spyware screen, Target tab Scan for Spyware/Grayware section,” on page 4-7:

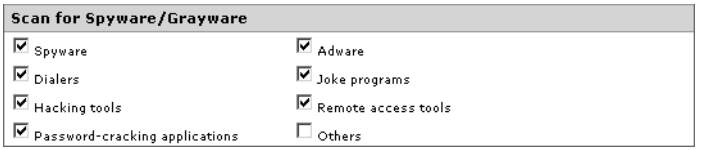


FIGURE 4-3. The HTTP Anti-Spyware screen, Target tab Scan for Spyware/Grayware section

3. Click **Save.**

Specifying Action to Take upon Detection of Spyware/Grayware

The Action tab of the HTTP Anti-Spyware screen contains only one section: Action on Spyware/Grayware. There are only three options to choose from:

- Quarantine
- Block
- Allow download (not recommended)

Note: Remember to click **Save** after selecting your action option.

Setting Notifications to Send upon Detection of Spyware/Grayware

In the Notification tab of the HTTP Anti-Spyware screen, you can select two kinds of notifications:

- The message to display in a user's browser when HTTP VirusWall has detected spyware or grayware in a file that the user is attempting to transfer.
- The message to send to the administrator when such an incident has occurred.

See figure 4-4, “HTTP Anti-Spyware screen, Notification tab with default message text and with Administrator check box selected,” on page 4-8 for an illustration of these two fields.

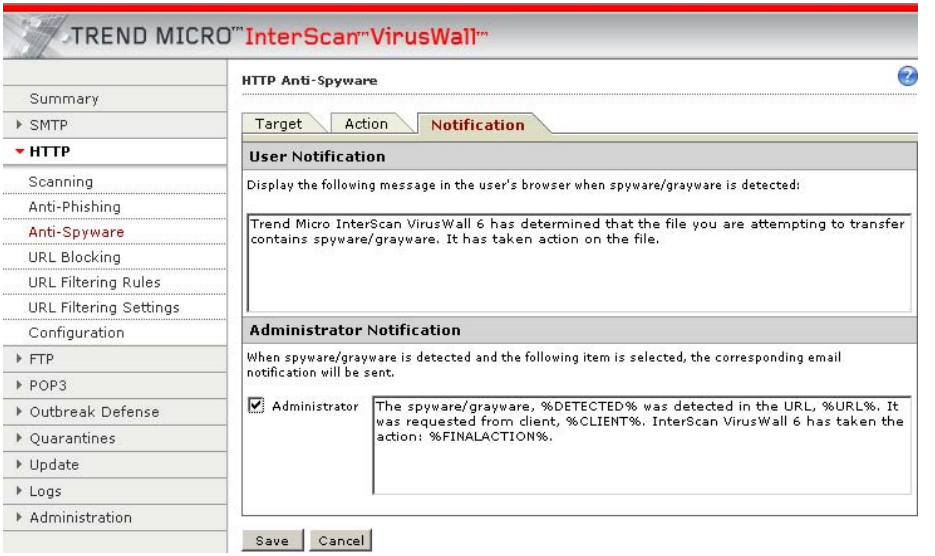


FIGURE 4-4. HTTP Anti-Spyware screen, Notification tab with default message text and with Administrator check box selected

User Notification

Set the first kind of notification in the User Notification section. You can either accept the default message or customize it. The notification will go out when HTTP VirusWall detects spyware or grayware in HTTP traffic, as targeted in your HTTP Anti-Spyware / Target tab.

Administrator Notification

For the administrator notification, select the Administrator check box to activate the text field. The default message comes with four variables (tokens):

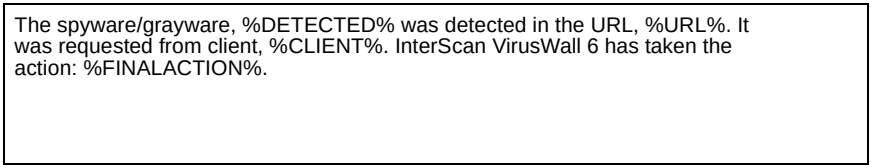


FIGURE 4-5. HTTP Anti-Spyware screen, Notification tab, default Administrator notification message, showing the four default tokens used

However, several other tokens are available to choose from in customizing your message. Table 4-1 on page 4-9 lists all available tokens for this notification.

TABLE 4-1. HTTP anti-spyware, administrator notification tokens and descriptions

Token	Description
%DATETIME%	The time that this URL access occurs
%CLIENT%	Client IP address
%DETECTED%	The name of the detected spyware/grayware program
%URL%	The URL at which the spyware/grayware was found
%FINALACTION%	Pass, Remove, Quarantine, or Clean
%PROTOCOL%	Always HTTP
%MACHINE_NAME%	The host name of the InterScan VirusWall server
%QUARANTINE_AREA%	The quarantine path for HTTP quarantined items
%FILTER_NAME%	Always FileVirusScan

Note: Remember to click **Save** at the bottom of the screen to save your choices.

Chapter 5

HTTP URL Blocking and Filtering

This chapter includes the following topics:

URL Blocking versus URL Filtering

HTTP VirusWall offers two features relating to the scanning of URLs:

- URL blocking
- URL filtering

These features are similar, but quite different in complexity.

URL Blocking Overview

URL blocking simply takes a list of URLs that you wish to block and prevents your clients from accessing them. URL blocking can also block sites that match certain text strings, IP addresses, or a combination of both. HTTP VirusWall also provides a URL blocking exception list. URL blocking applies at all times and does not attempt to separate URLs into categories. You can also import a list of URLs to block and URLs to exclude from blocking. For a complete discussion of URL blocking options and configuration, see *Configuring URL Blocking* on page 5-3.

URL Filtering Overview

The URL filtering feature provides more granularity in terms of which URLs it blocks and when. By using the URL filtering feature, you can select categories and subcategories of URLs to filter and can configure at which times of the day (workday hours versus leisure hours). Like URL blocking, URL filtering also contains a configurable exception list. Because of the complexity of the URL filtering feature, its settings are broken up into two left-side menu headings, URL Filtering Rules and URL Filtering Settings. Use the screens under both menu headings to fully calibrate your URL filtering strategy.

Configuring URL Blocking

You can set all configurations of the URL blocking feature by adjusting the settings on the screens under the URL Blocking menu heading on the left-side menu.

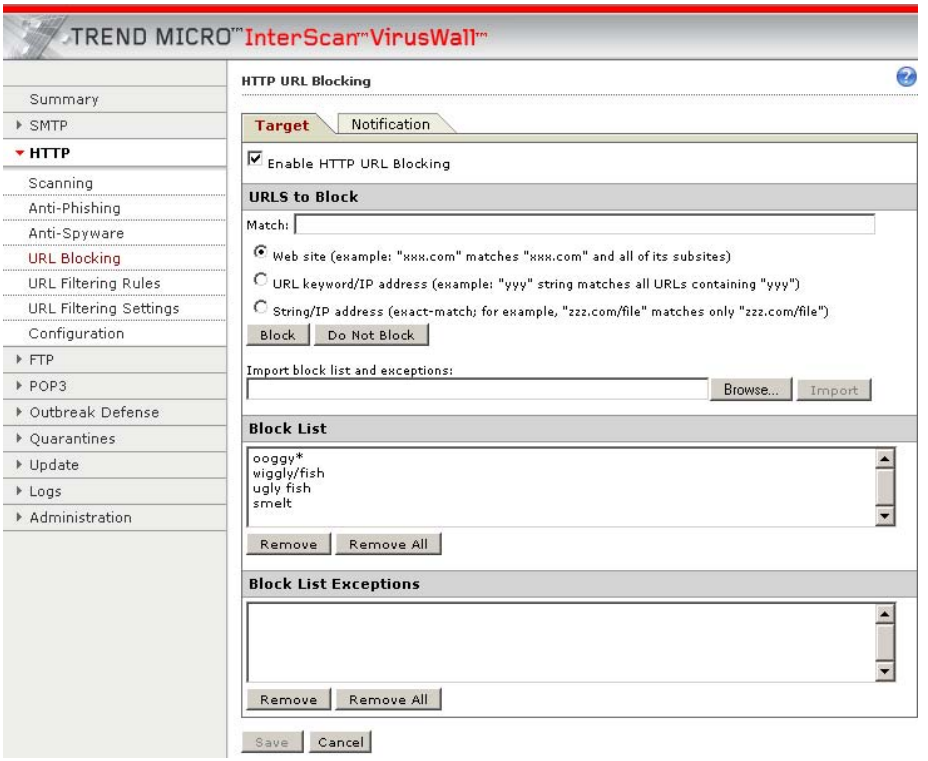


FIGURE 5-1. HTTP URL Blocking screen, Target tab

Enabling URL Blocking

When you enable HTTP scanning either during installation or on the Summary screen, URL blocking is enabled by default.

Follow the procedure below to enable or disable URL blocking independent of any other scan type.

To enable or disable URL blocking services:

1. Click **HTTP > URL Blocking.** The HTTP URL Blocking screen appears, displaying the Target tab.
2. Near the top of the Target tab, select (or deselect) the **Enable HTTP URL Blocking** check box.
3. Click **Save** at the bottom of the screen.

Configuring Blocked URLs and Exceptions

On the HTTP URL Blocking screen you can use patterns to identify URLs to either allow access to or to block, as shown in figure 5-2, “HTTP URL Blocking screen, Target tab, URLs to Block section showing the three pattern-matching options,” on page 5-4.

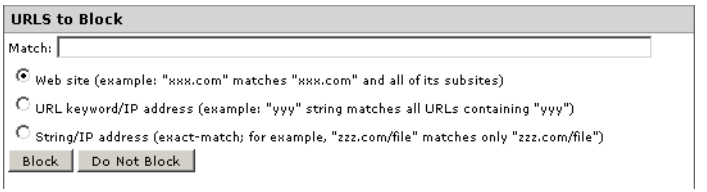


FIGURE 5-2. HTTP URL Blocking screen, Target tab, URLs to Block section showing the three pattern-matching options

For each matching pattern that you type in the Match field, HTTP VirusWall can block one of the following:

- An entire Web site and all of its subsites
- Certain pages or sections of a site, but not others
- Any URL that matches a string that you enter

Blocking by Web Site

Choose the **Web site (example: "xxx.com" matches "xxx.com" and all of its sub-sites)** option to block an entire Web site.

Blocking Portions of a Web Site

Choose the **String/IP address (exact-match; for example, "zzz.com/file" matches only "zzz.com/file")** option.

To identify a folder or directory in a given Web site, use a forward slash (/) after the last character. For example, if you want to block `www.blockedsite.com/porn/` but allow access to any other directories on the site, including the root directory, follow the procedure below.

To block a portion of a Web site but leave the rest unblocked:

1. Type, for example, *`www.blockedsite.com/porn/`* in the Match field, and then click **Block.**

   Note: Remember to type the trailing forward slash. (If you write *`porn`* without the forward slash, HTTP VirusWall will consider *`www.blockedsite.com/porn`* as a file.)

2. Click **Save.**

Blocking Any URL That Matches a String

Choose the **URL keyword/IP address (example: "yyy" string matches all URLs containing "yyy")** option.

To set up pattern matching to block URLs:

1. On the left-side menu, click **HTTP** > **URL Blocking.** The HTTP URL Blocking screen appears, displaying the Target tab.
2. Under the URLs to Block section, in the **Match** field, type the string for HTTP VirusWall to match in URLs. The format of the string that you type depends on which of the three matching options you choose.
3. Click **Block.** The pattern moves from the Match field to the text field in the Block List section.
4. Click **Save** at the bottom of the screen.
5. Optionally, repeat above steps to input as many patterns as you like.

You can use the pattern-matching feature either to block URLs that match the pattern or to allow them. Follow the procedure below to set up pattern matching for URLs that you wish to always allow access to.

To set up pattern matching to allow URLs:

1. On the left-side menu, click **HTTP > URL Blocking.** The HTTP URL Blocking screen appears, displaying the Target tab.
2. Under the URLs to Block section, in the **Match** field, type the string for HTTP VirusWall to match in URLs. The format of the string that you type depends on which of the three matching options you choose.
3. Click **Do Not Block.** The pattern moves from the Match field to the text field in the Block List Exceptions section.
4. Click **Save** at the bottom of the screen.
5. Optionally, repeat above steps to input as many patterns as you like.

Managing Lists of Blocked and Allowed URLs

By following the procedures in *Configuring Blocked URLs and Exceptions* on page 5-4, you are essentially creating a list of approved URLs, a list of URLs to block, or both (see figure 5-3, “HTTP URL Blocking screen, Target tab, Block List and Block List Exceptions sections showing Remove, Remove All, and Save buttons,” on page 5-6).

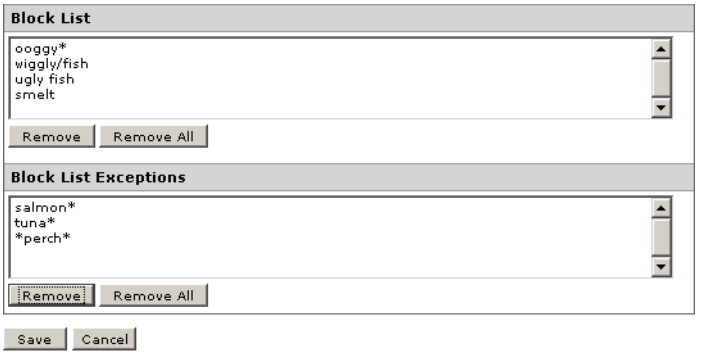


FIGURE 5-3. HTTP URL Blocking screen, Target tab, Block List and Block List Exceptions sections showing Remove, Remove All, and Save buttons

Once you have created these lists, you can manage them. Through the HTTP URL Blocking screen, Target tab, you can do any of the following:

- Remove selected patterns from either list
- Clear the entire list
- Import lists of URLs to block or allow

Removing Patterns from Existing Lists

To remove selected patterns from the Block List:

1. On the left-side menu, click **HTTP > URL Blocking.** The HTTP URL Blocking screen appears, displaying the Target tab.
2. In the Block List section, select each pattern that you wish to remove. (Multiple-select with **Ctrl** + left mouse button.)
3. Click **Remove.**
4. Click **Save** at the bottom of the screen.

Note: Just clicking **Remove** does not complete the process of removing the patterns from HTTP VirusWall. Always remember to click **Save** at the bottom of the screen to save your changes.

To remove all of the patterns in the Block List:

1. Follow steps 1 and 2 in *To remove selected patterns from the Block List:* on page 5-7 but then click **Remove All.**
2. Click **Save.**

To remove one or more patterns from the Block List Exceptions list:

1. Follow the steps 1 and 2 in *To remove selected patterns from the Block List:* on page 5-7, except apply them to the Block List Exceptions list.
2. Click **Save** at the bottom of the screen.

Importing a List of Patterns to Block and Allow

InterScan VirusWall can import a file containing lists of patterns to block and allow. This file must be in a specified format.

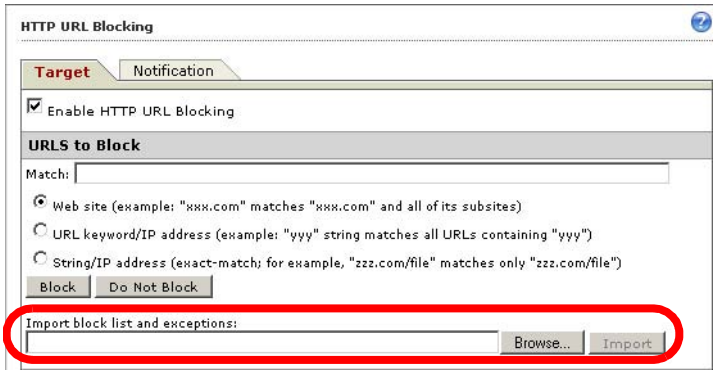


FIGURE 5-4. Detail from HTTP URL Blocking screen, Target tab showing Import block list and exceptions field

To import a list of Web sites and URL strings from a given file to Block List and Block List Exceptions:

1. On the left-side menu, click **HTTP > URL Blocking.** The HTTP URL Blocking screen appears, displaying the Target tab.
2. In the URLs to Block section, specify the location of the file in the **Import block list and exceptions** field by clicking **Browse**, and then click **Import**. HTTP VirusWall gets the list of URL blocking patterns and populates the Block List and Block List Exceptions fields with these patterns.

   Note: This HTTP VirusWall import feature supports only files formatted in UTF8 format.

3. Click **Save.**

   Note: The main purpose of importing these settings from a file is to make it easier to import these settings from a previous installation of InterScan VirusWall.

Format for Import File

#URL Blocking Import File is on the first line of a plain-text file that contains a list of Web sites, URL keywords, or strings, with one rule per line. Entries are grouped under the [block] or [allow] section. For example:

```
#URL Blocking Import File
[block]
*virus*
virus
*sasser*
[allow]
www.trendmicro.com*
www.antivirus.com*
```

After you have imported the file, the results will be added to a file called ***URLB.ini***, which resides in <isvw_installed_directory>/http/conf/.

The format for the import file to import a list of URL filtering exceptions (see *URL Filtering Exceptions Tab* on page 5-19) is exactly the same as the format shown above, except that it does not include a ***[block]*** section.

Tip: Trend Micro strongly recommends that you do not manually edit the URLB.ini file. InterScan VirusWall writes to this file when you use the Web console to add patterns for blocking and allowing URLs.

Setting Notifications upon Detection of an Attempted Access of a Blocked URL

In the Notification tab of the HTTP URL Blocking screen, you can select two kinds of notifications:

- The message to display in a user's browser when HTTP VirusWall has detected an attempted access of a URL that matches a blocking pattern.
- The message to send to the administrator when such an incident has occurred.

See figure 5-5, “HTTP URL Blocking screen, Notification tab,” on page 5-10 for an illustration of these two fields.

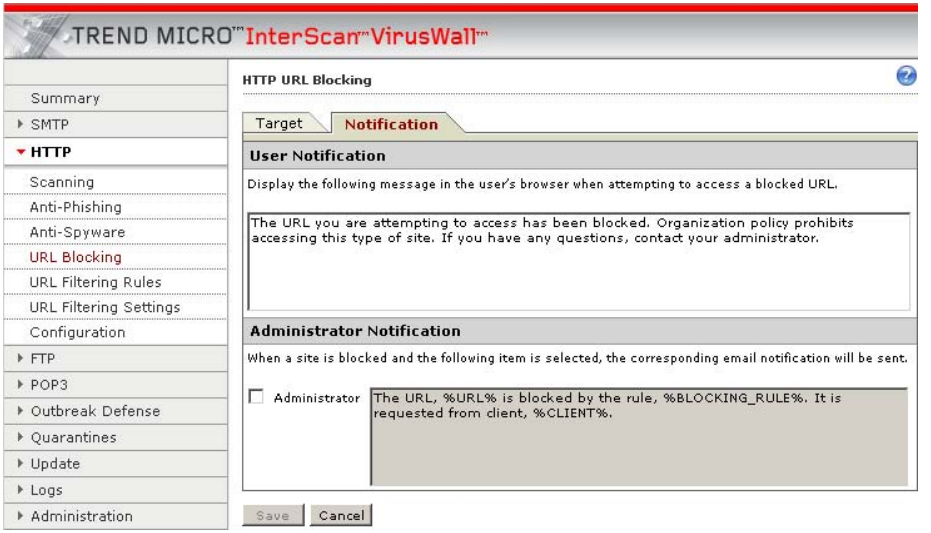


FIGURE 5-5. HTTP URL Blocking screen, Notification tab

User Notification

Set the first kind of notification in the User Notification section. You can either accept the default message or customize it. The notification will go out when a user attempts to access a blocked, as targeted in your HTTP URL Blocking / Target tab.

Administrator Notification

For the administrator notification, select the Administrator check box to activate the text field. The default message comes with three variables (tokens):

> The URL, %URL% is blocked by the rule, %BLOCKING_RULE%. It is requested from client, %CLIENT%.

FIGURE 5-6. HTTP URL Blocking screen, Notification tab, default Administrator notification message, showing the three default tokens used

However, several other tokens are available to choose from in customizing your message. Table 5-1 on page 5-11 lists all of the available tokens.

TABLE 5-1. HTTP URL blocking, administrator notification tokens and descriptions

Token	Description
%URL%	The URL that the rule blocks
%BLOCKING_RULE%	OPP, URL blocking rule set in Web console, URL port restriction, HTTPS CONNECT port restriction, or infected
%CLIENT%	The client IP address
%PROTOCOL%	Always HTTP
%MACHINE_NAME%	The host name of the InterScan VirusWall server
%DATETIME%	The Time that this URL access occurs
%FILTER_NAME%	Always URLBlocking

Note: Remember to click **Save** at the bottom of the screen to save your choices.

URL Filtering Overview

The default settings for the URL filtering module assume that your primary interest is to avoid legal liabilities associated with the viewing of offensive material.

URL filtering can enhance productivity as it combines dynamic filtering with advanced databases. Unrestricted access to the Internet can result in reduced worker productivity and can decrease bandwidth available for legitimate business purposes. Some examples of Internet use that may reduce employee productivity are online trading, shopping, auction bidding, selling, job-hunting, dating, gambling, and other non-work-related activities.

Two Customization Methods

The URL filtering policy of HTTP VirusWall is very flexible. There are two basic mechanisms for customizing:

1. The assignment of a subcategory to a category group is completely configurable. The subcategories are organized into six category groups:
   - Company Prohibited Sites
   - Not Work Related
   - Possible Research Topics
   - Business Function Related
   - Customer Defined
   - Others
2. Each category group may be blocked or unblocked.

You can manage access to all identified URLs within a targeted category according to policy. The database associates each URL with a set of categories. It is possible that a URL may be wrongly categorized; in which case, you can either submit the URL to Trend Micro TrendLabs for reclassification or use the URL Filtering Exceptions List to override the classification of the URL. The patterns specified in the URL Filtering Exceptions List are matched against the URL, not to the contents of the document that the URL refers to. You can use the URL Filtering Exceptions List to bypass internal Web sites and other sites for which the attempt to classify them introduces unnecessary overhead.

Remote Web-Based Classification Service

The URL filtering module works with the local classification database and policies and either allows access to or blocks the URL that it is filtering. However, when a URL is unclassified by the local classification database, HTTP VirusWall contacts a remote, Web-based classification service to do the classification, as shown in figure 5-7 below.

- A local classification database contains the URL classification information; thus, HTTP VirusWall retrieves most URL classifications with a minimum of overhead.
- If the classification information is not available locally, a remote Web-based classification service is contacted.

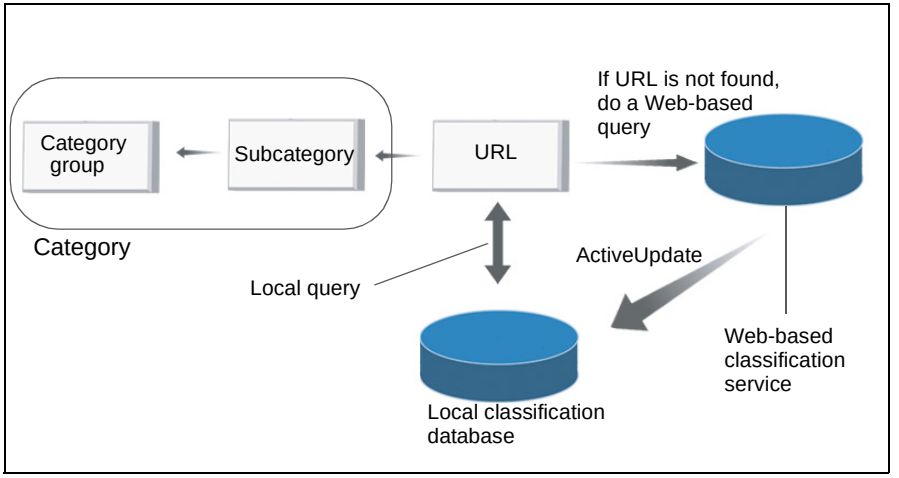


FIGURE 5-7. How URL classification works with the local and remote classification databases

The classification service may have more up-to-date information than the local database or may be able to classify the URL dynamically. The classification service compiles a list of previously unclassified URLs. Once classified, these URLs are added to a master database, which is distributed as an update to the local classification database. Such updates are periodically retrieved by InterScan VirusWall through ActiveUpdate.

Note: Manual updates to the URL filtering database can be invoked from the Summary screen.

The classification service classifies a queried URL into one of over 50 subcategories and then maps it into one of six category groups. HTTP VirusWall then checks the categories with the policies that user set in the Web console and either allows or blocks access to the requested URL.

Access to the remote Web-based classification service is enabled by default. Although the classification service is designed to provide quick responses to requests from all over the world, accessing it can impart a significant performance degradation in certain circumstances (particularly if your environment has large throughput requirements and frequently needs to query the classification service).

To disable access to the remote classification service, edit the ***urlfcIfx.ini*** configuration file under `{installation_folder}/HTTP/conf/` as follows:

```
[network]
no_web_access=yes
```

Configuring URL Filtering

In the Web console, the URL filtering feature of HTTP VirusWall comprises two main left-side menus: URL Filtering Rules and URL Filtering Settings. The URL Filtering Rules screen has no tabs and is relatively simple in appearance. On this screen you can enable URL HTTP filtering and select whether to block or allow Web sites of preset categories during work hours, leisure hours, or both.

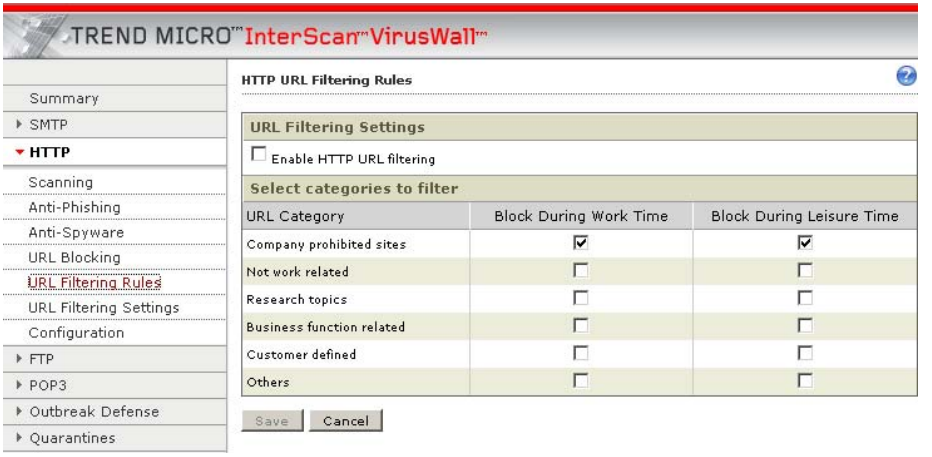


FIGURE 5-8. HTTP URL Filtering Rules screen

Enabling URL Filtering

Make sure that the URL filtering function is enabled before you start. You can enable URL filtering by selecting the **Enable HTTP URL filtering** check box on the URL Filtering Rules screen.

To enable URL filtering:

1. On the left-side menu, click **HTTP > URL Filtering.** The HTTP URL Filtering screen appears, displaying the Target tab.
2. Select the **Enable HTTP URL filtering** check box. A warning message appears advising you that this service forwards URLs and related data to Trend Micro for filtering purposes, as shown in the warning message below:

WARNING! *The URL Filtering Service blocks web sites that may include offensive or other unwanted content. The Service forwards the address of each web site that you attempt to access to our online secure servers, where it is compared against a dynamically updated database of rated web sites. Based on the ratings and your preference settings, your web browser will automatically permit or deny access. By activating this Service below, you authorize the transfer of URL and related data to Trend Micro servers for filtering purposes.*

3. Click **OK** to close the message and then click **Save** to finish enabling the URL filtering feature.

Note: When you enable HTTP scanning either during installation or on the Summary page, all HTTP scanning functions are enabled except URL filtering. To use URL filtering, you must manually enable it by following the procedure above.

URL Filtering Rules

Apart from enabling URL filtering, the second function of the URL Filtering Rules screen is to select whether to block or allow Web sites of preset categories during work hours, leisure hours, or both.

To select categories for blocking during work and leisure times:

1. Next to each category, on the URL Filtering Rules screen (**Select categories to filter** section), select the check box in the Block During Work Time column for each category that you wish to block during work time.
2. Next to each category, select the check box in the Block During Leisure Time column for each category that you wish to block during leisure time.
3. Click **Save.**

URL Filtering Settings

The URL Filtering Settings screen has four tabs:

- URL Categories
- URL Filtering Exceptions
- Schedule
- Notification

URL Categories Tab

Use this tab to select the URL categories to block. Simply select the check box in the Subcategory column (leftmost) next to each subcategory that you would like to block.

Because you can block individual subcategories or entire groups, HTTP VirusWall gives you the flexibility to rearrange the composition of the larger groups. You can move subcategories from one major group to another.

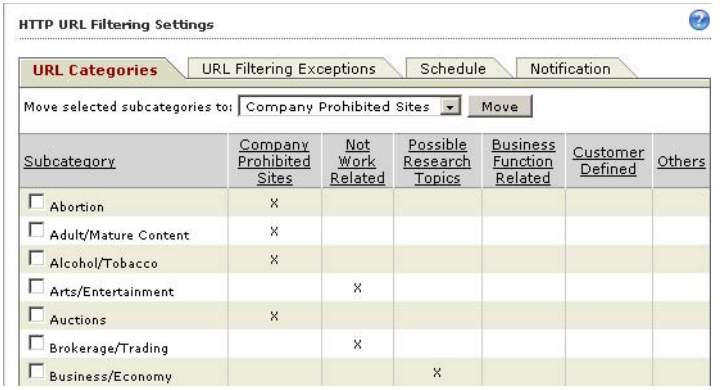


FIGURE 5-9. HTTP URL Filtering Settings screen, URL Categories tab, showing the first few subcategories belonging to the Company Prohibited Sites blocking group

To move one or more subcategories from one URL blocking group to another:

1. On the left-side menu, click **HTTP > URL Filtering Settings**. The HTTP URL Filtering Settings screen appears, displaying the URL Categories tab.
2. Select each subcategory that you would like to move.
3. In the **Move selected subcategories to** drop-down menu at the top of the table, select the category that you want to move the selected subcategories to. (Figure 5-10.)
4. Click **Move.** The table display changes, showing for each moved subcategory an **X** under the category to which you have moved the subcategories. (See Figure 5-10.)
5. Scroll down and click **Save** at the bottom of this long screen in order to save your changes.

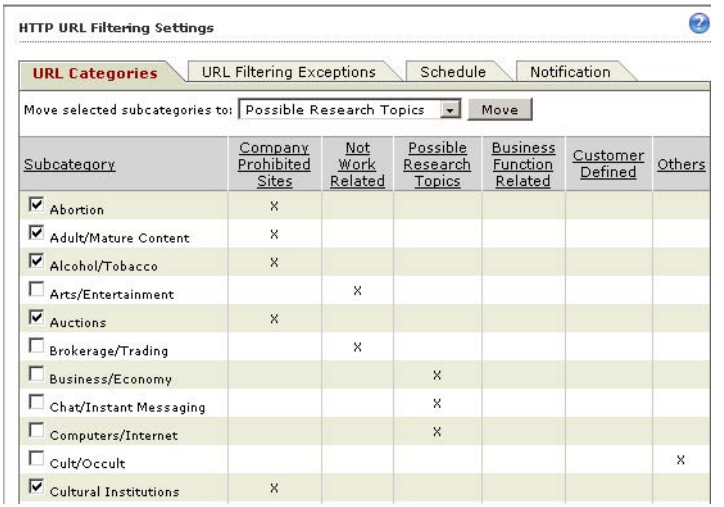
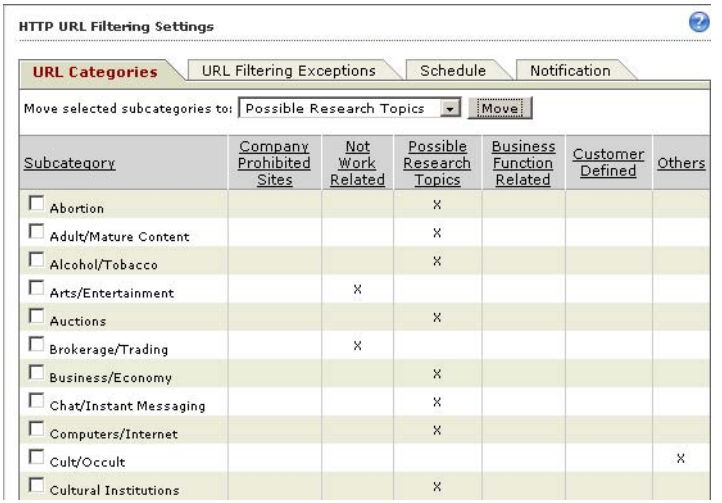


FIGURE 5-10. HTTP URL Filtering Settings screen, URL Categories tab showing several categories in the Company Prohibited Sites blocking group selected and ready for moving to the Possible Research Topics group (shown in the drop-down menu above the table)

Tip: You can sort subcategories by clicking any column heading. Doing so sorts subcategories by blocking group. Clicking the Subcategory column head sorts the subcategories alphabetically.



Subcategory	Company Prohibited Sites	Not Work Related	Possible Research Topics	Business Function Related	Customer Defined	Others
Abortion			X			
Adult/Mature Content			X			
Alcohol/Tobacco			X			
Arts/Entertainment		X				
Auctions			X			
Brokerage/Trading		X				
Business/Economy			X			
Chat/Instant Messaging			X			
Computers/Internet			X			
Cult/Occult						X
Cultural Institutions			X			

FIGURE 5-11. HTTP URL Filtering Settings screen, URL Categories tab, showing the new blocking group locations for the subcategories selected in the previous procedure

URL Filtering Exceptions Tab

On this tab you can import a list of URLs for your exceptions list and you can set three kinds of URL pattern matching to create a list of sites that HTTP VirusWall will not filter (see figure 5-13, “HTTP URL Filtering Settings screen, Schedule tab,” on page 5-21).

The format for the plain-text file of URLs to exclude from filtering is exactly the same as that shown in *Format for Import File* on page 5-9, except that there only one section: ***[allow]***.

FIGURE 5-12. HTTP URL Filtering Settings screen, URL Filtering Exceptions tab

To add an exception to URL filtering by importing a list:

1. Click **Browse** and navigate to the import file.
2. Click **Import.** HTTP VirusWall imports the URL filtering exceptions from the imported list and displays them in the Do Not Filter the Following Sites field.

   Note: This import feature supports only files formatted in UTF8 format.

3. Click **Save.**

To add matching criteria to your list of URL filtering exceptions:

1. Type the pattern to match in the **Match** field.
2. Select the kind of match from the adjacent drop-down menu. The options are:
   - Web site
   - URL keyword
   - String

   These options correspond to the matching rules explained in detail in *Configuring Blocked URLs and Exceptions* on page 5-4.

3. Click **Add.** The pattern and matching style appear in the list of filtering criteria in the field named Do Not Filter the Following Sites.
4. Click **Save.** (Your changes will be lost unless you click both **Add** and **Save.**)

Schedule Tab

On this tab you can select the days and hours to identify as leisure time and work time. HTTP VirusWall uses these settings in conjunction with other settings, such as those on the URL Filtering Rules screen.

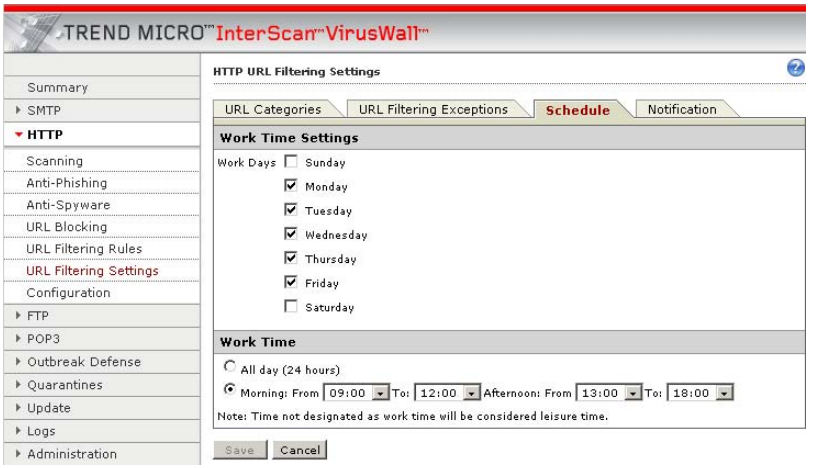


FIGURE 5-13. HTTP URL Filtering Settings screen, Schedule tab

Select the days and times for HTTP VirusWall to consider as "work time" for purposes of URL filtering. Remember to click **Save** to save your settings.

Notification Tab

On this tab you can customize the user notification and the administrator notification and you can submit URLs to TrendLabs for reclassification.

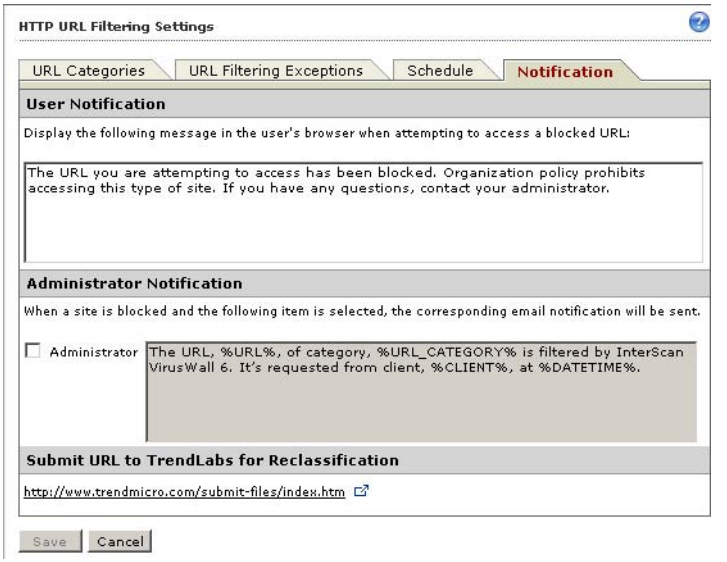


FIGURE 5-14. HTTP URL Filtering Settings screen, Notification tab

User Notification

In the Notification tab of the HTTP URL Filtering Settings screen, you can select two kinds of notifications:

- The message to display in a user's browser when HTTP VirusWall has that a user has attempted to access a blocked URL.
- The message to send to the administrator when such an incident has occurred.

Set the first kind of notification in the User Notification section. You can either accept the default message or customize it. The notification will go out when HTTP VirusWall detects that a user has attempted to access a site matching any of the URL filtering criteria that you have set up.

Administrator Notification

For the administrator notification, select the Administrator check box to activate the text field. The default message comes with four variables (tokens):

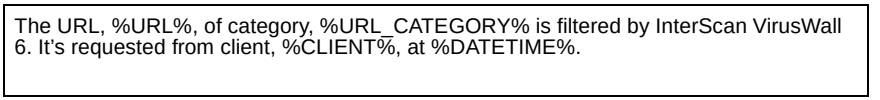


FIGURE 5-15. HTTP URL Filtering Settings screen, Notification tab, default Administrator notification message, showing the four default tokens used

However, several other tokens are available to choose from in customizing your message. Table 5-2 on page 5-23 lists all available tokens for this notification.

TABLE 5-2. HTTP URL filtering, administrator notification tokens and descriptions

Token	Description
%URL%	The target URL
%URL_CATEGORY%	Company Prohibited, Not Work Related, Possible Research Topics, Business Function Related, Customer Defined, or Other
%CLIENT%	The client IP address
%DATETIME%	Time and date of the attempted URL access
%PROTOCOL%	Always HTTP
%MACHINE_NAME%	The host name of the InterScan VirusWall server
%FILTER_NAME%	Always URLFiltering

Note: Remember to click **Save** at the bottom of the screen to save your choices.

Index

S

T

U

V

W