websense®

Installation Guide Supplement

for use with

Integrated Cisco Products

Websense® Web Security
Websense Web Filter

v7

Installation Guide Supplement for Integrated Cisco Products

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

Published 2008
Printed in the United States of America and Ireland.

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, Windows Vista and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Sun, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Novell Directory Services is a registered trademark of, and eDirectory is a trademark of, Novell, Inc., in the United States and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (http://www.apache.org).
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

WinPcap

Contents

1 Cisco Integration

This supplement provides additional information for installing and setting up an integration of Websense® Web Security™ or Websense Web Filter™ with Cisco® Adaptive Security Appliance (ASA), Cisco PIX® Firewall, Cisco IOS routers, and Cisco Content Engine.

See the *Websense Web Security and Websense Web Filter Installation Guide* for basic instructions.

When Websense software is integrated with a Cisco product, some differences exist in the installation and configuration, as compared to the Stand-Alone Edition:

- **Filtering Service**: The integrated Cisco product and Network Agent work with Filtering Service to filter Internet requests.
- **Network Agent**: Manages Internet protocols that are not managed by your integrated Cisco product. It can also detect HTTP network activity and instruct the Filtering Service to log this information.

  If Network Agent is installed, you must define the IP addresses of all proxy servers through which computers route their Internet requests. See the Network Configuration topic in the Websense Manager help system for instructions.
- **Configure your Cisco integration**: You must direct Internet requests through your Cisco integration product, and configure it for use with Websense software.
  - See *Chapter 2: Configuring a Cisco Security Appliance* for instructions on configuring Cisco PIX Firewall or Adaptive Security Appliance (ASA).
  - See *Chapter 3: Configuring a Cisco IOS Router* for instructions on configuring a Cisco IOS router.
  - See *Chapter 4: Configuring a Cisco Content Engine* for instructions on configuring a 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 DC Agent and manual authentication, this configuration is not necessary.

How Websense filtering works with Cisco

To be filtered by Websense software, a client must access the Internet through the Cisco product.

- If Websense software is integrated with a Cisco PIX Firewall or ASA, client browsers must be set to use the PIX Firewall or ASA as the default gateway.
- If Websense software is integrated with a Cisco IOS router or Cisco Content Engine, client browsers must be set for proxy-based connections.

When it receives an Internet request, the Cisco product queries Filtering Service to find out if the requested 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 see the site.

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:

- **`Boldface`** indicates commands and keywords that are entered as shown.
- Angle brackets (< >) containing text in *italics* 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

Refer the Chapter 3 of the Websense *Installation Guide* for complete instructions on downloading and installing the program.

When running the installer, select the following options:

- After you select **Integrated** in the Integration Options window, a list of integrations is displayed.
- Select either **Cisco Adaptive Security Appliances**, **Cisco Content Engine**, **Cisco PIX Firewall**, or **Cisco Routers**, as appropriate for your environment, and click **Next**.
- When prompted to select **Transparent User Identification**, select **None** if you plan to configure authentication of users through your Cisco product.
- Follow the onscreen prompts to complete the installation.

See the following chapters of this supplement to configure your Cisco product to work with Websense software.

Upgrade

If Websense software is integrated with a Cisco security appliance (PIX Firewall or ASA), the following configuration updates are recommended:

- Increase the size of the security appliance's internal buffer to handle long URL strings.
- Set the URL response block buffer to prevent the Web server replies from being dropped in high traffic situations.
- If you are upgrading your Websense system and changing your integration product, see *Migrating between integrations after installation*, page 7.

See the following chapters for configuration instructions.

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 any configuration data.

1. Install and configure your new Cisco integration product. See your 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 Websense Manager Help for instructions

3. Close all applications on the Filtering Service machine, and stop any anti-virus software.
4. Remove the Filtering Service using the procedures for removing components in the *Installation Guide*.
5. Restart the machine (Windows only).
6. Run the Websense installer.
7. Add the Filtering Service using the procedures for adding individual components in the *Installation Guide*.
8. When prompted to select an integration, select the new Cisco product.
9. Follow the onscreen instructions to complete the installation.

   The installer adds the new integration data to the `config.xml` file, while preserving the previous configuration data.
10. Restart the machine (Windows only).
11. Check to be sure that the Filtering Service has started.
    - In Windows:
      - Open the Services dialog box.
      - Check that **Websense Filtering Service** is started.
    - In Linux:
      - Open a command prompt.
      - Change directories to `opt/Websense/bin`.
      - Run `./WebsenseAdmin status`
      - Check that **Websense Filtering Service** is running.

    For instructions on starting Websense services, see the *Installation Guide*.
12. Open Websense Manager 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 Websense Manager.

    For more information, see the discussion of configuring local settings in the Network Configuration section of Websense Manager Help.
13. If you stopped your anti-virus 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 Websense software, which analyzes the request and determines whether to block or permit access, or limit access by using quotas set in Websense policies.

See Websense Manager Help for instructions on setting policies.

This chapter contains instructions for configuring the Websense integration with Cisco PIX Firewall or Adaptive Security Appliance (ASA).

✓ **Note**
Both the Cisco PIX Firewall and ASA are referred to as the *security appliance* in this chapter.

After Websense software is installed, you must configure the Cisco security appliance to send Internet requests to the software. This chapter describes how to configure the security appliance 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.

Configuration procedure

Use the following 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 Privilege 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 of the options.

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

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

The elements of the `url-server` command are defined as follows:

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.
`<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 5 seconds in earlier versions. • v7.0(1): 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 setting, and is also the default setting if a protocol is not specified. The recommended protocol version is **`4`**, If the version is not specified, the setting defaults to 1.

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.

An example of the `url-server` command might be:

```
url-server (perimeter) host 10.255.40.164 timeout 30
protocol TCP version 4
```

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 url-server**.
   - To review all the filter rules, enter **show filter**.
   - If you are running v7.0 of the Cisco product, enter **exit** to go up a level to run the `show` command.

   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]
   ```

   The elements of the `filter url` command are defined as follows:

Parameter	Definition
http *<port>[-<port>]*	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 v5.2 and later of the Cisco software. **NOTE**: In Cisco software versions 5.2 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`.

Parameter	Definition
<local_ip>	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>	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>	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>	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.
[**allow**]	Enter this parameter to let 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 traffic until Filtering Service is available again.
[**cgi-truncate**]	Enter this parameter to send 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.)
[**longurl-truncate** | **longurl-deny**]	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**]	Enter this parameter to prevent users from connecting to an HTTP proxy server. (Supported in Cisco PIX v6.2 and higher.)

Multiple `filter url` commands may be entered to achieve your filtering goals.

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, Class B 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 Websense Manager to apply filtering policies to individual clients (users, groups, domains/ organizational units, computers, or networks).

See Websense Manager Help for instructions on setting policies.

7. Configure the security appliance to filter HTTPS requests with the `filter https` command.

   - To review the current URL server rules, enter **`show url-server`**.
   - To review all the filter rules, enter **`show filter`**.
   - If you are running v7.0 of the Cisco product, 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]
```

The elements of the `filter https` command are defined as follows:

Parameter	Definition
<port>	Defines which port number the security appliance watches for HTTPS requests. You can either enter the standard HTTPS port, `443`, or a custom port number.
<local_ip>	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>	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>	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>	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.
[**allow**]	Enter this parameter to let 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 outbound HTTPS traffic until Filtering Service is available again.

Multiple `filter https` commands may be entered to achieve your filtering goals.

Command example	Action
filter https 443 0 0 0 0	Filters every HTTPS request 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 Class B 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 Websense Manager to apply filtering policies to individual clients (users, groups, domains/ organizational units, computers, or networks).

See Websense Manager Help for instructions on setting 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 url-server`**.
    - To review all the filter rules, enter **`show filter`**.
    - If you are running v7.0 of the Cisco product, 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]
```

The elements of the `filter ftp` command are defined as follows:

Parameter	Definition
<port>	Defines which port number the security appliance watches for FTP requests. You can either enter the standard FTP port number, **`21`**, or a custom port number.
<local_ip>	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>	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>	IP address to which access is requested. You can use `0.0.0.0` (or in shortened form, `0`) to specify all external destinations.

Parameter	Definition
<foreign_mask>	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.
[**allow**]	Enter this parameter to let 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 outbound FTP traffic until Filtering Service is available again.
[**interact-block**]	Enter this parameter to prevent 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.

Multiple `filter ftp` commands may be entered to achieve your filtering goals.

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, Class B 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 Websense Manager to apply filtering policies to individual clients (users, groups, domains/ organizational units, computers, or networks).

See Websense Manager Help for information on setting up 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, if 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 enter:

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

to allow any outbound HTTP traffic from the IP address 10.1.1.1 to go out 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>
   ```

   where <*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>
   ```

   where <*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>
```

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

- Enter `show url-block` to view the current configuration for all three `url-block` commands.
- Enter `show url-block block statistics` to view statistics that show 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

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

    was entered to enable filtering, then to disable filtering, enter:

    ```
    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`**
    - **`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 Websense Manager Help for information about configuring Websense software and downloading the Master Database.

Cisco Secure ACS authentication

Important

Do not use Cisco Secure ACS authentication with Websense filtering in a multiple domain environment. ACS cannot provide domain information about users to Websense software, and authentication fails.

To identify users in a multiple domain environment, use a Websense transparent identification agent, such as DC Agent, or use Websense manual authentication.

See Chapter 3 of the Websense *Installation Guide* for information about installing transparent identification agents.

See Websense Manager 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 the Websense software. This configuration is done through a console or telnet session.

Websense software analyzes the request and tells the router whether or not to permit it. The action taken is cached in the router. The router enforces the same policy the next time the site is requested, without communicating with Filtering Service.

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 you entered during the Websense installation. The default is 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 as a backup, repeat the command for the IP address of the second server.

The configuration settings you create in the following steps are always applied to the primary server, which is identified as the first server with which the Cisco IOS router can establish communications.

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

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

   This setting is enabled by default. When logging is enabled, the Cisco IOS router sends a log request immediately after the URL lookup request. If the destination IP address is found in the cache, Cisco IOS router does not send a URL lookup request but still sends a log request to Filtering Service.

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 entitled *fw_url* and apply that rule to the inbound interface of the router.

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

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

This setup command is required to identify Websense 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 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-SITE_ALLOWED: Client <*`IP-address:port-number`*> accessed server <*`IP-address:port-number`*>.

  This LOG_INFO message is logged for each request whose destination IP address is found in the cache. This message includes source IP address/port number and destination IP address/port number.
- %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 (>1000 bytes) are not 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 (>1000 bytes) are not logged.

`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. If the destination IP address is found in the cache, the router does not send a URL lookup request but does send a log request to Filtering Service. The log message contains information such as the URL, host name, source IP address, and destination IP address.

`ip urlfilter exclusive-domain` *`<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 need not send lookup requests to Filtering Service.

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. In this example, all URLs with domain name that ends 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 without having to send a lookup request to Filtering Service. When using partial domain names, always start the name with a period.

For example: `ip urlfilter exclv-domain .sdsu.edu`

`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 packet-buffer` *<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.

`ip urlfilter maxrequest` *<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, and to control caching. 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.

Cisco Web-based interface

1. Open a Web browser and connect to the Cisco Content Engine at:
   - **`https://`***`<ip-address>`***`:8003`** (for ACNS 5.1 and higher)
   - **`http://`***`<ip-address>`***`:8001`** (for versions prior to ACNS 5.1)

   where *`<ip-address>`* is the IP address of the Content Engine machine.

   The default port is 8003 for ACNS 5.1 and higher.

   The Enter Network Password dialog box appears.
2. 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 you entered during the Websense installation. 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 60.

6. If Websense software is filtering on a cluster of Content Engines, configure each Content Engine with the following commands to ensure that all traffic is filtered:

   ```
   url-filter http websense server <ip-address> port <port-number>
   url-filter http websense allowmode enable
   ```

   For Websense software installed on the Content Engine, use the following command:

   ```
   url-filter http websense “local”
   ```

For more information on using the Web-based interface, see the 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>
```

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 Websense installation. The default is 15868.
<seconds>	The amount of time (between 1 and 120 seconds) that the Content Engine waits for a response from Filtering Service. The default is 60.

4. The **`url-filter http websense allowmode enable`** command configures the Content Engine to permit requests after a Websense Filtering Service timeout.
5. To save your changes:
   a. Enter the **`exit`** command to leave the `configure` mode.
   b. Enter **`write memory`**.
6. If the Websense software is filtering on a cluster of Content Engines, configure each Content Engine with the following commands to ensure that all traffic is filtered:

   ```
   url-filter http websense server <ip-address> port <port-number>
   url-filter http websense allowmode enable
   ```

   For Websense software installed on the Content Engine, use the following command:

   ```
   url-filter http websense “local”
   ```

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 Websense Manager Help for information about configuring Websense software and downloading the Master Database.

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 the Websense software transparently handle Internet requests sent from routers with 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 Websense Manager 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 non-transparently. 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 non-transparently, Web browsers on all client computers are configured to send Internet requests to the Content Engine. See your 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 your 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 your Cisco Content Engine documentation for details on setting up a cluster.

A Troubleshooting

I upgraded my Cisco PIX Firewallsoftware 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, simply re-enter the **`url-server`** command.

See the Cisco documentation for more information.

Index