Websense i-Series Appliance Traffic Monitor

Topic 70188 | Updated 01-Mar-2016

Applies to:	i-Series appliance v1.6

You can configure display elements for a real-time traffic monitor to examine selected attributes of the traffic that is analyzed by the Websense i-Series appliance. This monitor is accessed via the appliance command-line interface (CLI).

The following commands are associated with configuring traffic monitor display elements and running the traffic monitor:

- *set_default_display*
- *reset_default_display*
- *show*
- *monitor*

Syntax format for the traffic monitor commands is:

```
<command> <attribute 1>,<attribute 2>...
```

These commands take the following set of parameters to configure the traffic attributes to display when the traffic monitor is running.

Entries marked with an asterisk (*) may accept wildcards (e.g., *.example.com).

Parameter	Traffic Monitor Display
disp	Current request disposition (e.g., allow, confirm, block, quota, redirect_to_auth, redirect_to_host) **Note:** A **redirect_to_auth** disposition means the appliance has redirected the transaction to begin an authentication sequence. This situation may apply if the user is not authenticated in the system. **Note:** A **redirect_to_host** disposition means the appliance has redirected the transaction to the cloud service for analysis. Any subsequent requests for this TCP session are monitored by the cloud service, not the traffic monitor.
src_ip	Source IP address for the request
dst_ip	Destination IP address for the request

Parameter	Traffic Monitor Display
src_port	Source port for the request
dst_port	Destination port for the request
date_time	Request start date/time
email*	End user email address (if the user is authenticated in the system)
protocol*	Request protocol type
reason*	Category that determined the disposition of the request
policy_name*	Policy applied to the traffic
Attributes that apply only to HTTP/HTTPS traffic	
url*	Full URL of the request (in HTTP and HTTPS requests)
url_short*	Request URL without the query string
hostname*	Hostname in the incoming request URL
user_agent*	User Agent header
browser*	Client browser (from the User Agent header of the incoming request)
os*	Client operating system (from the User Agent header of the incoming request)
elevated_risk	When an incoming URL is identified as being in an elevated risk category, the **elevated_risk** entry is marked with "ER".
categories*	List of categories that match the request

Access and run the traffic monitor using the following commands:

```
cmd> status
status> monitor
monitor <arguments>
```

To exit the traffic monitor tool, use the **Ctrl-C** key combination.

Command options

set_default_display

This command lets you set the default traffic request attributes that are displayed when attributes are not explicitly defined in the **monitor** command. Initially, the default display includes all available traffic attributes, shown in the table in the previous section.

Command syntax is:

```
set_default_display <attribute 1>,<attribute 2>,...
```

reset_default_display

This command lets you reset the default display attributes list to its initialized state. When you execute this command and then execute a **monitor** command without specifying any display attributes, all available display attributes (shown in the previous table) are included in traffic monitor log entries.

Command syntax is:

```
reset_default_display
```

show

This command allows you to view the available display and filter traffic attributes, along with available protocols. See the table at the beginning of this article for a list of traffic attributes. See *--display* and *--filter* for command syntax for these options.

You can also see the default attributes configured with the **set_default_display** command.

The **show** command parameters are summarized as follows:

Parameter	Description
default_display	Shows the default display attributes currently specified in the **set_default_display** option
display_attributes	Shows all available traffic attribute parameters for the **--display** option
filter_attributes	Shows all available traffic attribute parameters for the **--filter** option
protocols	Shows all available protocols for the **--filter protocol** option

monitor

This command lets you run the traffic monitor. The following options can be used with the **monitor** command:

- *--display*
- *--filter*
- *--upload*
- *--upload --username*

If you do not use any arguments with the **monitor** command, the traffic attributes displayed are those defined in the **set_default_display** command.

- -display

This option lets you specify traffic request attributes to display and the order of their appearance in the monitor entry. This setting overrides the **set_default_display** command settings.

Command syntax is:

```
monitor --display <attribute 1>,<attribute 2>,...
```

Parameters for this command are summarized in the table shown at the beginning of this article.

- -filter

This option lets you configure rules for the specific traffic you want the monitor to analyze. The **--filter** rules can use any of the parameters shown in the table at the beginning of this article to define the traffic monitor display.

Sample --filter option rules

A single **--filter** command option with multiple parameters implies an "and" relationship between the parameters. For example:

```
monitor --filter src_ip=1.1.1.1 src_port=8080
```

means to monitor traffic that has the following attributes:

source IP address is 1.1.1.1

and

source port is 8080

Multiple **--filter** command options, each with its own parameters, create an "or" relationship between the **--filter** option parameters. For example:

```
monitor --filter src_ip=1.1.1.1 --filter src_ip=2.2.2.2
```

means to monitor traffic that has the following attributes:

source IP address is 1.1.1.1

or

source IP address is 2.2.2.2

You can also use commas to create an "or" relationship between **--filter** command option parameters. Using the previous example:

```
monitor --filter src_ip=1.1.1.1,2.2.2.2
```

You can create rules that contain a mix of "and" and "or" relationships. For example:

```
monitor --filter src_ip=1.1.1.1 src_port=80 --filter
dst_ip=2.2.2.2 dst_port=80
```

means to monitor traffic that has the following attributes:

source IP address is 1.1.1.1 **and** source port is 80

or

destination IP address is 2.2.2.2 **and** destination port is 80

You can configure the **--filter** command option for ranges of values. For example:

```
monitor --filter src_ip=1.1.1.1-2.2.2.2
src_ports=80,443,1000-2000
```

means to monitor traffic that has the following attributes:

source IP address between 1.1.1.1 **and** 2.2.2.2

and

source ports 80 **or** 443 **or** between 1000 **and** 2000

You must use quotation marks for **--filter** command option parameters that contain a space. For example:

```
monitor --filter browser="microsoft internet explorer"
```

--upload

This option lets you upload traffic monitor results in a file to a server. The results file is compressed using gzip, so the recommended file extension to use is ".gz". For example:

```
monitor --upload ftp://example.com/mylog.csv.gz --file_type
csv
```

means to upload the **mylog.csv.gz** file in csv format to **ftp://example.com**.

> **Note**
> The uploaded results file may not exceed 100 MB. When the file exceeds this size limit, traffic monitor operation is stopped. If you need a larger file size limit, please contact Technical Support.

Use the **--file_type** command option shown in the previous code sample to specify one of the following file types to upload: text, block, or csv.

Text

Each log entry is shown on one line, with each display attribute shown in a distinct column (as displayed on the CLI screen).

Example output:

```
src                  | dst                  | categories                    | disp
-------------------------------------------------------------------------------------------------
10.0.39.245:50344 | 87.248.214.203:443 | Gambling, Elevated Risk Profile | ALLOW
```

Block

Each log entry is shown on multiple lines, with each display attribute on a different line (i.e., format for each line is <display attribute name> : <value>).

Example output:

```
src = 10.0.39.245:50344

dst = 87.248.214.203:443
categories = Gambling, Elevated Risk Profile
disp = ALLOW
--------------------
```

CSV

Each log entry is shown in one line, with each attribute separated by a comma (i.e., <display attribute name> <value>, <display attribute name> <value>, etc.).

Example output:

```
src,dst,categories,disp

10.0.39.245:50344,87.248.214.203:443,"Gambling, Elevated Risk Profile",ALLOW
```

- -upload - -username

This command lets you set a username and password for the upload operation. For example:

```
monitor --upload --username example_username
```

You are prompted to enter a password after you run this command.

Note that a username may not contain a colon (:).