# Cisco Secure Network Analytics

Proxy Log Configuration Guide 7.4



## Table of Contents

Introduction	3
Overview	3
Important Configuration Guidelines	3
Configuring the Blue Coat Proxy Logs	5
Creating the Format	5
Create a New Log	6
Configure the Upload Client	7
Configuring the Upload Schedule	9
Notes	9
Configuration of the Visual Policy Manager	9
Configuring the McAfee Proxy Logs	15
Configuring the Cisco Web Security Appliance (WSA) Proxy Logs	19
Configuring Squid Proxy Logs	
Configuring the Flow Collector	
Checking the Flows	
Contacting Support	

### Introduction

### Overview

In order to gather user information from your network proxy servers for the Cisco Secure Network Analytics (formerly Stealthwatch) System Proxy Log you need to configure the proxy servers logs so that the Flow Collector can receive the information and the Manager (formerly Stealthwatch Management Console) 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 WSA, 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.

Complete the following steps to set up Secure Network Analytics Proxy Log:

- 1. Configure your proxy server:
  - a. Blue Coat
  - b. <u>McAfee</u>
  - c. <u>Cisco WSA</u>
  - d. <u>Squid</u>
- 2. Configure the Flow Collector
- 3. Check the Flows

### Important Configuration Guidelines

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

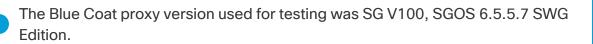
- The Flow Collector and the proxy must use the same NTP server or receive time from a common source for flow and proxy records to be matched.
- When setting the IP address for Flow Collector, select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.
- There is no specific size limit on syslog proxy messages imposed by Secure Network Analytics. However, we recommend that messages be kept shorter than the shortest maximum transmission unit (MTU) along the path between the proxy

and Flow Collector, usually 1500. This will eliminate packet fragmentation and increase reliability.

• Proxy Log is not supported in High Availability (HA) mode.

## Configuring the Blue Coat Proxy Logs

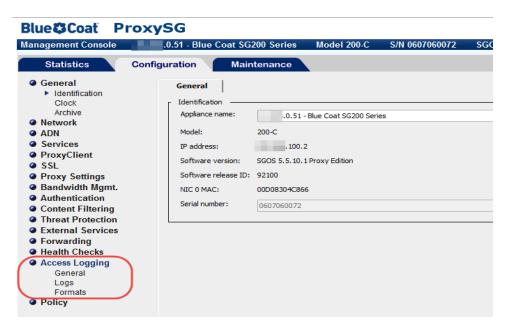
This chapter describes the procedure for configuring the Blue Coat proxy logs to deliver to Secure Network Analytics.



#### **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 **New** at the bottom of the page. The Create Format page opens.

	Create Format	
Format Settings:		
Format Name:		
<ul> <li>Custom format stri</li> </ul>	ng (specify below)	
W3C Extended Log	g File Format (ELFF) string (specify below)	
	ntent-Type) cs(User-Agent) sc-filter-result sc-filter-category x-virus-id s-ip s-sitename Test Format policy: Log last header v	
nurupie-valueu rieauer		
	OK Cancel	

- 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. In the Main Menu, click **Access Logging > Logs**, and then select the new log format. The Log page opens.

Create Log	×
Log Settings:	_
Log Name:	
Log Format: StealthWatch	
Description:	
Log file limits:	
The maximum size of each remote file is megabytes	
Start an early upload if log reaches 16000 megabytes	
Note: The maximum allowed upload threshold is: 19999 megabyte	s
OK Cancel	

2. Click the General Settings tab.

Logs   General Sett	ngs Upload Client Upload Schedule				
	Log: StealthWatch				
Log Settings:					
Log Format: StealthWatch		Ŧ			
Description:					
Log file limits:					
The maximum size of each r	mote file is 0 megabytes				
Start an early upload if log reaches 16000 megabytes					
Note: The maximum allowed	upload threshold is: 19999 megabytes				

- 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.

Logs General Set	ttings Upload Client Upload Schedule
Log:	StealthWatch 🗸
- Upload Client:	
Client type: Custom Clie	ent v Settings Test Upload
Transmission Parameters:	
Encryption Certificate:	<no encryption=""> V</no>
Signing Keyring:	<no signing=""></no>
Save the log file as:	⊖ gzip file  ● text file
Send partial buffer after:	5 seconds
Bandwidth Class:	<none> v</none>

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

Custom Client settings: Log StealthWatch	×
Custom server connection:	
Settings for: Primary Custom Server	
Host IP: .10.204 Port: 514	
Use secure connections (SSL)	
OK Cancel	

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

i) SSL is not supported at this time.

5. Click **OK**.

Transmission Parameters:	
Encryption Certificate: <no encryption=""></no>	~
Signing Keyring: <no signing=""></no>	*
Save the log file as: O gzip file	
Send partial buffer after: 5 seconds	
Bandwidth Class: <pre> </pre> <pre> </pre> <pre> </pre>	~

- 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.
- 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.

Logs General Settings	Upload Client Upload Schedule
	Log: StealthWatch
Upload type: Upload the access log	
<ul> <li>continuously O periodically</li> <li>Wait between connect attempts:</li> </ul>	60 seconds
Time between keep-alive log packets	5  seconds 

- 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

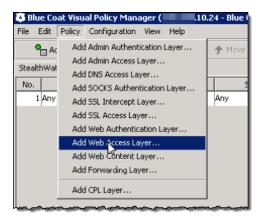
Configuration of the Visual Policy Manager enables you to check that the proxy log is being sent to the Flow Collector.



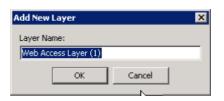
1. On the Configuration tab page in the Main Menu. click **Policy > Visual Policy Manager**. The Visual Policy Manager opens.

🔛 StealthWatch Management Console (admin - :=10.203)	
Blue Coat Visual Policy Manager (192.168.10.4 - Placet SG210 Series) 20	

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



3. Click **Policy > Add Web Access Layer**. The Add New layer screen opens.



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

	ction	Tra	ick
S Den	Allow Deny Deny (Cont	ent Filter)	
	Set Edit Delete		
-	Negate		
	Cut <b>Copy</b> Paste		

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

🐺 Set Action Object	×
Existing Action Objects	
Show: All (sort by object-name)	·
AccessLog1	<b>-</b>
Allow	
🕫 Always Verify	
👹 Block IM Message Encryption	
📸 Block Popup Ads	
🕋 Bypass Cache	
🚰 Check Authorization	
🚫 Deny	
🔗 Deny (Content Filter)	
E Dicabla East. Cachina in Windows Madia Cliant	-
New Remove Edit	
OK Cancel Help	

6. Click **New** and select **Modify Access Logging**. The Edit Access Logging Object dialogue opens.

🕃 Edit Acces	ss Logging Object	:	×
Name:	5tealthWatch_Lc	ogging	
	ll access logging: default access loggi	ina	
Enable lo	gging to:	StealthWatch	<b>_</b>
🔘 Disable lo	igging to	StealthWatch	<u>v</u>
	ОК	Cancel	Help

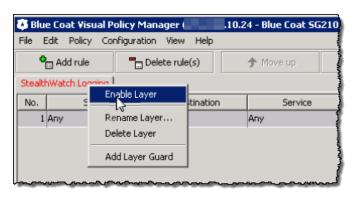
- 7. Click Enable logging to.
- 8. Type a name for your log and then select your log.
- 9. Click **OK**. The object is added.
- 10. In the Set Action Object dialogue, click **OK**.



- 11. Click the **Install policy** button at the top right.
- 12. Click **No** and then **OK** for the following windows.

Statistics Configuration Maintenance	
Summary Traffic Details Application Details ADN History	1
Bandwidth Mgmt.	ا

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.

Log Size Upload Status	1	
Log: StealthW.	atch	T
,		_
1458669295.851 0 .10.118 424	463 66.235.139.205 80 192.168.10.24 80 730 508 ·	- shutterfly.112.207.net http:/
1458669295.861 0 .10.110 651	22 23.195.245.198 80 192.168.10.24 80 149 345	- go.microsoft.com http://go.mi
	463 66.235.139.205 80 192.168.10.24 80 817 507 ·	
1458669300.396 0 .10.110 651	123 184.51.126.75 80 192.168.10.24 80 264 450 -	crl.microsoft.com http://crl.m
	122 23.195.245.198 80 192.168.10.24 80 149 344 ·	
1458669305.022 0 .10.110 651	123 184.51.126.75 80 192.168.10.24 80 278 448 -	crl.microsoft.com http://crl.m
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	᠂ᢞ᠖ᡔ᠕᠋ᡎᡎ᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆᠆	www.wiewer.ware.ware.ware.ware.ware.ware.ware.

- 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.

Statistics Conf	iguration Maintenance	
Summary	Event log: END OF LOG	
Traffic Details		
Application Details	2015-09-17 13:56:23-04:00EDT	"Access Log Custom (StealthWatch): Couldn't connect to server" 6F E000A:1 alog_stream_custom.cpp:317
ADN History	2015-09-17 13:56:23-04:00EDT	"Access Log (StealthWatch): Unable to connect to remote server for log uploading" 0 E0008:1 alog_facility
Bandwidth Mgmt.	2015-09-17 13:57:23-04:00EDT	"Access Log (StealthWatch): Unable to connect to remote server for log uploading" 0 E0008:1 alog_facility
ProxyClient	2015-09-17 13:58:19-04:00EDT	"Config admin at 10.89 'admin', access log custom client primary IP address set to "192.168.10.204;8
Network	2015-09-17 13:58:23-04:00EDT	"Access Log Custom (StealthWatch): Connecting to primary server 10.204:8514." 0 E0000:96 alog str
ICAP	2015-09-17 14:00:03-04:00EDT	"Snapshot sysinfo_stats has fetched /sysinfo-stats" 0 200006:96 snapshot_worker.cpp:236
Protocol details	2015-09-17 14:15:03-04:00EDT	"NTP: Periodic query of server .10.10, system clock is 0 seconds 367 ms slow compared to NTP time. Up
System	2015-09-17 14:25:47-04:00EDT	"Config admin at10.89 'admin', installed new VPM Policy File and VPN XML File" 0 140002:7D cli_
Resources	2015-09-17 14:28:21-04:00EDT	"Config admin at .10.89 'admin', installed new VPM Policy File and VPM XML File" 0 140002:7D clip
Contents	2015-09-17 14:33:14-04:00EDT	"Access Log (Stealthwatch2): Configure upload site for uploads to work" O E0006:7D alog facility impl.cp
Event Logging	2015-09-17 14:33:14-04:00EDT	"Access Log (Stealthwatch2): New Log Manager Object created. Max log size is 20000NB, upload threshold is
Failover		"Access Log (Stealthwatch2) has been initialized." O E0000:96 alog facility impl.cpp:269

21. Continue to the <u>Configuring the Flow Collector</u> chapter to set up your Flow Collector to receive syslog information.

## Configuring the McAfee Proxy Logs

This chapter describes the procedure for configuring the McAfee proxy logs from the McAfee Web Gateway to deliver to Secure Network Analytics.

- Be sure that you have downloaded the XML configuration file for the McAfee proxy. Go to the Secure Network Analytics Download and License Center (https://stealthwatch.flexnetoperations.com), to obtain the file and readme, Proxy Log XML Configuration File.
- 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.

"Date" indicates the date of the XML file, and "v" indicates the version of theMcAfee 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://stealthwatch.flexnetoperations.com, the Secure Network Analytics 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.

🐑 Rule Sets
🔂 Log Handler
狗 Error Handler
User Defined Properties

4. Select Log Handler, and then select Default.

Rule Sets	Lists	Settings	
📀 Add 👻	III. 🥔 🛛	× ↑ + 4	
🗄 Rule S	Rule Set		
🔚 Rule S	et from Lib	rary	
🔯 Log H	landler	1	

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.

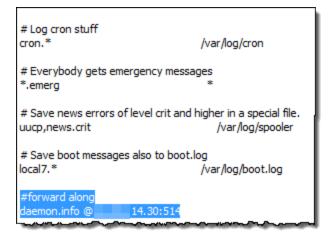
Make sure the rule set and the rule "create access logline" and "send to syslog" is enabled.

- 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.

Appliances	File Editor
Files	
reso reso ripd. ripng rsys	- 11
sshd	_config tl.conf a.conf

10. At the bottom of the text box (beside the list of files), type the follow text:

daemon.info @[FlowCollector IP Address:514]



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.
- 14. Continue to the <u>Configuring the Flow Collector</u> chapter to set up your Flow Collector to receive syslog information.

# Configuring the Cisco Web Security Appliance (WSA) Proxy Logs

This chapter describes the procedure for configuring the Cisco proxy logs to deliver to Secure Network Analytics.

Cisco WSA proxy does not support Virtual IPs for adding the proxy device.

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



1. Log in to the Cisco proxy server.

A	Reporting	Web Security Manager	Security Services	Network	System Administration	
					Policy Trace	
					Alerts	
					Log Subscriptions	
					Return Addresses	

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

Log Subsc	Log Subscriptions			
	Configured Log Subscriptions			
Log Name	Log Name Type Log Files			
access-w3c	access-w3c W3C Logs Syslog Push - Host 10.205.14.30			

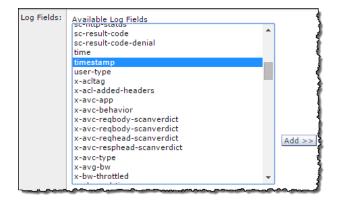
3. Click the Add Log Subscriptions button. The New Log Subscriptions pages opens.

Log Type:	Select a log type	-
	Feedback Logs	
	FIPS Logs	1
	FTP Server Logs	1
	GUI Logs	- 1
	Haystack Logs	_1
	Logging Logs	3
	NTP Logs	1
-	OCSP Logs	ł
	PAC File Hosting Daemon Logs	8
T T	Reporting Logs	1
	Reporting Query Logs	
	SaaS Auth Logs	
_	SHD Logs	1
	SNMP Logs	1
	Status Logs	3
	System Logs	ξ
	UDS Logs	
	Updater Logs	1
	W3C Logs	
	Welcome Page Acknowledgement Logs	1_

4. From the Log Type drop-down list, select W3C Logs. The available W3C Log fields appear.

Log Type:	W3C Logs 🔻	
Log Name:	(will be used to name the log directory)	
Log Fields:	Available Log Fields Selected CMF DCF bytes c-ip c-port cs(Coskie) cs(Coskie) cs(X-Forwarded-For) cs-auth-mechanism cs-bytes cs-method cs-method cs-mine-type cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs-url cs	Log Fields

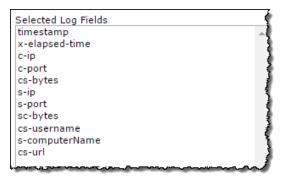
5. In the Log Name field, type a name for the log that you will use.



6. From the Available Log Fields list, select **Timestamp**, and then click **Add** to move it the Select Log Fields list.

- 7. Repeat the previous step for the 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:



The Selected Log Fields list must be in the order above, with no other fields present.

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

	Syslog Push	
	Hostname:	.22.12
	Protocol:	● UDP ○ TCP
	Facility:	user <b>T</b>
_		Submit

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

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.
- 11. Continue to the <u>Configuring the Flow Collector</u> chapter to set up your Flow Collector to receive syslog information.

## Configuring Squid Proxy Logs

This chapter describes the procedure for configuring the Squid proxy logs to deliver to Secure Network Analytics. 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</pre>
```

4. Restart squid using the following:

/etc/init.d/squid3 restart

 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
```

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.
- 7. Continue to the <u>Configuring the Flow Collector</u> chapter to set up your Flow Collector to receive syslog information.

## Configuring the Flow Collector

After you have configured the proxy server, you 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 your Manager.
- 2. Click the 🍄 (Global Settings) icon, then click Central Management.
- 3. Click the **(Ellipsis)** icon for your Flow Collector, then click **View Appliance Statistics**. The Flow Collector interface opens.
- 4. Click **Configuration > Proxy Ingest**. The Proxy Servers page opens.
- 5. Type the IP address of proxy server
- 6. From the Proxy Type drop-down list, select your proxy server.

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

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

### Checking the Flows

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

S.	Support	⊟
	Advanced Settings	
	Database Storage Statistics	
F	Backup/Restore Databas	se
( -	Browse Files	
F	Packet Capture	
	Update	

 In the Flow Collector interface, click Support > Browse Files in the main menu. The Browse Files page opens.

irowse Files (/sw-flow-proxyparser/logs) w-flow-proxyparser/logs					
unowith oxythm services					
nt Directory					
			-		
	<ul> <li>Size</li> </ul>	<ul> <li>Last N</li> </ul>			

2. Open the syslog file.

FlowCollector for NetFlow VE > https://gprocessor.log + +				
A https:// 1.232/swa/files/sw-flow-proxyparser/logs/syslogprocessor.log	🖾 🗵 🖉 🛛 🔍 Search			
🔒 Lancope 🎴 Documentation 🎴 CC-KB 🎴 Demo Servers 🔒 Sandbox Servers 🎴 Videos 🎴 Cisco	🕽 Partners 🦲 Training 🔒 Trial Res 🔒 Tools  Sales 🔒 Security Infe			
2015-06-12 1702111.062 INTO main root - syslopprocessor logping started 2015-06-12 1702111.064 INTO main com.lancope.www.syslopprocess.Configuration - Stript direct 2015-06-12 1702111.064 INTO main com.lancope.www.syslopprocess.Configuration - Log directory 2015-06-12 1702111.064 INTO main com.lancope.www.syslopprocess.Configuration - Log directory 2015-06-12 1702111.064 INTO main com.lancope.www.syslopprocess.Configuration - Log level INT 2015-06-12 1702111.064 INTO main com.lancope.www.syslopprocess.Configuration - Log level INT 2015-06-12 1702111.064 INTO main com.lancope.www.syslopprocess.Configuration - Metrics to co 2015-06-12 1702111.064 INTO main com.lancope.www.syslopprocess.Configuration - Metrics to co 2015-06-12 1702111.064 INTO main com.lancope.www.syslopprocess.Configuration - Metrics to co 2015-06-12 1702111.065 INTO main com.lancope.www.syslopprocess.Configuration - Metrics to co 2015-06-12 1702111.065 INTO main com.lancope.www.syslopprocess.Configuration - Betrics 11 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Betriest 11 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Betriest 11 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Betriester 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Listenser: 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Betriester 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Hastleres: 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Betriester 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Hastleres: 2015-06-12 170211.1065 INTO main com.lancope.www.syslopprocess.Configuration - Hastleres: 2015-06-12 170211.1055 INTO main com.lancope.www.syslopprocess.Configuration - Fisturg / 2015-06-12 170211.1055 INTO main com.lancope.www.syslopprocess.Configuration - Fisturg / 2015-06-12 170211.1055 INTO main com.lancope.www.sysloppr	ory: /lancope/var/sw-flow-proxyparser/templates : false false po nsole: 0 y: 40 T false tion: pot specified tules: true rest table ttics log lancope/var/admin/plugins/firewall/6514-FYFLOG_PARSER			

- 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.

# **Contacting Support**

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

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

# **Copyright Information**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <u>https://www.cisco.com/go/trademarks</u>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)