



# Filtering HTTP, HTTPS, or FTP Requests Using an External Server

This section tells how to enable HTTP, HTTPS, or FTP filtering for inside users, and contains the following topics:

- [Filtering Overview, page 14-1](#)
- [Configuring General Filtering Parameters, page 14-2](#)
- [Filtering HTTP URLs, page 14-5](#)
- [Filtering HTTPS URLs, page 14-6](#)
- [Filtering FTP Requests, page 14-6](#)
- [Viewing Filtering Statistics, page 14-6](#)

## Filtering Overview

Although you can use ACLs to prevent outbound access to specific websites or FTP servers, configuring and managing web usage this way is not practical because of the size and dynamic nature of the Internet. We recommend that you use the Firewall Services Module (FWSM) in conjunction with a separate server running one of the following Internet filtering products:

- Websense Enterprise—<http://www.websense.com>. Supports HTTP, HTTPS, and FTP filtering.
- Sentian by N2H2—<http://www.n2h2.com>. Supports HTTP filtering. Although some versions of Sentian support HTTPS, the FWSM only supports HTTP with Sentian.

Because URL filtering is handled on a separate platform, the performance of the FWSM is less affected. However, filtering can considerably increase access times to websites or FTP servers when the filtering server is remote from the FWSM.

When a user issues an HTTP, HTTPS, or FTP GET request, the FWSM sends the request to the web/FTP server as well as to the filtering server at the same time. If the filtering server permits the connection for the user, then the following action occurs for each request type:

- For HTTP, the FWSM allows the reply from the web server to reach the user who issued the original request.
- For HTTPS, the FWSM allows the completion of SSL connection negotiation, and allows the reply from the web server to reach the user who issued the original request.
- For FTP, the FWSM allows the successful FTP return code to reach the user unchanged. For example, a successful return code is “250: CWD command successful.”

If the filtering server denies the connection, then the following action occurs for each request type:

- For HTTP, the FWSM redirects the user to a block page, indicating that access was denied.
- For HTTPS, the FWSM prevents the completion of SSL connection negotiation. The browser displays an error message such as “The Page or the content cannot be displayed.”
- For FTP, the FWSM alters the FTP return code to show that the connection was denied. For example, the FWSM changes code 250 to “code 550: Directory not found.”

For N2H2, if you enabled user authentication on the FWSM for HTTP, HTTPS, or FTP, then the FWSM also sends the username to the filtering server. The filtering server can then use user-specific filtering settings or provide enhanced reporting per user. See the “[Configuring Authentication for Network Access](#)” section on page 12-20 to configure user authentication. Websense supports filtering by IP address only.

Filtering applies only for outbound connections (from a higher security interface to a lower security interface) or between same security interfaces.

## Configuring General Filtering Parameters

This section describes how to configure the FWSM to communicate with the filtering server and how to handle requests when the filtering server is down, how to handle long URLs, and whether to cache server addresses. This section includes the following topics:

- [Identifying the Filtering Server](#), page 14-2
- [Buffering Replies](#), page 14-3
- [Setting the Maximum Length of Long HTTP URLs](#), page 14-4
- [Caching URL Servers](#), page 14-4

## Identifying the Filtering Server

You can identify up to four filtering servers per context. The FWSM uses the servers in order until a server responds. You can only configure one type of server (Websense or N2H2) in your configuration.



### Note

You must add the filtering server before you can configure filtering for HTTP or HTTPS with the **filter** command. If you remove the filtering servers from the configuration, then all **filter** commands are also removed.

To identify the filtering server(s), enter one of the following commands for each server you want to identify. Only one type of server is allowed in your configuration.

- To identify a Websense Enterprise server, enter the following command:

```
FWSM/contexta(config)# url-server (if_name) vendor websense host ip_address
[timeout seconds] [protocol tcp [version {1 | 4}] | udp]
```

See the following options:

- *(if\_name)*—The interface through which the FWSM communicates with the server.
- *ip\_address*—The Websense server IP address.

- **timeout seconds**—The number of seconds between 10 and 120 before the FWSM stops trying to connect to the server, and attempts to connect to the next server in the list (if available). The default is 30 seconds.
  - **protocol tcp [version {1 | 4}]**—Specifies that communication between the FWSM and the Websense server uses TCP, which is the default protocol. We recommend version 4, although version 1 is the default. Version 4 allows the FWSM to send authenticated usernames to the Websense server and to support URL caching.
  - **protocol udp**—Specifies UDP, which has greater throughput, but which does not support long URLs.
- To identify an N2H2 Sentian server, enter the following command:

```
FWSM/contexta(config)# url-server (if_name) vendor n2h2 host ip_address [port number]
[timeout <seconds>] [protocol {tcp | udp}]
```

See the following options:

- (*if\_name*)—The interface through which the FWSM communicates with the server.
- *ip\_address*—The N2H2 server IP address.
- **port number**—The port used to communicate with the N2H2 server. The default is 4005 for TCP or UDP. Change this value if you change the port on the N2H2 server.
- **timeout seconds**—The number of seconds between 10 and 120 before the FWSM stops trying to connect to the server, and attempts to connect to the next server in the list (if available). The default is 30 seconds.
- **protocol {tcp | udp}**—Specifies the protocol used for communication between the FWSM and the N2H2 server. TCP is the default protocol, and is recommended.

For example, to identify redundant Sentian servers, enter:

```
FWSM/contexta(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
FWSM/contexta(config)# url-server (perimeter) vendor n2h2 host 10.0.1.2
```

## Buffering Replies

By default, when a user issues a request to connect to a website or FTP server, the FWSM sends the request to the web/FTP server and to the filtering server at the same time. If the filtering server does not respond before the web/FTP server, the reply from the web/FTP server is dropped.

To avoid dropping traffic, you can configure the FWSM to buffer replies from web and FTP servers. When the filtering server eventually responds, the FWSM can allow the connection.

---

To enable buffering, enter the following command:

```
FWSM/contexta(config)# url-block block block-buffer-limit
```

The *block-buffer-limit* sets the amount of memory assigned to the buffer from 0 to 128 blocks. Each block is 1550 bytes.

---

## Setting the Maximum Length of Long HTTP URLs

### Websense only

By default, the FWSM considers an HTTP URL to be a long URL if it is greater than 1159 characters. If the URL exceeds the maximum size, then it is dropped by default. You can set the FWSM to truncate or block a long URL when you configure HTTP filtering. (See the “[Filtering HTTP URLs](#)” section on page 14-5.)

To increase the maximum length and to set the amount of memory used for long URLs, follow these steps:

---

**Step 1** To change the limit for long URLs from 1159 bytes (characters), enter the following command:

```
FWSM/contexta(config)# url-block url-size long-url-size
```

Enter **2**, **3**, or **4** to change the limit to 2, 3, or 4 KB.

**Step 2** To set the maximum memory available for buffering long URLs, enter the following command:

```
FWSM/contexta(config)# url-block url-mempool memory-pool-size
```

The amount of memory dedicated to long URLs is limited to avoid a DoS attack, for example.

Set the size from 2 to 10240 KB. Typically, the amount of memory should be the number of sessions you want to allow times the maximum length of the URL. For example, to allow 100 sessions for 3 KB URLs, then set the memory to be 300 KB. However, we recommend setting the memory to the maximum, 10240 KB, because the FWSM has enough memory to handle the maximum number of sessions.

---

## Caching URL Servers

After a user accesses a site, the filtering server can allow the FWSM to cache the server address for a certain amount of time, as long as every site hosted at the address is in a category that is permitted at all times. Then, when the user accesses the server again, or if another user accesses the server, the FWSM does not need to consult the filtering server again.



### Note

---

Requests for cached IP addresses are not passed to the filtering server and are not logged. As a result, this activity does not appear in any reports.

---

To enable caching, enter the following command:

```
FWSM/contexta(config)# url-cache {dst | src_dst} kbytes
```

See the following options:

- **dst**—Caches the destination server address for any user that accesses the server.
  - **src\_dst**—Caches the source and destination server address, so access is only cached for a given user at the source address.
  - **kbytes**—The cache size between 1 and 128 KB.
-

## Filtering HTTP URLs

To filter HTTP web access for specified users, or to exempt some traffic from filtering, enter the following commands:

- To identify HTTP traffic to be filtered by a filtering server, enter the following command:

```
FWSM/contexta(config)# filter url [http | port[-port]] source_ip source_mask dest_ip
dest_mask [allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]
```

See the following options:

- **http** | *port[-port]*—The port to which the HTTP request is sent. **http** specifies port 80, which is commonly used, but you can specify other ports.
  - *source\_ip source\_mask*—The source address and mask. Specify **0 0** for all addresses. These addresses are the local, untranslated addresses. When you configure the filtering server, use these local addresses and not the translated addresses.
  - *dest\_ip dest\_mask*—The destination server address and mask. Specify **0 0** for all addresses. You typically specify all addresses and allow the filtering server to determine the websites that are allowed.
  - **allow**—When the filtering server is unavailable, this option allows connections to pass without filtering. Without this option, the FWSM stops HTTP traffic until the filtering server is back online.
  - **proxy-block**—Prevents users from connecting to an HTTP proxy server.
  - **longurl-truncate** | **longurl-deny**—By default, if a URL is longer than the maximum length then the FWSM drops the packet. (The default maximum length is 1159 bytes, but can be made larger for Websense. See the [“Setting the Maximum Length of Long HTTP URLs”](#) section on page 14-4). If you specify the **longurl-truncate** option, the FWSM sends the host name or IP address portion of the URL for evaluation to the filtering server. The **longurl-deny** option denies the URL, and forwards the user to the block page.
  - **cgi-truncate**—Truncates CGI URLs to include only the CGI script location and the script name (but not parameters). Many long HTTP requests are CGI requests. If the parameters list is very long, waiting and sending the complete CGI request including the parameter list can waste memory resources and impact performance.
- To exempt traffic from being filtered, enter the following command:

```
FWSM/contexta(config)# filter url except source_ip source_mask dest_ip dest_mask
```

For example, to filter all HTTP requests from the 10.1.1.0 network to any web server, but to exempt an administrator user (10.1.1.1) from filtering, enter the following commands:

```
FWSM/contexta(config)# filter url except 10.1.1.1 255.255.255.255 0 0
FWSM/contexta(config)# filter url http 10.1.1.0 255.255.255.0 0 0 longurl-truncate
cgi-truncate
```

To filter users only on the 10.1.2.0 network, enter the following commands:

```
FWSM/contexta(config)# filter url http 10.1.2.0 255.255.255.0 0 0
```

## Filtering HTTPS URLs

### Websense only

---

To filter HTTPS web access for specified users, enter the following command:

```
FWSM/contexta(config)# filter https source_ip source_mask dest_ip dest_mask [allow]
```

HTTPS content is encrypted, so the FWSM sends the URL lookup to the filtering server without directory and filename information.

For the source addresses, specify the local, untranslated addresses. When you configure the filtering server, use these local addresses and not the translated addresses.

When the filtering server is unavailable, the **allow** keyword allows connections to pass without filtering. Without this option, the FWSM stops HTTPS traffic until the filtering server is back online.

---

## Filtering FTP Requests

### Websense only

---

To enable FTP filtering, enter the following command:

```
FWSM/contexta(config)# filter ftp port source_ip source_mask dest_ip dest_mask [allow]  
[interact-block]
```

Websense only filters FTP GET commands and not PUT commands.

For the source addresses, specify the local, untranslated addresses. When you configure the filtering server, use these local addresses and not the translated addresses.

When the filtering server is unavailable, use the **allow** keyword allows connections to pass without filtering. Without this option, the FWSM stops FTP traffic until the filtering server is back online.

The **interactive-block** keyword prevents interactive FTP sessions that do not provide the entire directory path. An interactive FTP client is a non-browser client such as the **ftp** command from a DOS prompt or a UNIX shell prompt, or a stand alone FTP client. For example, when you use a web browser for FTP and you browse to a file, the URL for the file includes the entire path. When you use the **ftp** command at the command line, you can change directories without typing the entire path (**cd ./files** instead of **cd /public/files**), in which case the firewall cannot determine your exact location.

---

## Viewing Filtering Statistics

This section describes how to monitor filtering statistics, and includes the following topics:

- [Viewing Filtering Server Statistics, page 14-7](#)
- [Viewing Caching Statistics, page 14-7](#)
- [Viewing Filtering Performance Statistics, page 14-8](#)

## Viewing Filtering Server Statistics

To show information about the filtering server or to show statistics, enter the following command:

```
FWSM/contexta# show url-server stats
```

The following sample display shows filtering statistics:

```
FWSM/contexta# show url-server stats
URL Server Statistics:
-----
Vendor                               websense
URLs total/allowed/denied            50/35/15
HTTPSs total/allowed/denied          1/1/0
FTPs total/allowed/denied             3/1/2

URL Server Status:
-----
10.130.28.18                          UP

URL Packets Sent and Received Stats:
-----
Message          Sent      Received
STATUS_REQUEST   65155    34773
LOOKUP_REQUEST   0         0
LOG_REQUEST       0         NA
-----
```

## Viewing Caching Statistics

To show URL caching statistics, enter the following command:

```
FWSM/contexta# show url-cache stats
```

The following sample display shows how the cache is used:

```
FWSM/contexta# show url-cache stats
URL Filter Cache Stats
-----
Size :      128KB
Entries :   1724
In Use :    456
Lookups :   45
Hits :      8
```

## Viewing Filtering Performance Statistics

To show URL filtering performance statistics (as well as other performance statistics), enter the following command:

```
FWSM/contexta# show perfmon
```

The following sample display shows filtering statistics in the URL Access and URL Server Req rows:

```
FWSM/contexta# show perfmon
PERFMON STATS:      Current      Average
Xlates              0/s        0/s
Connections         0/s        2/s
TCP Conns           0/s        2/s
UDP Conns           0/s        0/s
URL Access          0/s        2/s
URL Server Req     0/s        3/s
TCP Fixup           0/s        0/s
TCPIntercept       0/s        0/s
HTTP Fixup          0/s        3/s
FTP Fixup           0/s        0/s
AAA Authen          0/s        0/s
AAA Author          0/s        0/s
AAA Account         0/s        0/s
```