61202880L1-29.2D
July 2008

Configuration Guide

URL Filtering/Top Websites Reporting

This configuration guide describes the unified resource locator (URL) filtering and the top website reporting features on ADTRAN Operating System (AOS) products without the use of a separate URL filtering server. The non-server URL filtering feature permits or denies specified URLs. The top website reporting feature allows system administratorss to view the most frequently requested websites on their system. This guide includes an overview of the URL filtering and top websites features, the configuration process, and a troubleshooting section including the **show** and **debug** commands.

This guide consists of the following sections:

URL Filtering Overview

URL filtering provides a method for businesses to restrict Internet access within their companies. As the Internet becomes more and more prevalent in company procedures, companies run greater risk of productivity loss, misuse of company resources, compromised security, and even legal liabilities. URL filtering allows system administrators to restrict Internet access by permitting or denying specified URLs.

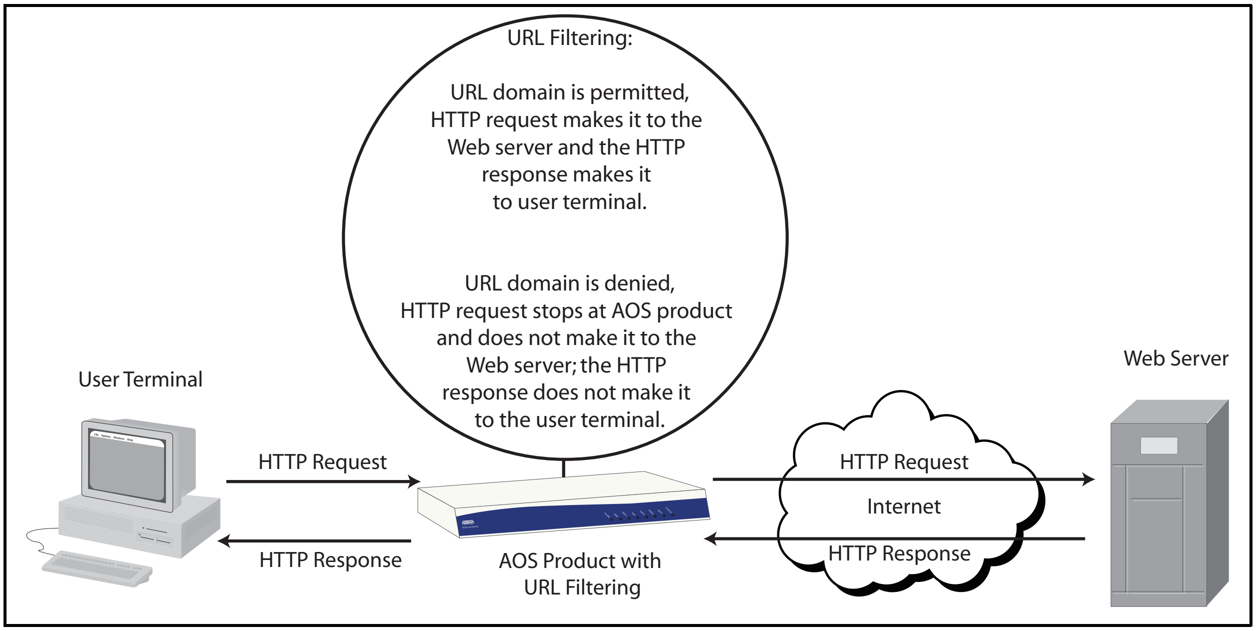
The ability to filter Web content based on a URL is integrated into the AOS firewall. AOS is capable of providing small- to medium-sized businesses with a simple URL filtering package without the use of an external server. This functionality saves time, money, and network resources while still providing Internet access control, added security, and a method of monitoring the most requested websites.

URL filtering works by blocking or allowing website URLs that have been determined by the system administrator as content to deny, or content to permit. Because these URLs have been previously specified as permit or deny, there is no need for an external server (such as Websense) to filter the Web content.

The AOS URL filtering feature also includes the ability for top websites reporting. This function produces reports of the most frequently requested websites in 15-minute increments, allowing system administrators to view the Internet habits of employees and make decisions about how to upgrade URL filter lists.

URL Filtering and Top Websites Reporting Processes

URL filtering checks Hypertext Transfer Protocol (HTTP) requests against an administrator-configured list of URLs that are permitted or denied on the network. As detailed in the illustration below, when an HTTP request is sent from a Web browser, AOS checks the URL against the URL filter list, determines the action to be taken, and either permits or denies the HTTP responses.



If the URL filter is monitoring outbound requests on an interface, it will either deny or permit requests that exit the router via that interface. If the URL filter is monitoring inbound requests on an interface, it will either deny or permit requests that enter the router via that interface.

Top Websites Reporting

The top websites reporting feature, in combination with the URL filtering, creates a filtering package for small- to medium-sized businesses without the use of an external server. Top websites reporting tracks the most requested domain names that are not included in the URL filter's exclusive-domain list. The feature tracks requests in 15-minute increments, and collects the requests in 15-minute, hourly, and 24-hour reports. These reports allow system administrators to view the most requested URLs and decide if those URLs should be permitted or denied by the URL filter.

Hardware and Software Requirements and Limitations

URL filtering and top websites reporting are available on the following AOS data products running firmware version 16.1 or later: NetVanta 1335, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 4305, and NetVanta 5305.

URL filtering and top websites reporting are available on the following AOS voice products running firmware version A1.1 or later: Total Access 900(e) Series, NetVanta 6355, and NetVanta 7000 Series.

Only one HTTP URL filter may be used in a given configuration.

HTTP over secure socket layer (HTTPS) and File Transfer Protocol (FTP) URL filtering are not currently supported.

Configuring URL Filtering in AOS

The following steps are required to implement URL filtering in AOS:

1. Enable the AOS firewall.
2. Create a URL filter.
3. Configure the URL filter.
4. Apply the URL filter to an interface.
5. Specify the URLs to permit or deny.

Step 1: Enable the AOS firewall

To enable the AOS firewall, enter the **ip firewall** command from the Global configuration mode in the AOS command line interface (CLI).

NOTE

*The firewall must be enabled in order to use URL filters. For more information regarding firewall configuration, refer to the **Global Configuration Mode** of the **AOS Command Reference Guide** on the AOS Documentation CD available at **www.adtran.com**.*

The following example enables the firewall:

#**configure terminal**
(config)#**ip firewall**

Step 2: Create a URL filter

Once the firewall is enabled, create a URL filter by entering the **ip urlfilter** *<name>* **http** command from the Global configuration mode. The *<name>* parameter is the name you will give to this particular filter; for example, **myfilter**. Use the **no** form of the command to delete the specified filter.

(config)#**ip urlfilter myfilter http**

The **http** parameter instructs the firewall to filter HTTP requests and responses.

Step 3: Configure the URL filter

The URL filter can be configured by using one of two methods. In the first method, the filter is placed in **allowmode**, and URLs are specified to be denied using the **exclusive-domain** command. In the second method, the filter is not in **allowmode**, and URLs are specified to be permitted using the **exclusive-domain** command. Refer to Step 5 for more information on the **exclusive-domain** command.

The **allowmode** parameter allows all HTTP requests. By default, a URL filter will block all HTTP requests unless it can communicate with a URL filter server (such as a Websense server) for permit or deny information. Because this URL filter feature is designed to operate without an external server, URL filters can either first allow all HTTP requests by using **allowmode**, and then deny those specified by the system administrator; or URL filters can block all HTTP requests and then permit those specified by the system administrator. Using the **no** form of the **allowmode** command returns the filter to the default in which it denies all HTTP requests.

To place the URL filter in **allowmode**, enter the **ip urlfilter allowmode** command from the Global configuration prompt.

(config)#**ip urlfilter allowmode**

The URL filter configuration will affect the top websites report. If **allowmode** is enabled on the URL filter, all allowed sites will be reported in the top websites report. If **allowmode** is disabled on the URL filter, only the attempted site connections that were blocked will be reported.

Step 4: Apply the URL filter to an interface

After the URL filter has been created and placed in **allowmode**, it should be applied to the desired interface. The URL filter can be used to filter either inbound or outbound traffic, depending on configuration preference. To apply the URL filter to an interface, enter the **ip urlfilter** *<name>* **[in | out]** command from the interface's configuration mode.

(config)#**interface ethernet 0/1**
(config-eth 0/1)#**ip urlfilter myfilter in**

In the preceding example, the URL filter named **myfilter** is applied to the Ethernet interface located in slot 0/port 1, and is set to filter incoming HTTP requests.

Step 5: Specifying the Permitted and Denied URLs

Permitted URLs are the websites that network users are allowed to access. Denied URLs are the websites that network users are not allowed to access. Each website or URL that you wish to permit or deny on your network must be entered individually. The **ip urlfilter exclusive-domain** command instructs AOS to always permit or always deny a domain.

To either deny or permit a website, enter **ip urlfilter exclusive-domain [deny | permit]** <*name*> from the Global configuration mode. The <*name*> parameter is the domain name of the website you wish to permit or deny.

The **deny** parameter specifies that the domain name be denied. The following example configures the URL filter to deny the Party Poker website:

(config)#**ip urlfilter exclusive-domain deny www.partypoker.com**

The **permit** parameter specifies that the domain name will be allowed. The following example configures the URL filter to allow the ADTRAN website:

(config)#**ip urlfilter exclusive-domain permit www.adtran.com**

To simplify the entry process, wildcards can be incorporated into the **ip urlfilter exclusive-domain** command. An asterisk (*) can be used to represent one or more characters.

In the following example, the asterisk (*) has been used to instruct AOS to match the domains of www.adtran.com, www.adtran.org, www2.adtran.com, etc.

(config)#**ip urlfilter exclusive-domain permit *adtran***

A second wildcard parameter is a question mark (?) that can be used to represent exactly one character in the domain name. The domain name must be enclosed in quotation marks when using the question mark wildcard.

In the following example, the question mark (?) has been used to match the domains of www.adtran.com and www.adtran.org, but it will not match www2.adtran.com.

(config)#**ip urlfilter exclusive-domain permit "www.adtran.???"**

The use of wildcards is beneficial in creating the list of permitted or denied websites because each variation of a domain does not have to be entered in separately. However, each separate domain that you wish to deny or permit must be entered individually.

Once the permit/deny list has been created, the URL filter is configured for the specified interface.

Configuring Top Websites Reporting in AOS

Once the URL filter has been created and applied to an interface, the top websites reporting feature can be configured. If no URL filter has been created, any attempt to enable top websites statistics will result in the following message:

Warning! A url filter must be configured and applied to interface to gather the Top Website statistics.

Configuring top websites reporting entails enabling the feature, and determining the best mode for viewing the results.

Enabling Top Websites Reporting

To enable top websites reporting, enter the **ip urlfilter top-website** command from the Global configuration mode. For example:

(config)#**ip urlfilter top-website**

AOS will begin collecting statistics in 15-minute increments and reporting them in 15-minute, hourly, and 24-hour statistical reports.

Viewing Top Websites Reports

There are three ways to view the top websites reports. They may be viewed through the CLI, through the Web-based graphical user interface (GUI), or through messages sent by AOS to specified email addresses.

CLI Viewing

To view the top websites report from the AOS CLI, enter the **show ip urlfilter top-websites [hourly | daily | all]** <*number*> command from the Enable mode. The optional **[hourly | daily | all]** parameters allow the system administrator to specify that the statistics for the current hour, the current day, or for all lists be displayed. By default, the 15-minute increment list will be shown. The 15-minute increment list is for the previous 15-minute interval, not the current one. The output shows the 15-minute period for which the statistics were collected, as well as the current time so the system administrator knows when the next update will occur. The <*number*> parameter specifies how many websites will be shown on the report. The report can show between 5 and 20 websites at one time, the default being 10 websites per list.

The following example displays the top 5 websites visited in the last 15 minutes:

#**show ip urlfilter top-websites 5**

```
Top Websites Visited
Period: Apr 26 08:55:00 – Apr 26 09:10:00         Current Time: 09:15:34

Allow mode: enabled

The visits listed below are visits which were permitted.  These statistics do not include
Websites explicitly filtered using exclusive domains.

Domain Name                              Visits            Last Visitor         Visit Time
www.gmail.com                            767               10.22.160.7        Apr 26 08:55:47
www.google.com                           540               10.22.160.88       Apr 26 09:05:27
www.adtran.com                           67                10.22.160.107      Apr 26 08:59:16
www.cisco.com                            67                10.22.160.5        Apr 26 09:01:05
www.partypoker.com                       15                10.22.160.45       Apr 26 09:04:43
```

GUI Viewing

To view the top websites report via the GUI, follow these steps:

1. Open a new Web page in your Internet browser.
2. Type your AOS product’s IP address in the Internet browser’s address field in the following form: **http://**<*ip address*>. For example:

   http://65.162.109.200

3. At the prompt, enter your user name and password and select **OK**.

NOTE *The default user name is **admin** and the default password is **password**.*

4. Select the **Top Websites** option under the **URL Filtering** portion of the **Data** menu on the left.

5. From the **View Top Websites** menu, select from the **15-minute List**, the **Hourly List**, or the **Daily List** tabs. Each list also provides the option to select websites to be added to the **Excluded-domain List**, which will be updated after the next report is generated. To add a URL to the **Excluded-domain List**, highlight the URL to add and select **Apply**. Domains added to the **Excluded-domain List** will no longer appear on the top websites report.

Email Viewing

The top websites report can also be configured to be sent to you via email. This configuration is done through the CLI. To configure the top websites feature for email reporting, follow these steps:

1. Turn on logging email with the following command:

   (config)#**logging email on**

2. Use the **logging email receiver-ip** *<hostname | IP address>* to configure the email server. Enter the email server's host name or IP address (expressed in dotted decimal notation) as follows:

   (config)#**logging email receiver ip XX.XXX.XXX.XXX**

   For example,

   (config)#**logging email receiver ip 65.162.109.200**

3. Enter the email addresses of those to receive the top websites report using the **logging email ip urlfilter top-websites address-list** *<email addresses>* command as follows:

   (config)#**logging email ip urlfilter top-websites address-list sys.admin@adtran.com**

> **NOTE** *Multiple recipient email addresses can be listed separated by a semi-colon* ***(;).***

4. Set the time that the emails should be sent using the **logging email ip urlfilter top-websites send-time** *<HH:MM:SS>* command. The *<HH:MM:SS>* parameter refers to hours, minutes, and seconds expressed in 24-hour format. The default time for sending the emails is midnight. To change the default time, enter the command from the Global configuration mode as follows:

   (config)#**logging email ip urlfilter top-websites send-time 05:30:00**

   In the previous example, emails containing the top website information will be sent at 5:30 a.m.

Configuration Example

The following example configures a URL filter named **myfilter** for an outbound WAN interface (**ppp 1**) with top websites reports emailed to one recipient at 9:00 p.m.

```
#configure terminal
(config)#ip firewall
(config)#ip urlfilter myfilter http
(config)#ip urlfilter allowmode
(config)#interface ppp 1
(config-ppp 1)#ip urlfilter myfilter out
(config-ppp 1)#exit
(config)#ip urlfilter top-website
(config)#logging email on
(config)#logging email receiver ip 65.162.109.201
(config)#logging email ip urlfilter top-websites address-list system.admin@somewhere.com
(config)#logging email ip urlfilter top-websites send-time 21:0:0
```

Command Summary

Access Prompt	Command	Description	Default
(config)#	**ip firewall**	Enables the AOS firewall.	Disabled.
(config)#	**ip urlfilter** *<name>* **http**	Creates a URL filter.	No URL filters are configured.
(config)#	**ip urlfilter allowmode**	Allows all URLs.	All URLs are blocked.
(config-interface)#	**ip urlfilter** *<name>* **[in | out]**	Applies a URL filter to an interface.	No URL filters are applied to an interface.
(config)#	**ip urlfilter exclusive-domain [deny | permit]** *<name>*	Adds domains to the URL filter and specifies permit or deny.	No domains are in the URL filter list.
(config)#	**ip urlfilter top-website**	Enables the top websites statistics.	Disabled.
(config)#	**logging email on**	Enables logging email.	Disabled.
(config)#	**logging email receiver-ip** *<hostname> <address>*	Configures an email server to receive top websites information.	No server configured.
(config)#	**logging email ip urlfilter top-websites address-list** *<email addresses>*	Specifies email recipients for the top websites report.	No recipients specified.
(config)#	**logging email ip urlfilter top-websites send-time** *<HH:MM:SS>*	Sets the time to email top websites reports.	Email sent at midnight.
#	**show ip urlfilter top-websites [hourly | daily | all]** *<number>*	Displays the top websites report in the CLI.	Displays 10 websites at a time.

Troubleshooting

After configuring a URL filter and top websites reporting, several different commands can be issued from Enable mode in the CLI to assist in troubleshooting. These commands are detailed in the following table.

AOS URL Filter Troubleshooting Command Summary

Command	Explanation
#**show ip urlfilter**	Displays configured URL filter information.
#show ip urlfilter top-websites [hourly | daily | all] *<number>*	Displays the latest top websites information in an hourly, daily, or all lists format.
#**debug ip urlfilter**	Displays a summary of debug information for the URL filter.
#**debug ip urlfilter top-websites**	Enables debug output for the top websites feature.
#**clear ip urlfilter statistics**	Clears all statistics counters for URL filter requests and responses.
#**clear ip urlfilter top-websites**	Clears the top websites statistics.

Show Commands

Use the **show ip urlfilter** commands to display information pertinent to the URL filter configuration on your AOS product and to reveal configuration problems. This command displays the current configuration of the URL filter–its name, the ports used, the interface it's applied to, and excluded or permitted URLs. The following is sample output from the **show ip urlfilter** command:

```
#show ip urlfilter
Filters
-------
Name: “filter1”
Ports: HTTP(80)
Interfaces that filter is applied to:
eth 0/2 inbound
Servers
-------
IP address: 10.100.23.116
Port: 15868
Timeout: 5
Excluded domains
----------------
Permit www.adtran.com
Other Settings
--------------
Allow mode: Off
Maximum outstanding requests: 500
Maximum number of response packets buffered: 100
```

To view the top websites report from the AOS CLI, enter the **show ip urlfilter top-websites [hourly | daily | all]** <*number*> command from the Enable mode. This command displays the website request statistics for the specified interval. More detailed information about this command is located on page 6 of this guide.

Debug Commands

Debug commands are another useful tool to diagnose problems with the URL filter or top websites reporting configurations. By enabling **debug** commands, debug messages are sent to alert you whenever specified actions take place. These messages can be beneficial when you are troubleshooting your configuration.

NOTE *Using **debug** commands can be very processor intensive, and should be used with caution.*

To receive notification whenever an action takes place on the part of the URL filter, use the **debug ip urlfilter** command. This command indicates when the URL filter has allowed or blocked a URL. The following is sample output from the **debug ip urlfilter** command:

```
#debug ip urlfilter
2005.11.06 05:33:26 Allowed http://www.adtran.com/
```

The **debug ip urlfilter top-websites** command displays when the generated top websites lists merge (as the 15-minute list is rolled into the hourly list, the hourly list into the daily list, and so on). The following example is sample output from the **debug ip urlfilter top-websites** command:

```
#debug ip urlfilter top-websites
  2007.05.08 09:55:00 Merging displayed 15 minute list into hour list
  2007.05.08 09:55:00 Merging hour list into twenty-four hour list
  2007.05.08 09:55:00 Validating timers; timerAdj=0, update=0, lastThen=462
  2007.05.08 09:55:00 Scheduled next run in 900; timerAdj=0, nowUpTime=462,
  last Period=306
```

Clear Commands

You can easily clear the statistics of your URL filter list or top websites reports by using the **clear ip urlfilter** commands, allowing new statistics to be configured and observed.

To clear statistics for the URL filter, use the following command:

#**clear ip urlfilter statistics**

To clear statistics for the top websites reporting feature, use the following command:

#**clear ip urlfilter top-websites**

