Stealthwatch® System

Proxy Log Configuration

(for Stealthwatch System v6.9.x)
Copyrights and Trademarks

© 2017 Cisco Systems, Inc. All rights reserved.

NOTICE

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.
Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Overview</td>
<td>6</td>
</tr>
<tr>
<td>Important Configuration Guidelines</td>
<td>6</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>6</td>
</tr>
<tr>
<td><strong>Configuration of the Blue Coat Proxy Logs</strong></td>
<td>8</td>
</tr>
<tr>
<td>Creating the Format</td>
<td>8</td>
</tr>
<tr>
<td>Create a New Log</td>
<td>9</td>
</tr>
<tr>
<td>Configure the Upload Client</td>
<td>10</td>
</tr>
<tr>
<td>Configuring the Upload Schedule</td>
<td>12</td>
</tr>
<tr>
<td>Notes</td>
<td>13</td>
</tr>
<tr>
<td>Configuration of the Visual Policy Manager</td>
<td>13</td>
</tr>
<tr>
<td><strong>Configuration of the McAfee Proxy Logs</strong></td>
<td>18</td>
</tr>
<tr>
<td><strong>Configuration of the Cisco Proxy Logs</strong></td>
<td>22</td>
</tr>
<tr>
<td>Configuration of the Flow Collector</td>
<td>25</td>
</tr>
<tr>
<td>Checking the Flows</td>
<td>25</td>
</tr>
<tr>
<td><strong>Configuration of Squid Proxy Logs</strong></td>
<td>27</td>
</tr>
</tbody>
</table>

© 2017 Cisco Systems, Inc. All Rights Reserved.
INTRODUCTION

Overview

In order to gather user information from your network proxy servers for the Stealthwatch System ProxyWatch you need to configure the proxy servers logs so that the Flow Collector can receive the information and the SMC will display the information on the Flow Proxy Records page. This page provides URLs and application names of the traffic inside a network going through the proxy server.

This document describes the various procedures needed to configure the logs for different proxy servers. These servers are Blue Coat, McAfee, Cisco, and Squid. This document assumes that you already have the proxy server running as part of your network. The procedures describe how to configure the proxy’s logs so that the files necessary for the Flow Collector are given and the information is provided.

Important Configuration Guidelines

When configuring the logs for any of the proxies, you must make certain to adhere to these guidelines:

- The Flow Collector and the proxy must use the same NTP server or receive time from a common source for flow and proxy records to be matched.
- When setting the IP address for Flow Collector, select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Stealthwatch Support
  - To open a case by email: tac@cisco.com
  - For phone support: 1-800-553-2447 (U.S.)
CONFIGURATION OF THE BLUE COAT PROXY LOGS

This chapter describes the procedure for configuring the Blue Coat proxy logs to deliver to the Stealthwatch System.

Note: The Blue Coat proxy version used for testing was SG V100, SGOS 6.5.5.7 SWG Edition.

Creating the Format

To create a new log format, complete the following steps:

1. In your browser, access your Blue Coat proxy server.
2. Click the Configuration tab.

3. In the Main Menu of the Management Console, click Access Logging > Formats.
4. Click the New button at the bottom of the page. The Create Format page opens.
5. In the Format Name field, type a name for the new format.
6. Select the W3C Extended Log File format (ELFF) option.
7. In the format field, type the following string:

```
timestamp duration c-ip c-port r-ip r-port s-ip s-port cs-bytes sc-bytes cs-user cs-host cs-uri
```

8. Click **OK**. Continue to the next section, **Create a New Log**.

## Create a New Log

To create the logs, complete the following steps:

1. **Click New**

   1. In the Main Menu, click **Access Logging > Logs**, and then select the new log format. The Log page opens.
2. Click the General Settings tab.

3. From the Log Format drop-down list, select the log you created in Step 1.
4. In the Description field, type a description for your new log.
5. Click the Apply button at the bottom of the page. Continue to the next section, Configure the Upload Client.

Configure the Upload Client

To configure the upload client, complete the following steps:

1. Click the Upload Client tab. The Upload Client page opens.
2. From the Client type drop-down list, select **Custom Client**.
3. Click the **Settings** button. The Custom Client settings page opens.

4. In the appropriate fields, type the IP address of the Flow Collector and listening port of the proxy parser.

   **Note:** SSL is not supported at this time.

5. Click **OK**.
6. For the Transmission Parameters, complete these steps:
   a. For the Encryption Certificate, select **No encryption**.
   b. From the Signing Keyring drop-down list, select **no signing**.
   c. From "Save the log file as" select the Text file option.
   d. In the "Send partial buffer after" text box, type **5**.
   e. Click the Upload schedule tab, and select the continuously option for the Upload the access log.
   f. In the Wait between connect attempts field, type **60**.
   g. In the Time between keep-alive log packets field, type **5**.

7. Click the **Apply** button at the bottom of the page. Continue to the next section, *Configuring the Upload Schedule*

### Configuring the Upload Schedule

To configure the upload schedule, complete the following steps:

1. Click the Upload Schedule tab.
2. For the "Upload the access log," select continuously.  
3. Wait between correct attempts is 60 seconds.  
4. Time between keep-alive log packet 5 seconds.  
5. Click the Apply button at the bottom of the page.  

This completes the configuration for the Blue Coat proxy logs for the Flow Collector.

Notes

Further notes on configuration:

- The Flow Collector and Proxy must be on the same NTP server or receive time from a common source for flow and proxy records to be matched.
- Only ONE log output mechanism for the proxy is supported. If you are already exporting logs for some particular reason we will not be able to capture and parse proxy records.
- UDP is not supported.

Configuration of the Visual Policy Manager

Configuration of the Visual Policy Manager enables you to check that the proxy log is being sent to the Flow Collector.

2. Click the Launch button at the bottom for your configured log. The Visual Policy Manager for the log window opens.


4. Type a name for the new layer, and then click **OK**.

5. Right-click **Deny** in the Action column and then click **Set**. The Set Action Object dialogue opens.

7. Click Enable logging to.
8. Type a name for your log and then select your log.
9. Click OK. The object is added.
10. In the Set Action Object dialogue, click OK.
11. Click the **Install policy** button at the top right.
12. Click **No** and then **OK** for the following windows.

13. Launch the Blue Coat Visual Policy Manager again.

14. Right-click the logging tab and then select **Enable Layer**.
15. Click the Install Policy button. The Policy Installed opens.
16. Click **OK**

17. Click the **Statistics** tab, and in the log menu, select your log.

18. In the main menu, click **Access Logging**, and then click the Log Tail tab. The Log Tail window opens.
19. Click **Start Tail** button at the bottom of the page.
20. On the Statistics main menu, click **System > Event Logging**.

This page will show if the log file is uploaded to the Flow Collector and the changes made. It shows whether the proxy is connected to the Flow Collector.
CONFIGURATION OF THE McAfee Proxy Logs

This chapter describes the procedure for configuring the McAfee proxy logs from the McAfee Web Gateway to deliver to the Stealthwatch System.

**Important:** Be sure that you have downloaded the XML configuration file for the McAfee proxy. Go to the Stealthwatch Download and License Center (https://lancope.flexnetoperations.com), to obtain the file and readme, ProxyWatch XML Configuration File.

**Note:** The McAfee proxy version used for testing was 7.4.2.6.0 - 18721.

To set up the McAfee proxy log, complete the following steps:

1. Download the XML file, FlowCollector_[date]_McAfee_Log_XML_Config_[v].xml, and then save it to your preferred location.

   **Note:** "Date" indicates the date of the XML file, and "v" indicates the version of the McAfee proxy version. Be sure to select the XML file with the same version number as your McAfee proxy.

Follow these steps to acquire it:

   a. Go to https://lancope.flexnetoperations.com, the Stealthwatch Download and License Center. The Login page opens.
   b. Enter your Login ID and Password in the appropriate fields, and then click Login. The Product Home page opens.
   c. Click Downloads.
   d. Select the link, "vX.X Updates for the FlowCollector NetFlow Series."
   e. Download and save the XML file.

2. Log in to the McAfee proxy server.

3. Click the Policy icon, and then click the Rule Sets tab.
4. Select **Log Handler**, and then select **Default**.

5. Click **Add > Rule Set from the Library**.

6. Click **Import from file**, and then select the XML file.
7. Select **mcafeelancopelog** in the log handler that was just imported.

   **Note:** Make sure the rule set and the rule “create access logline” and “send to syslog” is enabled.

8. Click the Configuration icon at the top of the page.
9. At the left of the page, click the File Editor tab, and then select the rsyslog.conf file.
10. At the bottom of the text box (beside the list of files), type the follow text:

daemon.info @[FlowCollector IP Address:514]

Important: Make certain to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

11. Comment out this line: *.info;mail.none;authpriv.none;cron.none.
12. Add this line: *.info;daemon.!=info;mail.none;authpriv.none;cron.none -/var/-log/messages.
13. Click the Save Changes button at the top right of the page.
CONFIGURATION OF THE CISCO PROXY LOGS

This chapter describes the procedure for configuring the Cisco proxy logs to deliver to the Stealthwatch System.

To set up the Cisco proxy log, complete the following steps:

1. Log in to the Cisco proxy server.

2. On the main menu, click **System Administration > Log Subscriptions**. The Log Subscriptions page opens.

3. Click the **Add Log Subscriptions** button. The New Log Subscriptions pages opens.
4. From the Log Type drop-down list, select W3C Logs. The available W3C Log fields appear.

5. In the Log Name field, type a name for the log that you will use.

6. From the Available Log Fields list, select **Timestamp**, and then click the Add button to move it the Select Log Fields list.
7. Repeat the previous step for each of the following log fields in order:

   a. x-elapsed-time
   b. c- ip
   c. c-port
   d. cs-bytes
   e. s-ip
   f. s-port
   g. sc-bytes
   h. cs-usernames
   i. s-computerName
   j. cs-url

   The Selected Log Fields list should contain these fields as illustrated:

![Selected Log Fields](image)

8. Scroll to the bottom of the page, and then select the **Syslog Push** option.

![Syslog Push](image)

9. In the Hostname field, type the Flow Collector IP address or its host name that the proxy sends logs to.

   **Important:** Make certain to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

10. Click **Submit**.
The new log is added to the Log Subscription list and logs from the proxy will be collected by the Flow Collector.

**Configuration of the Flow Collector**

After you have configured the Cisco proxy to send syslog information, you now need to configure the Flow Collector to accept the data.

To configure the Flow Collector to receive syslog information, complete the following steps:

1. Log in to the Flow Collector Admin interface.
2. On the main menu, click **Configuration > Proxy Ingest**. The Proxy Servers page opens.
3. Type the IP address of proxy server
4. From the Proxy Type drop-down list, select **Cisco**.

**Note:** If your type of proxy server is not listed, you will not be able to use ProxyWatch at this time.

5. In the Proxy ID field, type the IP address of the proxy server.
6. In the Proxy Service Port field, type the port number of the proxy server.
7. If you want the proxy server to trigger alarms, clear the Exclude from Alarming check box.
8. Click **Add**.
9. Click **Apply**. The proxy server appears in the Proxy Ingest table at the top of the page.

**Checking the Flows**

To check that you are receiving the flows, complete the following steps:

1. In the Flow Collector Admin interface, click **Support > Browse Files** in the main menu. The Browse Files page opens.
2. Open the syslog file.

3. Check that the marked files are not blank. If there are then, there is an issue.
   - Listeners has the number of the proxies.
   - Handlers is only one that parses out the data.
   - Emitters take parsed data from the handler and convert it into a format the engine is looking for.
   - Firewall

4. Check that the count is counting upwards to show that you are receiving data.
**Configuration of Squid Proxy Logs**

This chapter describes the procedure for configuring the Squid proxy logs to deliver to the Stealthwatch System. To configure the logs requires using SSH to edit files on the proxy server.

To configure the Squid proxy logs, complete the following steps:

1. Log into a shell for the machine running Squid
2. Go to the directory containing squid.conf (typically /etc/squid) and open it in an editor
3. Add the following lines to squid.conf to configure logging:

   ```
   logformat access_format %ts%03tu %<tt %><a %>p %>st %<A %><st %<la %><lp %la %lp %un %ru
   access_log syslog:user.6 access_format
   ```

4. Restart squid using the following:

   ```
   /etc/init.d/squid3 restart
   ```

5. Configure the syslog service on the Squid server to forward logs to the Flow Collector. This is dependent on the Linux distribution, but for syslog-ng you would add the following to /etc/syslog-ng:

   ```
   # Audit Log Facility BEGIN
   filter bs_filter { filter(f_user) and level(info) };
   destination udp_proxy { udp("10.205.14.15" port(514)); };
   log {
   source(s_all);
   filter(bs_filter);
   destination(udp_proxy);
   }
   # Audit Log Facility END
   ```

   **Important:** Make certain to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

6. Then restart syslog-ng with /etc/init.d/syslog-ng restart.