CHAPTER 4

Configuring Web (HTTP) and File Transfer (FTP) Traffic

This chapter describes how to make HTTP and FTP traffic configuration updates, and includes the following sections:

Default Web and FTP Scanning Settings

After installation, by default your HTTP and FTP traffic is scanned for viruses, worms, and Trojans. Malware such as spyware and other grayware require a configuration change before they are detected. Table 4-1 summarizes the web and file transfer configuration settings, and the default values that are in effect after installation.

Table 4-1 Default Web and FTP Scanning Settings

Feature	Default Setting
Web (HTTP) scanning of file downloads	Enabled using All Scannable Files as the scanning method.
Webmail scanning	Configured to scan Webmail sites for Yahoo, AOL, MSN, and Google.
File transfer (FTP) scanning of file transfers	Enabled using All Scannable Files as the scanning method.

Table 4-1 Default Web and FTP Scanning Settings (continued)

Feature	Default Setting
Web (HTTP) compressed file handling for downloading from the Web File transfer (FTP) compressed file handling for file transfers from an FTP server	Configured to skip scanning of compressed files when one of the following is true: • Decompressed file count is greater than 200. • Decompressed file size exceeds 30 MB. • Number of compression layers exceeds three. • Decompressed or compressed file size ratio is greater than 100 to 1.
Web (HTTP) and file transfer (FTP) large file handling (do not scan files larger than a specified size) Enabled deferred scanning of files larger than a specified size	Configured to skip scanning of files larger than 50 MB. Configured to enable deferred scanning of files larger than 2 MB.
Web (HTTP) downloads and file transfers (FTP) for files in which malware is detected	Clean the downloaded file or file in which the malware was detected. If uncleanable, delete the file.
Web (HTTP) downloads and file transfers (FTP) for files in which spyware or grayware is detected	Files are deleted.
Web (HTTP) downloads when malware is detected	An inline notification is inserted in the browser, stating that Trend Micro InterScan for CSC SSM has scanned the file you are attempting to transfer, and has detected a security risk.
File transfers (FTP) notification	The FTP reply has been received.

These default settings give you some protection for your Web and FTP traffic after you install Trend Micro InterScan for Cisco CSC SSM. You may change these settings. For example, you may prefer to use the Scan by specified file extensions option rather than All Scannable Files for malware detection. Before making changes, review the online help for more information about these selections.

After installation, you may want to update additional configuration settings to obtain the maximum protection for your Web and FTP traffic. If you purchased the Plus License, which entitles you to receive URL blocking, anti-phishing, and URL filtering functionality, you must configure these additional features.

Downloading Large Files

The Target tabs on the HTTP Scanning and FTP Scanning windows allow you to define the size of the largest download you want scanned. For example, you might specify that a download under 20 MB is scanned, but a download larger than 20 MB is not scanned.

In addition, you can:

- Specify large downloads to be delivered without scanning, which may introduce a security risk.
- Specify that downloads greater than the specified limit are deleted.

By default, the CSC SSM software specifies that files smaller than 50 MB are scanned, and files 50 MB and larger are delivered without scanning to the requesting client.

Deferred Scanning

The deferred scanning feature is not enabled by default. When enabled, this feature allows you to begin downloading data without scanning the entire download. Deferred scanning allows you to begin viewing the data without a prolonged wait while the entire body of information is scanned.

Caution When deferred scanning is enabled, the unscanned portion of information can introduce a security risk.

If deferred scanning is not enabled, the entire content of the download must be scanned before it is presented to you. However, some client software may time out because of the time required to collect sufficient network packets to compose complete files for scanning. The following table summarizes the advantages and disadvantages of each method.

Method	Advantage	Disadvantage
Deferred scanning enabled	Prevents client timeouts	May introduce a security risk
Deferred scanning disabled	Safer. The entire file is scanned for security risks before being presented to you.	May result in the client timing out before the download is complete

Note Traffic moving via HTTPS cannot be scanned for viruses and other threats by the CSC SSM software.

When the file is eventually scanned by CSC SSM, it may be found to contain malicious content. If so, CSC SSM takes following action:

- Sends a notification message, provided notifications are enabled
- Logs the event details
- Automatically blocks the URL from other users from four hours after malicious code detection. Access to the URL is restored after four hours elapses, and content from it will be scanned

If CSC SSM has been registered to a Damage Cleanup Services (DCS) server, a DCS clean-up request is issued under the following conditions:

- Someone (usually a client PC) attempts to access a URL classified as Spyware, Disease Vector, or Virus Accomplice by the PhishTrap pattern (requires a Plus license) or
- Someone (usually a client PC) uploads a virus classified as a “worm”

DCS connects to the client to clean the file. See more about DCS in Appendix C, “Using CSC SSM with Trend Micro Damage Cleanup Services”.

Spyware and Grayware Detection and Cleaning

Grayware is a category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

Spyware/grayware presents two main problems to network administrators. It can compromise sensitive company information and reduce employee productivity by causing infected machines to malfunction. In addition to detecting and blocking incoming files that may install spyware, CSC SSM can prevent installed spyware from sending confidential data via HTTP.

If a client tries to access a URL classified as spyware, disease vector, or virus accomplice by the PhishTrap pattern, or a client PC uploads a virus classified as a worm as a Web mail attachment, CSC SSM can send a request to Trend Micro Damage Cleanup Services (DCS) to clean the infected machine. DCS reports the outcome of the cleaning attempt (either successful or unsuccessful) to the CSC SSM server.

If the cleaning attempt is not successful, the client's browser is redirected to a special DCS-hosted cleanup page the next time it tries to access the Internet. This page contains an ActiveX control that again tries to clean the infected machine. If access permissions were the reason for the first failed cleaning attempt, the ActiveX control may be successful where cleaning via remote logon was unsuccessful.

See more about DCS in Using CSC SSM with Trend Micro Damage Cleanup Services, page C-1.

Note To avoid excessive cleanup attempts, CSC SSM only sends requests to cleanup a target IP once every four hours by default. If the client at that IP continues to perform suspicious actions, then no further cleanup requests will be issued until this lockout period has expired. You can modify the length of this lockout period by going to `/opt/trend/isvw/config/web/intscan.ini` on the CSC SSM and changing the value of the `[DCS]/cleanup_lockout_hours` field. The value in this field is interpreted as the number of hours, and partial values (such as 0.5) are supported.

Detecting Spyware and Grayware

Spyware or grayware detection is not enabled by default. To detect spyware and other forms of spyware and other grayware in your Web and file transfer traffic, you must configure this feature in the following windows:

- Web (HTTP) > Scanning > HTTP Scanning/Target
- File Transfer (FTP) > Scanning > FTP Scanning/Target

To configure web scanning, do the following:

On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure Web Scanning** link.

To configure FTP scanning, do the following:

On the Configuration > Trend Micro Content Security > File Transfer window in ASDM, click the **Configure File Scanning** link.

For more information, see the "Enabling SMTP and POP3 Spyware and Grayware Detection" section on page 3-3 and the online help for these windows.

Scanning Webmail

As specified in Table 4-1, Webmail scanning for Yahoo, AOL, MSN, and Google is already configured by default.

Caution If you elect to scan only Webmail, HTTP scanning is restricted to the sites specified on the Webmail Scanning tab of the Web (HTTP) > Scanning > HTTP Scanning window. Other HTTP traffic is not scanned. Configured sites are scanned until you remove them by clicking the **Trashcan** icon.

To add additional sites, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure Webmail Scanning** link.

The Target tab of the HTTP Scanning window appears.

Step 2 Click the **Webmail Scanning** tab.

Step 3 In the Name field, enter a name for the Webmail site.

Step 4 In the Match field, enter the exact website name/IP address, a URL keyword, and a string.

Step 5 Choose the appropriate radio button to correspond with the text entered in the Match field.

Note Attachments to messages that are managed via Webmail are scanned.

Step 6 Click **Save** to update your configuration.

For more information about how to configure additional Webmail sites for scanning, see the online help.

File Blocking

This feature is enabled by default; however, you must specify the types of files you want blocked. File blocking helps you enforce your organization policies for Internet use and other computing resources during work time. For example, your company does not allow downloading of music, both because of legal issues as well as employee productivity issues.

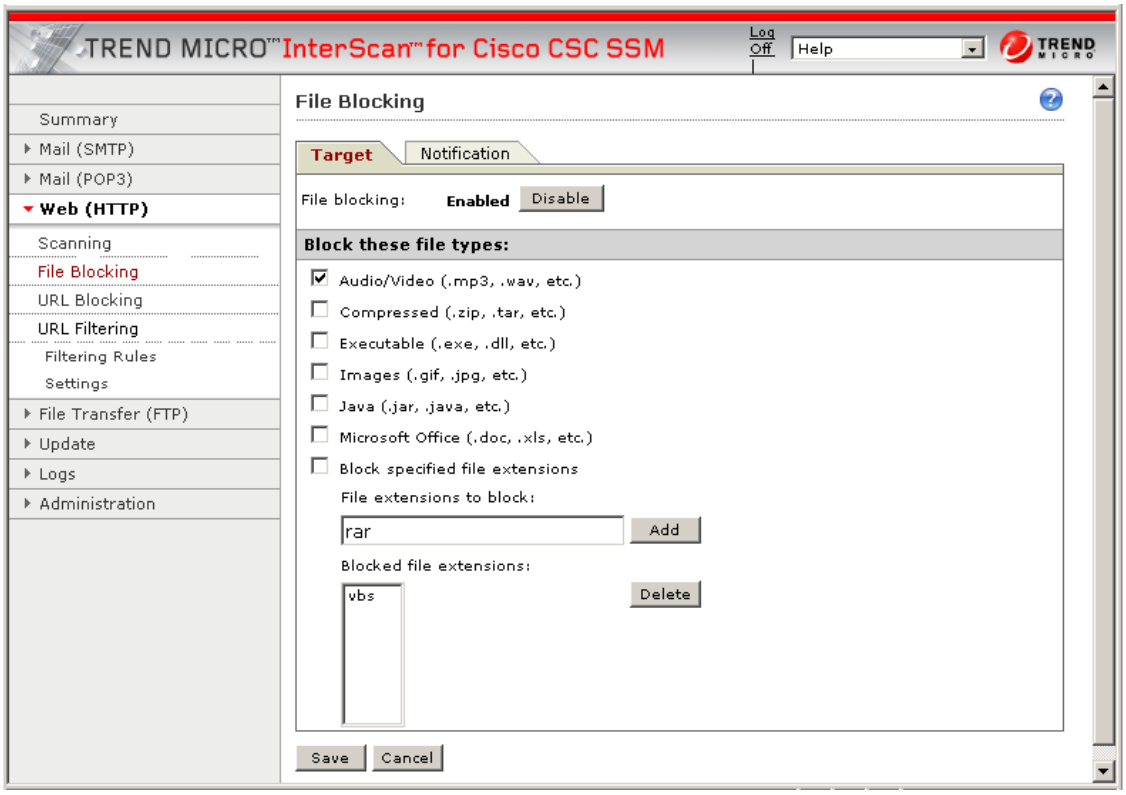
To configure file blocking, perform the following steps:

Step 1 To block downloads via HTTP, on the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure File Blocking** link to display the File Blocking window.

Step 2 To block downloads via FTP, on the Configuration > Trend Micro Content Security > File Transfer window in ASDM, click the **Configure File Blocking** link.

Step 3 To block transferring of music files, on the Target tab of the File Blocking window, check the **Audio/Video** check box, as shown in Figure 4-1.

Figure 4-1 Enable File Blocking



Step 4 You can specify additional file types by file name extension. To enable this feature, check the **Block specified file extensions** check box.

Step 5 Then enter additional file types in the File extensions to block field, and click **Add**. In the example, .vbs files are blocked.

For more information about file blocking and for information about deleting file extensions you no longer want to block, see the online help.

Step 6 To view the default notification that displays in the browser or FTP client when a file blocking event is triggered, click the **Notifications** tab of the File Blocking window.

Step 7 To customize the text of these messages, select and redefine the default message. An optional notification to the administrator is available for HTTP file-blocking events, but is turned off by default. Check the **Send the following message** check box to activate the notification.

Step 8 Click **Save** when you are finished to update the configuration.

URL Blocking

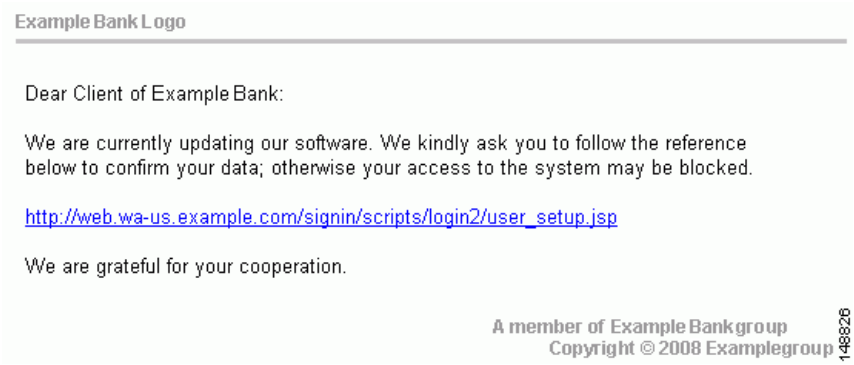
This section describes the URL blocking feature, and includes the following topics:

The URL blocking feature helps you prevent employees from accessing prohibited websites. For example, you may want to block some sites because policies in your organization prohibit access to dating services, online shopping services, or offensive sites.

Note This feature requires the Plus License.

You may also want to block sites that are known for perpetrating fraud, such as phishing. Phishing is a technique used by criminals who send e-mail messages that appear to be from a legitimate organization, which request revealing private information such as bank account numbers. Figure 4-2 shows an example of an e-mail message used for phishing.

Figure 4-2 Example of Phishing



By default, URL blocking is enabled. However, only sites in the TrendMicro PhishTrap pattern file are blocked until you specify additional sites for blocking.

Blocking from the Via Local List Tab

To configure URL blocking from the Via Local List tab, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click **Configure URL Blocking** to display the URL Blocking window.

Step 2 On the Via Local List tab of the URL Blocking window, type the URLs you want to block in the Match field. You can specify the exact website name or IP address, a URL keyword, and a string.

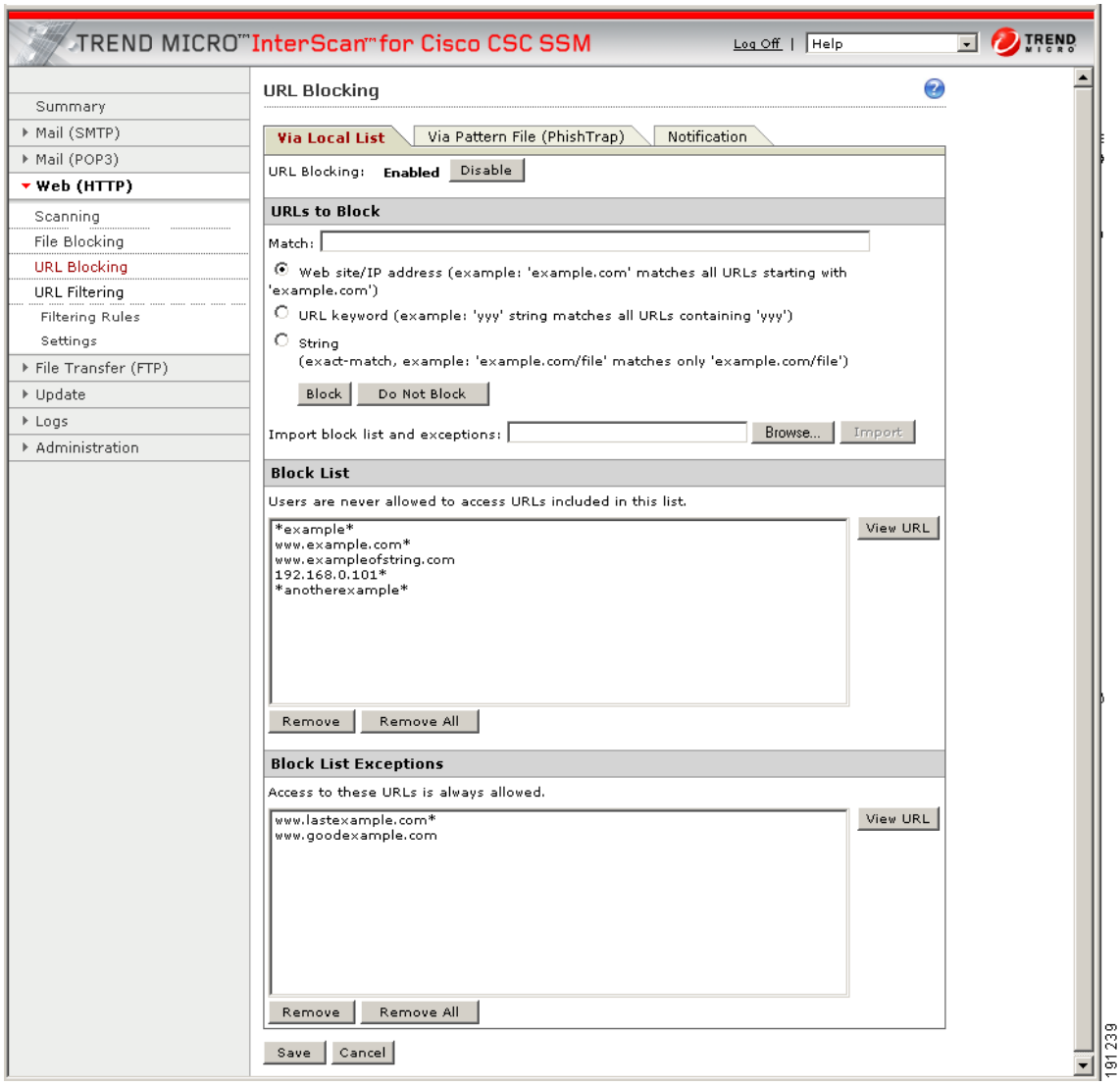
See the online help for more information about formatting entries in the Match field.

Step 3 To move the URL to the Block List, click **Block** after each entry. To specify your entry as an exception, click **Do Not Block** to add the entry to Block List Exceptions. Entries remain as blocked or exceptions until you remove them.

Note You can also import a block and exception list. The imported file must be in a specific format. See the online help for instructions.

Figure 4-3 shows an example of the URL Blocking window.

Figure 4-3 URL Blocking Window



Blocking from the Via Pattern File (PhishTrap) Tab

To configure URL file blocking from the Via Pattern File (Phishtrap) Tab, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure URL Blocking** link to display the URL Blocking window.

Step 2 Then click the **Via Pattern File (PhishTrap)** tab.

Step 3 By default, the Trend Micro PhishTrap pattern file detects and blocks known phishing sites, spyware sites, virus accomplice sites (sites associated with known exploits), and disease vectors (websites that exist only for malicious purposes). To submit sites that you think should be added to the PhishTrap pattern file, use the **Submit the Potential Phishing URL to TrendLabs** fields. TrendLabs^{SM} evaluates the site and may add the site to this file if such action is warranted.

Step 4 To review the text of the default message that appears in the browser when an attempt is made to access a blocked site, click the **Notification** tab. The online help shows an example. Customize the default message by highlighting and redefining it. Add a company logo to the notification message, if desired.

Step 5 Click **Save** when you are finished to update the configuration.

URL Filtering

This section describes how to configure the URL filtering feature, and includes the following topics:

- Filtering Settings, page 4-14
- Filtering Rules, page 4-15

The URLs defined on the URL Blocking windows described previously are either always allowed or always disallowed. The URL filtering feature, however, allows you to filter URLs in categories, which you can schedule to allow access during certain times, such as leisure and work time.

Note This feature requires the Plus License.

Six URL Filtering types can be assigned to the URL Filtering categories as follows:

- Company-prohibited
- Not work related
- Research topics
- Business function
- Customer defined
- Others

By default, company-prohibited sites are blocked during both work and leisure times.

URL Filtering Categories

Table 4-2 lists the category definitions and grouping.

Table 4-2 URL Filtering Categories and Definitions

Category Type	Category Group	Category Definition
Adult/Mature Content	Adult	Sites with profane or vulgar content generally considered inappropriate for minors; includes sites that offer erotic content or ads for sexual services, but excludes sites with sexually explicit images
Pornography	Adult	Sites with sexually explicit imagery designed for sexual arousal, including sites that offer sexual services
Sex Education	Adult	Sites with or without explicit images that discuss reproduction, sexuality, birth control, sexually transmitted disease, safe sex, or coping with sexual trauma

Table 4-2 URL Filtering Categories and Definitions (continued)

Category Type	Category Group	Category Definition
Intimate Apparel/ Swimsuit	Adult	Sites that sell swimsuits or intimate apparel with models wearing them
Nudity	Adult	Sites showing nude or partially nude images that are generally considered artistic, not vulgar or pornographic
Alcohol/Tobacco	Adult	Sites that promote, sell, or provide information about alcohol or tobacco products
Illegal/Questionable	Adult	Sites that promote and discuss how to perpetrate "nonviolent" crimes, including burglary, fraud, intellectual property theft, and plagiarism; includes sites that sell plagiarized or stolen materials
Tasteless	Adult	Sites with content that is gratuitously offensive and shocking; includes sites that show extreme forms of body modification or mutilation and animal cruelty
Gambling	Adult	Sites that promote or provide information on gambling, including online gambling sites
Violence/Hate/ Racism	Adult	Sites that promote hate and violence; includes sites that espouse prejudice against a social group, extremely violent and physically dangerous activities, mutilation and gore, or the creation of destructive devices
Weapons	Adult	Sites about weapons, including their accessories and use; excludes sites about military institutions or sites that discuss weapons as sporting or recreational equipment
Abortion	Adult	Sites that promote, encourage, or discuss abortion, including sites that cover moral or political views on abortion
Recreation/Hobbies	Lifestyle	Sites about recreational activities and hobbies, such as collecting, gardening, outdoor activities, traditional (non-video) games, and crafts; includes sites about pets, recreational facilities, or recreational organizations
Arts	Lifestyle	Sites that promote and provide information about books, poetry, comics, movie theatres, and artists.
Entertainment	Lifestyle	Sites that promote or provide information about movies, music, non-news radio and television, books, humor, or magazines
Business/Economy	Business	Sites about business and the economy, including entrepreneurship and marketing; includes corporate sites that do not fall under other categories
Cult/Occult	Lifestyle	Sites about alternative religions, beliefs, and religious practices, including those considered cult or occult
Internet Radio and TV	Network Bandwidth	Sites that primarily provide streaming radio or TV programming; excludes sites that provide other kinds of streaming content
Internet Telephony	Communica-tions and Search	Sites that provide Web services or downloadable software for Voice over Internet Protocol (VoIP) calls

Table 4-2 URL Filtering Categories and Definitions (continued)

Category Type	Category Group	Category Definition
Illegal Drugs	Adult	Sites that promote, glamorize, supply, sell, or explain how to use illicit or illegal intoxicants
Marijuana	Adult	Sites that discuss the cultivation, use, or preparation of marijuana, or sell related paraphernalia
Education	General	School sites, distance learning sites, and other education-related sites
Cultural Institutions	Lifestyle	Sites controlled by organizations that seek to preserve cultural heritage, such as libraries or museums; also covers sites owned by the Boy Scouts, the Girl Scouts, Rotary International, and similar organizations
Activist Groups	Social	Sites that promote change in public policy, public opinion, social practice, economic activities, or economic relationships; includes sites controlled by service, philanthropic, professional, or labor organizations
Financial Services	Business	Sites that provide information about or offer basic financial services, including sites owned by businesses in the financial industry
Brokerage/Trading	Business	Sites about investments in stocks or bonds, including online trading sites; includes sites about vehicle insurance
Games	Lifestyle	Sites about board games, card games, console games, or computer games; includes sites that sell games or related merchandise
Government/Legal	General	Sites about the government, including laws or policies; excludes government military or health sites
Military	General	Sites about military institutions or armed forces; excludes sites that discuss or sell weapons or military equipment
Political/Activist Parties	General	Sites that discuss or are sponsored by political parties, interest groups, or similar organizations involved in public policy issues; includes non-hate sites that discuss conspiracy theories or alternative views on government
Health	General	Sites about health, fitness, or well-being
Computers/Internet	General	Sites about computers, the Internet, or related technology, including sites that sell or provide reviews of electronic devices
Proxy Avoidance	Internet Security	Sites about bypassing proxy servers or Web filtering systems, including sites that provide tools for that purpose
Search Engines/ Portals	Communica-tions and Search	Search engine sites or portals that provide directories, indexes, or other retrieval systems for the Web
Infrastructure	Communica-tions and Search	Content servers, image servers, or sites used to gather, process, and present data and data analysis, including Web analytics tools and network monitors

Table 4-2 URL Filtering Categories and Definitions (continued)

Category Type	Category Group	Category Definition
Blogs/Web Communications	Communica-tions and Search	Blog sites or forums on varying topics or topics not covered by other categories; sites that offer multiple types of Web-based communication, such as email or instant messaging
Photo Searches	Network Bandwidth	Sites that primarily host images, allowing users to share, organize, store, or search for photos or other images
Job Search/Careers	Business	Sites about finding employment or employment services
News/Media	General	Sites about the news, current events, contemporary issues, or the weather; includes online magazines whose topics do not fall under other categories
Personals/Dating	Lifestyle	Sites that help visitors establish relationships, including sites that provide singles listings, matchmaking, or dating services
Translators (circumvent filtering)	General	Online page translators or cached Web pages (used by search engines), which can be used to circumvent proxy servers and Web filtering systems
Reference	General	General and specialized reference sites, including map, encyclopedia, dictionary, weather, how-to, and conversion sites
Social Networking	Communication s and Search	Sites devoted to personal expression or communication, linking people with similar interests
Chat/Instant Messaging	Communica-tions and Search	Sites that provide Web-based services or downloadable software for text-based instant messaging or chat
Emails	Communica-tions and Search	Sites that provide email services, including portals used by companies for Web-based email
Newsgroups	Communica-tions and Search	Sites that offer access to Usenet or provide other newsgroup, forum, or bulletin board services
Religion	Lifestyle	Sites about popular religions, their practices, or their places of worship
Personal Websites	Lifestyle	Sites maintained by individuals about themselves or their interests; excludes personal pages in social networking sites, blog sites, or similar services
Personal Network Storage/File Download Servers	Network Bandwidth	Sites that provide personal online storage, backup, or hosting space, including those that provide encryption or other security services
Peer-to-Peer	Network Bandwidth	Sites that provide information about or software for sharing and transferring files within a peer-to-peer (P2P) network
Shopping	Business	Sites that sell goods or support the sales of goods that do not fall under other categories; excludes online auction or bidding sites
Auctions	Business	Sites that serve as venues for selling or buying goods through bidding, including business sites that are being auctioned

Table 4-2 URL Filtering Categories and Definitions (continued)

Category Type	Category Group	Category Definition
Real Estate	Business	Sites about real estate, including those that provide assistance selling, leasing, purchasing, or renting property
Society/Lifestyle	Lifestyle	Sites that provide information about life or daily matters; excludes sites about entertainment, hobbies, sex, or sports, but includes sites about cosmetics or fashion
Gay/Lesbian/Bisexual	Lifestyle	Sites about gay, lesbian, transgender, or bisexual lifestyles
Sport Hunting and Gun Clubs	Lifestyle	Sites about gun clubs or similar groups; includes sites about hunting, war gaming, or paintball facilities
Restaurants/Dining/ Food	Lifestyle	Sites that list, review, discuss, advertise, or promote food, catering, dining services, cooking, or recipes
Sports	Lifestyle	Sites about sports or other competitive physical activities; includes fan sites or sites that sell sports merchandise
Travel	Lifestyle	Sites about travelling or travel destinations; includes travel booking and planning sites
Vehicles	General	Sites about motorized transport, including customization, procurement of parts and actual vehicles, or repair services; excludes sites about military vehicles
Humor/Jokes	Lifestyle	Sites about motorized transport, including customization, procurement of parts and actual vehicles, or repair services; excludes sites about military vehicles
Streaming Media/ MP3	Network Bandwidth	Sites that offer streaming video or audio content without radio or TV programming; sites that provide music or video downloads, such as MP3 or AVI files
Ringtones/Mobile Phone Downloads	Network Bandwidth	Sites that provide content for mobile devices, including ringtones, games, or videos
(Software) Downloads	Network Bandwidth	Sites dedicated to providing free, trial, or paid software downloads
Pay to Surf	Network Bandwidth	Sites that compensate users who view certain Web sites, email messages, or advertisements or users who click links or respond to surveys
Potentially Malicious Software	Internet Security	Sites that contain potentially harmful downloads
Spyware	Internet Security	Sites with downloads that gather and transmit data from computers owned by unsuspecting users
Phishing	Internet Security	Fraudulent sites that mimic legitimate sites to gather sensitive information, such as user names and passwords
Spam	Internet Security	Sites whose addresses have been found in spam messages
Adware	Internet Security	Sites with downloads that display advertisements or other promotional content; includes sites that install browser helper objects (BHOs)
Virus/Malware Accomplice	Internet Security	Sites used by malicious programs, including sites used to host upgrades or store stolen information

Table 4-2 URL Filtering Categories and Definitions (continued)

Category Type	Category Group	Category Definition
Disease Vector	Internet Security	Sites that directly or indirectly facilitate the distribution of malicious software or source code
Cookies	Internet Security	Sites that send malicious tracking cookies to visiting Web browsers
Dialers	Internet Security	Sites with downloads that dial into other networks or premium-rate telephone numbers without user consent
Hacking	Internet Security	Sites that provide downloadable software for bypassing computer security systems
Joke Program	Internet Security	Sites that provide downloadable “joke” software, including applications that can unsettle users
Password Cracking Application	Internet Security	Sites that distribute password cracking software
Remote Access Program	Internet Security	Sites that provide tools for remotely monitoring and controlling computers
Made for AdSense sites (MFA)	Lifestyle	Sites that use scraped or copied content to pollute search engines with redundant and generally unwanted results
For Kids	General	Sites designed for children
Web Advertisement	Internet Security	Sites dedicated to displaying advertisements, including sites used to display banner or popup ads
Web Hosting	Communica-tions and Search	Sites of organizations that provide top-level domains or Web hosting services
Unrated	General	Sites that have not been classified under a category

Filtering Settings

To configure the URL filtering feature, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click **Configure URL Filtering Settings** to display the URL Filtering Settings window.

Step 2 On the URL Categories tab, review the subcategories listed and the default classifications assigned to each category to see whether the assignments are appropriate for your organization. For example, “Illegal Drugs” is a subcategory of the “Company-prohibited” category. If your organization is a financial services company, you may want to leave this category classified as company-prohibited. Check the **Illegal Drugs** check box to enable filtering for sites related to illegal drugs. However, if your organization is a law enforcement agency, you should reclassify the “Illegal Drugs” subcategory to the “Business function” category. See the online help for more information about reclassification.

Step 3 After you have reviewed and refined the subcategory classifications, check the associated subcategory to enable all the subcategories for which you want filtering performed.

Step 4 If there are sites within some of the enabled subcategories that you do not want filtered, click the **URL Filtering Exceptions** tab.

Step 5 Type the URLs you want to exclude from filtering in the Match field. You can specify the exact website name or IP address, a URL keyword, and a string.

See the online help for more information about formatting entries in the Match field.

Note You can also import a list of URL filtering exceptions. The imported file must be in a specific format. See the online help for instructions.

Step 6 Click **Add** after each entry to move it to the "URL to the Do Not Filter the Following Sites" list. Entries remain as exceptions until you remove them.

Step 7 In the Approved Client IP Addresses section, type the client IP addresses you want to exclude from URL filtering rules in the IP/IP range/subnet mask: field. Approved clients can be added by individual IP address, IP range or subnet mask. See on-screen examples for formatting details.

Step 8 Click **Add** after each entry to move the IP address, IP range, or subnet mask to the approved list. To remove an entry, select it from the list and click **Delete**.

Note Client IP addresses added to the approved list may not function correctly for DHCP client PC users or mobile PC users who do not have a static IP addresses.

Step 9 Click the **Schedule** tab to define the days of the week and hours of the day that should be considered work time. Time not designated as work time is automatically designated as leisure time.

Step 10 Click **Save** to update the URL filtering configuration.

Step 11 Click the **Reclassify URL** tab to submit suspect URLs to TrendLabs for evaluation.

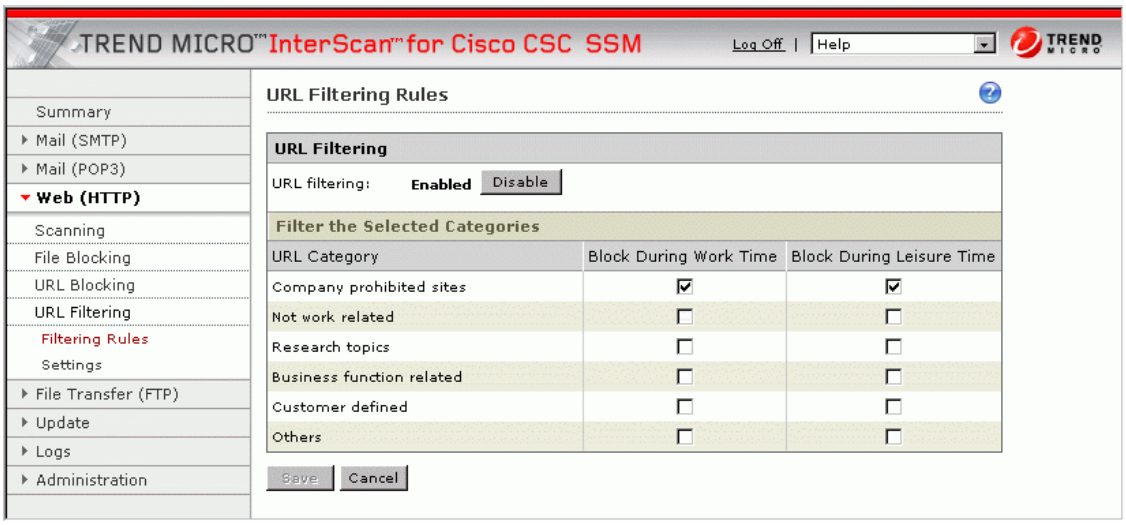
Filtering Rules

After you have assigned the URL subcategories to correct categories for your organization, defined exceptions (if any), and created the work and leisure time schedule, assign the filtering rules that determine when a category is filtering.

To assign the URL filtering rules, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure URL Filtering Rules** link to display the URL Filtering Rules window, shown in Figure 4-4.

Figure 4-4 URL Filtering Rules Window



Step 2 For each of the six major categories, specify whether the URLs in that category are blocked, and if so, during work time, leisure time, or both. See the online help for more information.

Step 3 Click **Save** to update the configuration.

Note For URL Filtering to work correctly, the CSC SSM module must be able to send HTTP requests to the Trend Micro service. If an HTTP proxy is required, configure the proxy setting by choosing **Update > Proxy Settings**.