Installation Guide Supplement

for use with

Integrated Cisco® Products

Websense® Web Security
Websense Web Filter

v7.5

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2010
Printed in the United States of America and Ireland.

Trademarks

Contents

1 Cisco Integration

This supplement to the *Websense Web Security and Websense Web Filter Installation Guide* (*Installation Guide*) provides information specific to integrating Websense software with Cisco® Adaptive Security Appliance (ASA), Cisco PIX® Firewall, Cisco IOS routers, and Cisco Content Engine. For general installation instructions, refer to the *Installation Guide*.

Integrating Websense software with a Cisco product involves the following components:

- **Filtering Service**: The integrated Cisco product and Network Agent work with Filtering Service to filter Internet requests. For redundancy, two or more instances of Filtering Service may be used. Only one instance will be active at any given time—referred to as the primary server. URL look-up requests will be sent only to the primary server. For more information see the configuration chapter, in this supplement, for your Cisco product. Also see Cisco documentation for detailed explanations of configuration commands.
- **Network Agent**: Manages Internet protocols that are not managed by your integrated Cisco product.

  If Network Agent is installed, you must define the IP addresses of all proxy servers through which computers route their Internet requests. See *Network Configuration* in the TRITON - Web Security Help for instructions.
- **Configure your Cisco integration**: You must direct Internet requests through your Cisco integration product, and configure it for use with Websense software.
  - *Chapter 2: Configuring a Cisco Security Appliance* discusses Cisco PIX Firewall and Adaptive Security Appliance (ASA)
  - *Chapter 3: Configuring a Cisco IOS Router* discusses Cisco IOS router.
  - *Chapter 4: Configuring a Cisco Content Engine* discusses Cisco Content Engine.
- **User authentication**: To work properly, Filtering Service must be installed in the same domain (Windows), or the same root context (LDAP), as Cisco Secure ACS.

  If you are using a Websense transparent identification agent or manual authentication, this configuration is not necessary.

How Websense filtering works with Cisco products

To be filtered by Websense software, a client's Internet requests must pass through the Cisco product.

- If Websense software is integrated with a Cisco PIX Firewall or ASA, browser requests must go through the PIX Firewall or ASA to reach the Internet.
- If Websense software is integrated with a Cisco Content Engine, client browser requests may be forwarded to the Content Engine transparently or explicitly. See *Browser access to the Internet*, page 33.

When it receives an Internet request, the Cisco product queries Filtering Service to determine if the requested Web site should be blocked or permitted. Filtering Service consults the policy assigned to the user. Each policy designates specific time periods and lists the category filters that are applied during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database.

- If the site is assigned to a blocked category, the user receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies the Cisco product that the site is not blocked, and the client is allowed to visit the site.

> **Note**
> Before enabling Websense URL filtering, make sure there is not another URL filtering scheme configured, such as N2H2. There can be only one active URL filtering scheme at a time.

Supported Cisco integration product versions

Websense software is compatible with the following versions of Cisco products:

- Cisco PIX Firewall Software v5.3 and higher
- Cisco ASA Software v7.0 and higher
- Cisco Content Engine ACNS versions 5.4, 5.5, and 5.6
- Cisco routers with Cisco IOS Software Release 12.3 and higher

Command conventions

The following conventions are used for commands in this document:

- Angle brackets (< >) indicate variables that must be replaced by a value in the command.

- Square brackets ([ ]) indicate an optional element or value.
- Braces ({ }) indicate a required choice.
- A forward slash (/) separates each value within curly braces.
- Vertical bars (|) separate alternative, mutually exclusive elements

Installation of Websense software

Refer to the *Installation Guide* for complete instructions on downloading and running the Websense installer.

After launching the installer, follow the instructions in the *Installation Guide*, with the following modifications. (Note: for those screens or steps not mentioned here, follow the instructions as presented in the *Installation Guide*.)

- On the **Integration Option** screen, select **Integrated with another application or device**.
- On the **Select Integration** screen, select one of the following and then click **Next**:
  - **Cisco Adaptive Security Appliances**
  - **Cisco Content Engine**
  - **Cisco PIX Firewall**
  - **Cisco Routers**
- Do not install a transparent identification agent if you plan to configure user authentication through your Cisco product.

  In a typical installation (*Filtering and Management* or *Filtering, Management, and Reporting*), the **Transparent User Identification** screen is used to select a transparent identification agent. Select **Do not install a transparent identification agent now** if you will authenticate users through your Cisco product.

  In a custom installation (or when adding components), on the **Select Components** screen, do not select any of the components under **User identification** if you will authenticate users through your Cisco product.

> **Note**
> Websense software cannot use Cisco Secure Access Control Server (ACS) for user authentication for more than one user domain. If there are multiple user domains, use a Websense transparent identification agent.

Upgrading Websense software

When Websense software, already integrated with a Cisco product, is upgraded no additional configuration is necessary on the Cisco product. See the *Installation Guide*

and *Websense Web Security and Websense Web Filter Installation Guide Supplement for Upgrading* for upgrading instructions.

> **Note**
> Prior to upgrading Websense software, make sure your Cisco product is supported by the new version. See *Supported Cisco integration product versions*, page 6.

If you are upgrading your Websense deployment and changing your integration product, see *Migrating between integrations after installation*, below.

Migrating between integrations after installation

You can change the Cisco integration product (for example, change from a PIX Firewall to an IOS router) after installing Websense software without losing configuration data.

1. Install and configure your new Cisco integration product. See Cisco documentation for instructions.

   Ensure that it is deployed so that it can communicate with Filtering Service and Policy Server.
2. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
3. Close all applications on the Filtering Service machine, and stop any antivirus software.
4. Remove Filtering Service. Instructions for removing components are available in the *Installation Guide*.

   > **Warning**
   > Remove Filtering Service only. Do **not** remove the associated Policy Server.

5. Restart the machine (Windows only).
6. Use the Websense installer to reinstall Filtering Service. Procedures for adding individual components can be found in the *Installation Guide*.
7. On the **Select Integration** screen, select the new Cisco product, and then follow the on-screen instructions to complete the installation.

   The installer adds the new integration data to the Websense software configuration files, while preserving existing configuration data.
8. Restart the machine (Windows only).

9. Check to be sure that Filtering Service has started.
   - Windows: Use the Windows Service Control Manager box to verify that **Websense Filtering Service** has started.
   - Linux: Navigate to the Websense installation directory (/opt/Websense, by default), and use the following command to verify that **Websense Filtering Service** is running:

     ```
     ./WebsenseAdmin status
     ```

   For instructions on starting Websense services, see the *Installation Guide*.
10. Open TRITON - Web Security to identify which Filtering Service instance is associated with each Network Agent.
    a. Open the **Settings** tab.
    b. Go to **Settings > Network Agent** and click the appropriate IP address in the navigation pane to open the **Local Settings** page.
    c. Under **Filtering Service Definition**, select the IP address for the machine running Filtering Service. During the migration, the setting may have been reset to None.
    d. Log out of TRITON - Web Security.

    For more information, see the information about configuring local settings in the *Network Configuration* section of TRITON - Web Security Help.
11. If you stopped your antivirus software, be sure to start it again.

2 Configuring a Cisco Security Appliance

After Websense software is installed, the Cisco security appliance, PIX firewall, or Adaptive Security Appliance (ASA) must be configured to work with Websense software. The Cisco firewall passes each Internet request to Filtering Service, which analyzes the request and determines whether to block or permit access, or limit access by using quotas set in Websense policies.

See the TRITON - Web Security Help for information about implementing filtering policies.

This chapter contains instructions for configuring Websense integration with Cisco PIX Firewall or Adaptive Security Appliance (ASA) through a console or Telnet session:

For information on configuring your security appliance through the management interface, see the documentation for your Cisco product, available at www.cisco.com.

> **Note**
> In this chapter, the term *security appliance* is used to refer to both Cisco PIX Firewall and ASA collectively.

Configuration procedure

To configure your security appliance to send Internet requests to Websense software for filtering:

1. Access the security appliance from a console or from a remote terminal using telnet for access
2. Enter your password.
3. Enter **enable**, followed by the enable password to put the security appliance into privileged EXEC mode.

4. Enter **configure terminal** to activate configure mode.

> **Note**
> For help with individual commands, enter **help** followed by the command. For example, **help filter** shows the complete syntax for the **filter** command and explains each option.

5. Use the **url-server** command to enable URL filtering by Websense software.

```
url-server (<if_name>) vendor websense host <ip_address>
[timeout <seconds>] [protocol {TCP | UDP} version {1 | 4}
[connections <num_conns>]]
```

The **url-server** command takes the following parameters:

Parameter	Definition
`(<if_name>)`	The network interface where Websense Filtering Service resides. In v7.0 of the Cisco security appliance software, a value for this parameter must be entered. In v6.3.1 and earlier, <*if_name*> defaults to `inside` if not specified. You must type the parentheses ( ) when you enter a value for this parameter.
`vendor websense`	Indicates the URL filtering service vendor is Websense.
`<ip_address>`	IP address of the machine running Filtering Service.
`timeout <seconds>`	The amount of time, in seconds, that the security appliance waits for a response before switching to the next Filtering Service that you defined as a **url-server**, or, if specified, going into allow mode and permitting all requests. If a timeout interval is not specified, this parameter defaults to 30 seconds in v7.0(1) and later, and 5 seconds in earlier versions of the Cisco PIX or ASA software. • v7.0(1) and later: Range: 10 - 120; Default: 30 • v6.3: Range: 1 - 30; Default: 5
`protocol {TCP | UDP} version {1 | 4}`	Defines whether the Cisco security appliance should use TCP or UDP protocol to communicate with Filtering Service, and which version of the protocol to use. **TCP** is the recommended and default setting. The recommended protocol version is **4**. The default is 1. (*Note*: To send authenticated user information to Filtering Service, TCP version 4 must be selected.)

Parameter	Definition
`connections <num_conns>`	Limits the maximum number of TCP connections permitted between the Cisco security appliance and Filtering Service. If this parameter is not specified, it defaults to **5**, which is the recommended setting. If you select the UDP protocol, this option is not available. Range: 1 - 100; Default: 5.

Example:

```
url-server (inside) vendor websense host 10.255.40.164
timeout 30 protocol TCP version 4 connections 5
```

The **url-server** command communicates the location of Filtering Service to the Cisco security appliance. More than one **url-server** command can be entered. Multiple commands allow redirection to another Filtering Service after the specified timeout period, if the first server becomes unavailable.

6. Configure the security appliance to filter HTTP requests with the **filter url** command.

   - To review the current URL server rules, enter **show running-config url-server** (v7.0) or **show url-server** (v6.3).
   - To review all the filter rules, enter **show running-config filter** (v7.0) or **show filter** (v6.3).

   To configure HTTP request filtering, use the following command:

   ```
   filter url http <port>[-<port>] <local_ip> <local_mask>
   <foreign_ip> <foreign_mask> [allow] [cgi-truncate]
   [longurl-truncate | longurl-deny] [proxy-block]
   ```

   For an explanation of the **filter url** parameters, see *Parameters for the filter commands*, page 18.

   Examples:

Command example	Action
`filter url http 0 0 0 0`	Filters every HTTP request to all destinations. Filtering is applied to traffic on port 80.
`filter url http 10.5.0.0 255.255.0.0 0 0`	Filters the 10.5.x.x network going to any destination. Filtering is applied to traffic on port 80.
`filter url http 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255`	Filters the 10.5.0.69 host going to the 132.239.29.189 destination. Filtering is applied to traffic on port 80.

Using zeroes for the last two entries, <*foreign_ip*> and <*foreign_mask*>, allows access from the specified local IP address to all Web sites, as filtered by Websense software

You can enter multiple **filter url** commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. Use a general **filter url** command for all computers to be filtered, and then use TRITON - Web Security to apply filtering policies to individual clients (computers, networks, users, groups, and domains [OUs]).

See the TRITON - Web Security Help for information about implementing filtering policies.

7. Configure the security appliance to filter HTTPS requests with the **filter https** command.
   - To review the current URL server rules, enter **show run url-server** (v7.0) or **show url-server** (v6.3.1).
   - To review all the filter rules, enter **show run filter** (v7.0) or **show filter** (v6.3.1).
   - If you are running v7.0 of Cisco software, enter **exit** to go up a level to run the show command.

   Note
   The **filter https** command is supported in v6.3.1 and higher of the Cisco PIX Firewall/ASA software.

   To configure HTTPS request filtering, use the following command:

   ```
   filter https <port> <local_ip> <local_mask> <foreign_ip>
   <foreign_mask> [allow]
   ```

   For an explanation of the **filter https** parameters, see *Parameters for the filter commands*, page 18.

   Examples:

Command example	Action
`filter https 443 0 0 0 0`	Filters all HTTPS requests to all destinations. Filtering is applied to traffic on port 443.
`filter https 443 10.5.0.0 255.255.0.0 0 0`	Filters the 10.5.x.x network going to any destination. Filtering is applied to traffic on port 443.
`filter https 443 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255`	Filters the 10.5.0.69 host going to the 132.239.29.189 destination. Filtering is applied to traffic on port 443.

Using zeroes for the last two entries, <*foreign_ip*> and <*foreign_mask*>, allows access from the specified local IP address to all Web sites, as filtered by Websense software.

You can enter multiple **filter https** commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. Use a general **filter https** command for all computers to be filtered, and then use TRITON - Web Security to apply filtering policies to individual clients (computers, networks, users, groups, and domains [OUs]).

See the TRITON - Web Security Help for information about implementing filtering policies.

8. Configure the Cisco security appliance to filter FTP requests with the **filter ftp** command.
   - To review the current URL server rules, enter **show run url-server** (v7.0) or **url-server** (v6.3.1).
   - To review all the filter rules, enter **show run filter** (v7.0) or **show filter** (v6.3.1).
   - If you are running v7.0 of Cisco software, enter **exit** to go up a level to run the **show** command.

   Note

   The **filter ftp** command is supported in v6.3.1 and higher of the Cisco PIX Firewall/ASA software.

   To configure FTP request filtering, use the following command:

   ```
   filter ftp <port> <local_ip> <local_mask> <foreign_ip>
   <foreign_mask> [allow] [interact-block]
   ```

   For an explanation of the **filter ftp** parameters, see *Parameters for the filter commands*, page 18.

   Examples:

Command example	Action
`filter ftp 21 0 0 0 0`	Filters every FTP request to all destinations. Filtering is applied to traffic on port 21.
`filter ftp 21 10.5.0.0 255.255.0.0 0 0`	Filters the 10.5.x.x network going to any destination. Filtering is applied to traffic on port 21.
`filter ftp 21 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255`	Filters the 10.5.0.69 host going to the 132.239.29.189 destination. Filtering is applied to traffic on port 21.

   Using zeroes for the last two entries, <*foreign_ip*> and <*foreign_mask*>, allows access via Websense software from the specified local IP address to all Web sites.

You can enter multiple **filter ftp** commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. Use a general **filter ftp** command for all computers to be filtered, and then use TRITON - Web Security to apply filtering policies to individual clients (computers, networks, users, groups, and domains [OUs]).

See the TRITON - Web Security Help for information about implementing filtering policies.

9. After entering commands to define filtering for HTTP, HTTPS, and FTP requests, you can define any required exceptions to these filtering rules by adding the **except** parameter to the **filter** command:

   ```
   filter {url | https | ftp} except <local_ip> <local_mask>
   <foreign_ip> <foreign_mask>
   ```

   This command allows you to bypass Websense filtering for traffic coming from, or going to a specified IP address or addresses.

   For example, suppose that the following filter command was entered to cause all HTTP requests to be forwarded to Filtering Service:

   ```
   filter url http 0 0 0 0
   ```

   You could then enter:

   ```
   filter url except 10.1.1.1 255.255.255.255 0 0
   ```

   This would allow any outbound HTTP traffic from the IP address 10.1.1.1 to go unfiltered.

10. Configure the security appliance to handle long URLs using the **url-block url-mempool** and **url-block url-size** commands:

    Note

    The **url-block** commands are supported in v6.2 and higher of the Cisco PIX Firewall/ASA software.

    a. Increase the size of the security appliance's internal buffer to handle long URL strings. If the URL buffer size is set too low, some Web pages may not display.

       To specify the amount of memory assigned to the URL buffer, enter:

       ```
       url-block url-mempool <memory_pool_size>
       ```

       Here, *<memory_pool_size>* is the size of the buffer in KB. You can enter a value from 2 to 10240. The recommended value is 1500.

    b. Increase the maximum permitted size of a single URL by adding the following line to the configuration:

       ```
       url-block url-size <long_url_size>
       ```

       Here, *<long_url_size>* is the maximum URL size in KB. You can enter a value from 2 to 4. The recommended value is 4.

11. Configure the URL response block buffer using the **url-block block** command to prevent replies from the Web server from being dropped in high-traffic situations.

    > **Note**
    > The **url-block** commands are supported in v6.2 and higher of the Cisco PIX Firewall/ASA software.

    On busy networks, the lookup response from Filtering Service may not reach the security appliance before the response arrives from the Web server.

    The HTTP response buffer in the security appliance must be large enough to store Web server responses while waiting for a filtering decision from the Filtering Service.

    To configure the block buffer limit, use the following command:

    ```
    url-block block <block_buffer_limit>
    ```

    Here, <*block_buffer_limit*> is the number of 1550-byte blocks to be buffered. You can enter a value from 1 to 128.

    - To view the current configuration for all 3 **url-block** commands, enter **show running-config url-block** (v7.0) or **show url-block** (v6.3).
    - Enter **show url-block block statistics** to see how the current buffer configuration is functioning. The statistics include the number of pending packets held and the number dropped. The **clear url-block block statistics** command clears the statistics.

12. If you need to discontinue filtering, enter the exact parameters in the original **filter** command, preceded by the word **no**.

    For example, if you entered the following to enable filtering:

    ```
    filter url http 10.0.0.0 255.0.0.0 0 0
    ```

    Enter the following to disable filtering:

    ```
    no filter url http 10.0.0.0 255.0.0.0 0 0
    ```

    Repeat for each filter command issued, as appropriate.

13. Save your changes in one of the following ways:

    ```
    copy run start
    ```

    or

    ```
    exit
    write memory
    ```

Websense software is ready to filter Internet requests after the Websense Master Database is downloaded and the software is activated within the Cisco security appliance. See the Websense *Installation Guide* and the TRITON - Web Security Help for information about configuring Websense software and downloading the Master Database.

Parameters for the filter commands

The parameters used by the **filter http**, **filter https**, and **filter ftp** commands include the following. Note that some of the parameters listed do not apply to all 3 commands.

Parameter	Applies to	Definition
`http <port>[-<port>]`	`filter http`	Defines which port number, or range of port numbers, the security appliance watches for HTTP requests. If you do not specify a port number, port 80 is used by default. The option to set a custom Web port or port range is only available in v5.3 and higher of Cisco software. **Note:** In Cisco software versions 5.3 to 6.3, it is not mandatory to enter **http** before the port number; you can either enter **http** (to use port 80), or you can enter a port number. In Cisco software version 7.0, you must always enter **http**.
`<port>`	`filter https` `filter ftp`	Defines the port number the security appliance watches for https or ftp requests. The standard HTTPS port is **443**. The standard FTP port is **21**.

`<local_ip>`	`filter http`
	`filter https`
	`filter ftp`
		IP address requesting access.
		You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all internal clients. This address is the source for all connections to be filtered.

`<local_mask>`	`filter http`
	`filter https`
	`filter ftp`
		Network mask of the **local_ip** address (the IP address requesting access).
		You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the local network.

`<foreign_ip>`	`filter http`
	`filter https`
	`filter ftp`
		IP address to which access is requested.
		You can use 0.0.0.0 (or in shortened form, 0) to specify all external destinations.

`<foreign_mask>`	`filter http`
	`filter https`
	`filter ftp`
		Network mask of the **foreign_ip** address (the IP address to which access is requested).
		Always specify a mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the external network.

Parameter	Applies to	Definition

`[allow]`	`filter http`
	`filter https`
	`filter ftp`
		Lets outbound connections pass through the security appliance without filtering when Filtering Service is unavailable.
		If you omit this option, and Filtering Service becomes unavailable, the security appliance stops all outbound HTTP, HTTPS, or FTP traffic until Filtering Service is available again.

`[cgi-truncate]`	`filter http`	Sends CGI scripts to Filtering Service as regular URLs. When a URL has a parameter list starting with a question mark (?), such as a CGI script, the URL is truncated. All characters after, and including the question mark, are removed before sending the URL to Filtering Service. (Supported in Cisco PIX v6.2 and higher.)
`[interact-block]`	`filter ftp`	Prevents users from connecting to the FTP server through an interactive FTP client. An interactive FTP client allows users to change directories without entering the complete directory path, so Filtering Service cannot tell if the user is requesting something that should be blocked.
`[longurl-truncate | longurl-deny]`	`filter http`	Specify how to handle URLs that are longer than the URL buffer size limit. • Enter **longurl-truncate** to send only the host name or IP address to Filtering Service. • Enter **longurl-deny** to deny the request without sending it to Filtering Service. (Supported in Cisco PIX v6.2 and higher.)
`[proxy-block]`	`filter http`	Enter this parameter to prevent users from connecting to an HTTP proxy server. (Supported in Cisco PIX v6.2 and higher.)

Cisco Secure ACS authentication

For the Cisco security appliance to provide user authentication information to Websense software (for transparent identification of users), Websense Filtering Service must be installed in the same domain (Windows), or root context (LDAP), as Cisco Secure ACS.

Note

Cisco Secure ACS can provide user information for one domain only. To transparently identify users in multiple domains, use a Websense transparent identification agent. See the Websense *Installation Guide* for information about installing transparent identification agents.

See the TRITON - Web Security Help for information about configuring manual authentication, or configuring transparent identification agents.

3 Configuring a Cisco IOS Router

After Websense software is installed, you must configure the Cisco IOS router to send HTTP requests to Websense software. This configuration is done through a console or telnet session. Websense software analyzes each request and tells the router whether or not to permit it.

This chapter contains the following sections:

Startup configuration

Before Websense software can filter Internet requests, the Cisco IOS router must be configured to use Filtering Service as a URL filter.

1. Access the router's software from a console, or from a remote terminal using telnet.
2. Enter your password.
3. Enter **enable** and the enable password to put the router into enabled mode.
4. Enter **configure terminal** to activate configure mode.
5. Enter the following command to identify the Filtering Service machine that will filter HTTP requests:

   ```
   ip urlfilter server vendor websense <ip-address> [port
   <port-number>] [timeout <seconds>] [retransmit <number>]
   ```

Variable	Description
`<ip-address>`	The IP address of the machine running Websense Filtering Service.
`<port-number>`	The Filtering Service port (also referred to as the integration communication port), default 15868.

Variable	Description
<seconds>	The amount of time the Cisco IOS router waits for a response from Filtering Service. The default timeout is 5 seconds.
<number>	How many times the Cisco IOS router retransmits an HTTP request when there is no response from Filtering Service. The default is 2.

An example of this command is:

```
ip urlfilter server vendor websense 12.203.9.116 timeout
8 retransmit 6
```

To define an additional Filtering Service instance as a backup, repeat the command using the IP address of the second Filtering Service machine.

The configuration settings you create in the following steps are always applied to the primary server.

Only one Filtering Service instance is used at a time—referred to as the primary server; all other instances are referred to as secondary. If the primary server becomes unavailable, one of the secondary servers is designated primary. The system goes to the beginning of the list of configured servers (i.e. Filtering Service instances) and attempts to activate the first one. If the first server is not available, the system attempts to activate the next one. This continues until an available server is found or the end of the list of configured servers is reached. If all servers are down, the router goes into allow mode.

6. Enable the logging of system messages to Filtering Service by entering the following command:

   ```
   ip urlfilter urlf-server-log
   ```

   This setting is disabled by default. When logging is enabled, the Cisco IOS router sends a log request immediately after the URL lookup request.

7. Tell the Cisco IOS router how to filter URL requests by entering the following commands, in sequence:

   ```
   ip inspect name <inspection–name> http urlfilter

   interface <type> <slot/port>

   ip inspect <inspection-name> {in|out}
   ```

   Examples of these commands are:

   ```
   ip inspect name fw_url http urlfilter

   interface FastEthernet 0/0

   ip inspect fw_url in
   ```

   For this sequence to function properly, you must create an inspection rule called *fw_url* and apply that rule to the inbound interface of the router.

   See Cisco documentation for information about creating and applying inspection rules.

To improve performance, Cisco suggests disabling the Java applet scanner. Java applet scanning increases CPU processing load. To disable the Java applet scanner, use the following commands, in sequence:

```
access-list <num> permit any
```

```
ip inspect name <inspection–name> http java-list <num>
urlfilter
```

See Cisco documentation for more information about these commands.

8. To save your changes:
   a. Enter the **exit** command twice to leave the configure mode.
   b. Enter **write memory**.

   These commands store the configuration settings in the Cisco IOS router's startup configuration so they are not lost if the router is shut down or loses power.
9. Use the following commands to view various aspects of your installations:

Command	Action
`show ip inspect name <inspection-name>`	Displays a specific inspection rule.
`show ip inspect all`	Displays all available inspection information.
`show ip urlfilter config`	Displays all URL filtering information.
`<command-name> ?`	Displays help on individual commands. For example, **ip inspect ?** displays the complete syntax for the **inspect** command, and explains each argument.

10. To discontinue filtering or to change a Filtering Service, enter the following command to remove a server configured in Step 5, page 21.

```
no ip urlfilter server vendor websense <ip-address>
```

Configuration commands

These commands are used to configure the Cisco IOS router to filter HTTP requests through Websense Filtering Service. These configuration settings can be saved into the startup configuration. See Step 8 in the preceding procedure for instructions.

Note

To turn off a feature or service, add the value **no** before the command.

```
ip inspect name <inspection-name> http urlfilter [java-list
<access-list>] [alert {on|off}] [timeout <seconds>] [audit-
trail {on|off}]
```

This global command turns on HTTP filtering. The **urlfilter** value associates URL filtering with HTTP inspection rules. You may configure two or more inspections in a router, but the URL filtering feature only works with those inspections in which the **urlfilter** field is enabled. This setup command is required.

```
ip port-map http port <num>
```

Use this command to filter proxy traffic on port <*num*> through Websense Filtering Service.

```
ip urlfilter server vendor websense <IP-address> [port
<num>] [timeout <secs>] [retrans <num>]
```

This setup command is required to identify Filtering Service to the Cisco IOS router and configure additional values. When using this command, the Cisco IOS router checks for a primary Filtering Service—one that is active and being sent URL lookup requests. If a primary server is configured, the router marks the server being added as a secondary server.

Parameter	Description
`port <num>`	The Filtering Service port (referred to as the integration communication port) you entered during Websense installation. The default port number is 15868.
`timeout <secs>`	The amount of time the Cisco IOS router waits for a response from Websense Filtering Service. The default timeout is 5 seconds.
`retrans <secs>`	How many times the router retransmits an HTTP request when there is no response from Filtering Service. The default value is 2.

```
ip urlfilter alert
```

This optional setting controls system alerts. By default, system alerts are enabled. The following messages can be displayed when alerts are enabled:

- %URLF-3-SERVER_DOWN: Connection to the URL filter server <*IP address*> is down.

  This level three LOG_ERR type message appears when a configured Filtering Service goes down. The router marks the offline server as a secondary server. It then attempts to use a defined secondary server as the primary server. If the router cannot find another Filtering Service, the URLF-3-ALLOW_MODE message is displayed.

- %URLF-3-ALLOW_MODE: Connection to all URL filter servers is down and ALLOW MODE is OFF.

  This message appears when the router cannot find a defined Filtering Service. When the **allowmode** flag is set to **off**, all HTTP requests are blocked.

- %URLF-5-SERVER_UP: Connection to a URL filter server <*IP address*> is made. The system is returning from ALLOW MODE.

  This LOG_NOTICE type message is displayed when a Filtering Service is detected as being up and the system returns from the ALLOW MODE.
- %URLF-4-URL_TO_LONG: URL too long (more than 3072 bytes), possibly a fake packet.

  This LOG_WARNING message is displayed when the URL in a GET request is too long.
- %URLF-4-MAX_REQ: The number of pending requests has exceeded the maximum limit <*num*>.

  This LOG_NOTICE message is displayed when the number of pending requests in the system exceeds the maximum limit defined. Subsequent requests are dropped.

`ip urlfilter audit-trail`

This command controls the logging of messages into the syslog server and is disabled by default. The messages logged are:

- %URLF-6-URL_ALLOWED: Access allowed for URL <*site's URL*>; client <*IP address:port number*> server <*IP address:port number*>
- This message is logged for each URL requested that is allowed by Websense software. The message includes the allowed URL, the source IP address/port number, and the destination IP address/port number. Long URLs are truncated to 300 bytes and then logged.
- %URLF-6-URL_BLOCKED: Access denied URL <*site's URL*>; client <*IP address:port number*> server <*IP address:port number*>
- This message is logged for each URL requested that is blocked by Websense software. The message includes the blocked URL, the source IP address/port number, and the destination IP address/port number. Long URLs are truncated to 300 bytes and then logged.
- %URLF-4-SITE-BLOCKED: Access denied for the site <site's URL>; client <IP address:port number> server <IP address:port number>

  This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list.

`ip urlfilter urlf-server-log`

This command is used to control the logging of system messages to Filtering Service and is disabled by default. To allow logging (and consequently reporting) of Internet activity on your system, you must enable this feature.

When logging is enabled, the Cisco IOS router sends a log request immediately after the URL lookup request. The log message contains information such as the URL, host name, source IP address, and destination IP address.

`ip urlfilter exclusive-domain {permit|deny} <domain-name>`

This optional command is used to add a domain to, or remove a domain from, the exclusive domain list. Cisco IOS router URL filtering allows you to specify a list of domain names for which the router does not send lookup requests to Websense Filtering Service.

The **permit** flag permits all traffic to <*domain-name*>. The **deny** flag blocks all traffic to <*domain-name*>.

For example, if www.yahoo.com is added to the exclusive domain list, all the HTTP traffic whose URLs are part of this domain (such as www.yahoo.com/mail/index.html, www.yahoo.com/news, and www.yahoo.com/sports) are permitted without sending a lookup request to Filtering Service.

You may also specify a partial domain name. For example, you can enter .cisco.com instead of the complete domain name. All URLs with a domain name ending with this partial name (such as www.cisco.com/products, www.cisco.com/eng, people-india.cisco.com/index.html, and directory.cisco.com) are permitted or denied without having to send a lookup request to Filtering Service. When using partial domain names, always start the name with a dot (i.e., period).

For example:

```
ip urlfilter exclusive-domain permit .sdsu.edu
```

Use the `no` form of this command (i.e., add the keyword `no` to the beginning) to undo permitting or blocking of a domain name. The permitting or blocking of a domain name stays in effect until the domain name is removed from the exclusive list. Using the `no` form of this command removes the specified domain name from the exclusive list. For example, to stop the automatic permitting of traffic (and send lookup requests to Filtering Service) to www.sample.com:

```
no ip urlfilter exclusive-domain permit www.sample.com
```

As another example, to stop the automatic blocking of traffic to the same domain name:

```
no ip urlfilter exclusive-domain deny www.sample.com
```

`ip urlfilter allowmode {on|off}`

This command controls the default filtering policy if Filtering Service is down. If the **allowmode** flag is set to **on**, and the Cisco IOS router cannot find a Filtering Service, all HTTP requests are permitted.

If **allowmode** is set to **off**, all HTTP requests are blocked when Filtering Service becomes unavailable. The default for **allowmode** is **off**.

`ip urlfilter max-resp-pak <number>`

Use this optional command to configure the maximum number of HTTP responses that the Cisco IOS router can store in its packet buffer.

The default value is 200 (this is also the maximum you can specify).

`ip urlfilter max-request <number>`

Use this optional command to set the maximum number of outstanding requests that can exist at a given time. When this number is exceeded, subsequent requests are dropped. The **allowmode** flag is not considered in this case because it is only used when Filtering Service is down.

The default value is 1000.

Executable commands

These Cisco IOS router commands allow you to view configuration data and filtering information. These settings cannot be saved into the startup configuration.

`show ip urlfilter config`

This command shows configuration information, such as number of maximum requests, **allowmode** state, and the list of configured Filtering Services.

Technical Support typically requests this information when trying to solve a problem.

`show ip urlfilter statistics`

This command shows statistics of the URL filtering feature, including:

- Number of requests sent to Filtering Service
- Number of responses received from Filtering Service
- Number of requests pending in the system
- Number of requests failed
- Number of URLs blocked

`debug ip urlfilter {function-trace/detailed/events}`

This command enables the display of debugging information from the URL filter system.

Parameter	Description
`function-trace`	Enables the system to print a sequence of important functions that get called in this feature.
`detailed`	Enables the system to print detailed information about various activities that occur in this feature.
`events`	Enables the system to print various events, such as queue events, timer events, and socket events.

4 Configuring a Cisco Content Engine

After Websense software is installed, you must activate it within the Cisco Content Engine. This configuration is done through the Cisco Web-based interface, or through a console or Telnet session.

> **Note**
> If load bypass or authentication bypass is enabled in the Content Engine, Internet requests that are rerouted are filtered by Websense software. See your Content Engine documentation for more information.

This chapter contains the following sections:

Cisco Web-based interface

1. Open a Web browser and connect to the Cisco Content Engine at:
   - **https://<IP address>:8003** (secure connection)
   - **http://<IP address>:8001** (non-secure connection)

   Here, <*IP address*> is the IP address of the Content Engine machine.

By default, ACNS is configured for secured access to the Content Engine GUI (i.e., HTTPS on port 8003).

> **Note**
> The Content Engine GUI may be configured for either secured or non-secured access, but not both. For example, if the Content Engine GUI is configured for secured access, non-secured connections (i.e., HTTP on port 8001) are not allowed.

2. The **Enter Network Password** dialog box appears. Enter a user name and password to access the initial management page.
3. Select **Caching > URL Filtering**.
4. Select the filtering option appropriate to your ACNS version.
   - For ACNS versions 5.5 and 5.6, select **Websense Filtering (Remote)**.
   - For ACNS version 5.4, select either **Websense Filtering (Remote)** or **Websense Filtering (Local)**.
5. Enter the following information in the appropriate fields:

Field	Description
Websense Filtering Service *or* Websense Server	The host name or IP address of the machine running Filtering Service.
Port	The Filtering Service port (also referred to as the integration communication port) you entered during installation for Websense software. The default is 15868.
Timeout	The amount of time (between 1 and 120 seconds) that the Content Engine waits for a response from Filtering Service before permitting a site. The default is 20.
Allowmode	When allowmode is enabled, the Content Engine allows HTTP traffic if Filtering Services does not respond. When allowmode is disabled, the Content Engine blocks all HTTP traffic that is served through it if Filtering Service does not respond.
Connections	The number of persistent connections (1-250) per CPU. Use this option to configure the number of persistent connections to Filtering Service. The default is 40. Do not change from the default value unless you know for certain that a different value is required.

6. If Websense software is filtering on a cluster of Content Engines, configure each Content Engine as described in steps 1-5.

For more information on using the Web-based interface, see Cisco documentation, available at www.cisco.com.

Console or telnet session

If you cannot access the Web-based interface, or prefer to use the command-line interface, use the procedure below to configure the Cisco Content Engine.

1. Access the Cisco Content Engine from a console or from a remote terminal using telnet for access.
2. Enter the global configuration mode with the **configure** command.

   You must be in global configuration mode to enter global configuration commands.

   ```
   Console# configure
   Console(config)#
   ```

3. To enable Websense URL filtering, use the **url-filter** global configuration command.

   ```
   url-filter http websense server {<ip-address>} [port
   <port-number>] [timeout <seconds>] [connections <number-
   of-connections>]
   ```

Variable	Description
`<ip-address>`	The host name or IP address of the machine running Filtering Service.
`<port-number>`	The Filtering Service port you entered during the installation of Websense software. The default is 15868.
`<seconds>`	The amount of time (0-240) in seconds that the Content Engine waits for a response from Filtering Service. The default is 20.
`<number-of-connections>`	The number of persistent connections (1-250) per CPU. Use this option to configure the number of persistent connections to Filtering Service. The default is 40. Do not change from the default value unless you know for certain that a different value is required.

4. Use the **url-filter http websense allowmode enable** command to configure the Content Engine to permit requests after a Websense Filtering Service timeout.
5. Use the **url-filter http websense enable** command to enable Websense software as the current URL filtering scheme for HTTP.
6. To save your changes:
   a. Enter the **exit** command to leave **configure** mode.

b. Enter **write memory**.

7. If Websense software is filtering on a cluster of Content Engines, configure each Content Engine as described in steps 1-6.

Websense software is ready to filter Internet requests after the Websense Master Database is downloaded and the software is activated within the Cisco Content Engine.

See the TRITON - Web Security Help for information about configuring Websense software and downloading the Master Database.

Verifying configuration

Use the following console commands to view current configuration information.

`show url-filter http`

Displays the currently enabled filtering scheme for HTTP traffic and also configuration information about Websense Filtering Service (e.g., IP address and integration communication port).

`show statistics url-filter http websense`

Displays request-reply statistics about the communication between the Content Engine and Websense Filtering Service. Included are number of requests sent, replies received, pages blocked, pages allowed, and failure cases.

Configuring firewalls or routers

To prevent users from circumventing Websense filtering, your firewall or Internet router should be configured to allow outbound HTTP, HTTPS, and FTP requests only from the Cisco Content Engine.

The Content Engine and Websense software transparently handle Internet requests sent from routers using Web Cache Communication Protocol (WCCP).

Network Agent cannot perform protocol filtering on traffic encapsulated with WCCP.

Note

For Internet connectivity, Filtering Service may require authentication through a proxy server or firewall for HTTP traffic. To allow downloads of the Websense Master Database, configure the proxy or firewall to accept clear text or basic authentication.

See the proxy or firewall documentation for configuration instructions.

See the TRITON - Web Security Help for instructions on running the Websense Master Database download.

Browser access to the Internet

Cisco Content Engine can regulate Internet activity either transparently or explicitly. In transparent mode, the firewall or Internet router is configured to send Internet requests to the Cisco Content Engine, which queries Filtering Service. All configuration changes can be performed through the Content Engine and any connected firewalls or routers, with no special configuration required on client computers. To run transparently, you must enable WCCP on both the Content Engine and the firewall or router.

When regulating Internet activity explicitly, Web browsers on all client computers are configured to send Internet requests to the Content Engine. See Cisco Content Engine documentation for instructions.

To prevent users from circumventing Websense filtering, your firewall or Internet router should be configured to allow outbound HTTP and FTP requests only from the Cisco Content Engine.

To set up promptless, browser authentication for NTLM or LDAP, refer to Cisco documentation.

Clusters

If you have several Content Engines running in a cluster, you must configure each Content Engine to use Filtering Service as an HTTP, HTTPS, and FTP filter. Several Content Engines can use the same Filtering Service. See Cisco Content Engine documentation for details on setting up a cluster.

A Troubleshooting

I upgraded my Cisco PIX Firewall software to version 7.0, and Web filtering stopped working

In version 7.0(1) of the Cisco PIX Firewall software, the **url-server** command was changed to increase the minimum value for the timeout parameter to **10** seconds.

In previous versions, the minimum value for this parameter was 1 second, and the default value was 5 seconds.

If the timeout was set to a value less than 10 seconds, the **url-server** command was deleted when you upgraded your software.

To resolve this issue, re-enter the **url-server** command.

See Cisco documentation for more information.

Index

S

T

U

W