Using TestLogServer for Troubleshooting

Using TestLogServer | Web Protection Solutions | v8.4.x, v8.5.x | 30-Nov-2018

A command-line utility called TestLogServer is included with Forcepoint Web Security and Forcepoint URL Filtering. The utility displays log data sent from Filtering Service to Log Server.

Use TestLogServer to verify that logging data is being sent to Log Server as expected, and to diagnose problems with:

- URL request management and policy enforcement
- Authentication
- Logging
- URL categorization and protocol identification

This collection includes the following articles to help you use TestLogServer:

Running TestLogServer

Using TestLogServer | Web Protection Solutions |v8.4.x, v8.5.x | 30-Nov-2018

In order to screen log traffic with TestLogServer without interrupting the flow of log records to Log Server, first launch the utility using parameters that forward all traffic to Log Server, then use the Forcepoint Web Security module of the Forcepoint Security Manager to configure Filtering Service to pass log traffic to TestLogServer.

1. On the Log Server machine, open a command prompt or PowerShell and navigate to the **bin** directory (C:\Program Files\Websense\Web Security\bin, by default).
2. Start the TestLogServer utility with the following parameters. (For a complete list of available parameters, see *TestLogServer parameters*, page 2.)

   ```
   testlogserver -port 5555 -forward <IP address>:55805
   ```

   - Provide the IP address of the Log Server machine. If port 5555 is in use, you can use any available port.

- If you are running TestLogServer in a production environment at a time of normal or higher traffic loads, you may want to use one or both of the following additional parameters:

  ```
  -file <filename.txt>
  -onlyip <IP address>
  ```

  The first parameter allows you to redirect traffic to a file for review, rather than having it scroll rapidly across the console. The file is created by default in the bin directory.

  The second parameter allows you to monitor traffic only from the IP address specified.

Initially, when the utility launches, no traffic appears. Traffic must still be redirected to TestLogServer, as described in the steps that follow.

3. Log on to the Security Manager and navigate to the **Web** > **Settings** > **General** > **Logging** page.
4. Make sure that the Log Server IP address is correct. This should be the actual IP address of the Log Server machine, and not the loopback address (127.0.0.1), even if Log Server and Security Manager are installed on the same machine.
5. Change the port to **5555** (or the value you've selected).
6. Click **Check Status** to verify the connection to TestLogServer.
7. Click **OK** and then **Save and Deploy**.
8. Review the captured data. See *Understanding TestLogServer output*, page 4, for help in parsing the data.
   - If you are in a test environment, or performing this test at a low-traffic period, generate traffic from specific machines while monitoring TestLogServer to verify that the traffic appears.
   - If you are using the tool in a production environment while normal traffic flow is occurring, and the data is coming too rapidly to process, review step 2 for options for redirecting output or capturing traffic only for a specific machine.
9. When you are finished, first return to the **Settings** > **General** > **Logging** page, and change the logging port back to its original value (55805, by default). Remember to click **OK** and **Save and Deploy** to cache and then implement your change.

   At this point, traffic is sent directly to Log Server and stops appearing in TestLogServer.
10. In the command window where TestLogServer is running, press Ctrl+C to stop the utility.

TestLogServer parameters

Using TestLogServer | Web Protection Solutions |v8.4.x, v8.5.x | 30-Nov-2018

TestLogServer uses input from parameters you enter as part of a command. (See *Running TestLogServer*, page 1, for details on executing the command.)

Each parameter should be preceded by a dash (-) and followed by a space and value (argument), if indicated. Parameters may be entered in any order.

The supported parameters are:

Parameter	Description
-file	Used to direct output to a file, and to specify the file name. By default, the file is created in the **bin** directory (C:\Program Files\Websense\Web Security\bin) on the TestLogServer machine. For example: `-file testlogdata.txt` By default, TestLogServer sends output to the console. If you are running the utility during a time of high traffic, the scrolling output may be difficult to read.
-forward	Used to forward data from TestLogServer to Log Server. This prevents loss of log data while troubleshooting is occurring. Use this parameter and include the Log Server IP address and port, in the following format: `-forward 10.201.130.4:55805`
-help	Used to display a list of TestLogServer parameters.
-iprange	Used to specify the range of source IP addresses from which to display logging data. For example: `-iprange 10.100.67.10 10.100.67.50` Do not include a dash between the two IP addresses. This parameter is valuable if you are researching logging traffic at times of high load.
-nopp	Used to omit formatting and display data in binary format. Requires the -file parameter. This parameter is used primarily for debugging.
-onlyip	Used to display data for a single IP address. For example: `-onlyip 10.57.98.16`
-port	Used to specify the TestLogServer listening port. By default, 55805 (the Log Server default listening port) is used. If the default port is used, Log Server must be stopped before TestLogServer is run. For this reason, an alternate port is typically specified. Any custom port must also be added to the **Web >Settings > General > Logging** page in Security Manager so that Filtering Service forwards data correctly.
-raw	Used to display all of the raw data that TestLogServer receives. Both formatted and raw binary data are shown. This parameter is used primarily for debugging.

Understanding TestLogServer output

When you run TestLogServer, the output includes the following information, if available.

Field	Description
Log Source	The component that sent the Internet request to Filtering Service
Client Hostname	Hostname of the machine from which the request originated, if available. If a hostname is not available, the client IP address is displayed.
SourceIP	IP address from which the request originated This can be used to verify that Filtering Service is seeing traffic from specific machines.
DestinationIP	IP address of the requested (target) URL Incorrect or missing data can indicate DNS issues, which prevent proper filtering.
server	IP address of the Filtering Service machine
time	Exact time that the request was generated, as provided by the Filtering Service machine
version	Version of the log record being processed *(internal use only)*
disposition	Action applied to the request by Filtering Service. For example, category blocked, permitted by exception, continue user blocked, and so on.
URL	The requested (target) URL
protocol	The protocol (for example, HTTP, FTP) associated with the request. In the case of non-HTTP protocols, this value can indicate whether or not Filtering Service is classifying protocols correctly.
port	The port number the connection attempted to use
networkDirection	The direction of the network request (inbound or outbound)
method	The HTTP method (get or post)
contentType	Type of content specified in the record header
category	Master Database or custom category assigned to the requested URL
categoryReason	Reason the URL was categorized as it was (for example, defined in the Master Database, recategorized by content scanning, recategorized by custom URL, and so on)
bytes sent	Number of bytes sent
bytes received	Number of bytes received
file name	Name of the file, if any, retrieved from the URL

Field	Description
True File Type	The file type associated with the file, as confirmed by Content Gateway file type analysis (Forcepoint Web Security)
roleId	The number assigned to the delegated administration role that assigned the policy applied to this request. The Super Administrator role ID number is 8.
user	The name of the user making the request, if user identification or authentication is enabled and applied to the client IP address
duration	Time, in milliseconds, it took to look up the site
scan duration	Time, in milliseconds, it took Content Gateway to analyze the site (*Forcepoint Web Securityonly*)
policyName	Name of the policy applied to the request
keyword	The keyword, if any, used to recategorize and block a request

If you have enabled SIEM integration in the Security Manager, an additional **SIEM Results** section appears in the TestLogServer output. The SIEM Results section includes the following information. Note that information provided by Content Gateway is available only with Forcepoint Web Security.

Field	Description
protocol version	Current version of the protocol used to send data to the SIEM integration
server status code	HTTP status code sent from the origin server to Content Gateway
proxy status code	HTTP status code sent from the Content Gateway proxy to the client machine
client source port	Client ephemeral TCP source port
client destination port	Client TCP destination port
proxy source	IP address of the Content Gateway outbound interface
proxy source port	Outbound ephemeral TCP port used by Content Gateway
user agent	User agent string sent by the client browser or application.
X-Forwarded-For	IP address of the client which sent the request. The request was sent through a client proxy, load balancer, or similar device.

If the request was to a cloud application, an additional **Cloud App Results** section appears in the output. The Cloud App Results section includes the following information.

Field	Description
app id	Internal ID assigned to the cloud application.
app name	Name of the requested cloud application.
app risk level	Risk level (high, medium, or low) assigned to the cloud application.
app category id	Internal ID assigned to the type of cloud application.
app category name	Name of the cloud application type.

The output for each request looks something like this:

```
Log Source= Integration
Client Hostname= 192.168.3.50
SourceIp= 10.201.136.35
DestinationIp= 74.125.128.104
server= 10.201.136.130
time= Tue Jul 18 11:41:33 2017
version= 6
disposition= 1026 - Category Not Blocked
URL= http://www.google.com/
protocol= 1 - http
port= 80
networkDirection= Inbound
method= GET
contentType = text/html;
charset=UTF-8
category= 76 - SEARCH ENGINES AND PORTALS
categoryReason= 1 - Master Database: URL
bytes sent= 647
bytes received= 24041
file name=
True File Type= 0 - None
roleId= 8
user= WinNT://QA/qauser
duration= 719 ms
scan duration= 0 ms
policyName= role-8**Default
SIEM Results
   protocol version= 257
   server status code= 200
   proxy status code= 200
   client source port=49372
   client destination port= 8080
   proxy source=10.201.136.130
   proxy source port= 26615
   user agent= Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
```

```
6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729)
   X-Forward For=
Cloud App Results
   app id = 0
   app name =
   app risk level = 0
   app category id = 0
   app category name =
```