

Troubleshooting Guide

Cisco Cloud Web Security Troubleshooting Guide

Contents

Introduction	3
Connectivity to the Cloud Web Security Proxy	3
Verifying Connectivity Distinguishing Between ASA and CWS Proxy Problems License Problems	3 4 9
Cisco Cloud Web Security Functions	. 10
Mismatched Time Zones Session Flows	. 11 . 11

Introduction

This document offers tips for resolving common errors that may occur with Cisco[®] Cloud Web Security (CWS) running on the Cisco Adaptive Security Appliance (ASA) Software 9.0. We assume that you are familiar with the Cisco ASA and the CWS connector that runs on it. We also assume that Cisco Cloud Web Security has already been configured on your ASA and you have obtained proper licensing for the Cisco Cloud Web Security administrator portal, Cisco ScanCenter.

For more information about the integration between Cisco Cloud Web Security and the Adaptive Security Appliance, please refer to the ASA configuration guide for Cisco Cloud Web Security at: http://tools.cisco.com/squish/eF3bE.

The following sections cover connectivity from the ASA to the CWS proxy, CWS functions, and user experience. These sections build upon each other, so you should troubleshoot in the order of these sections. You should resolve problems in previous sections before moving on to the next section.

Connectivity to the Cloud Web Security Proxy

CWS will not operate properly if the ASA cannot reach the CWS proxy. This section will help you determine whether the ASA has connectivity to the CWS proxy and possible steps for resolution if the proxy is not reachable.

Verifying Connectivity

To verify connectivity to the proxy, issue the command **show content-scan summary**. As you can see in the configuration that follows, if connectivity is established with the CWS proxy, you should see the word **(REACHABLE)** in parenthesis.

```
ciscoasa(config)# show scansafe server
Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
Backup: proxy137.scansafe.net (80.254.152.99)
```

If instead you are seeing **(UNREACHABLE)** for one of the proxies, the ASA most likely does not have connectivity to that proxy.

```
# sh scansafe server
Primary: proxy555.scansafe.net (NOT RESOLVED) (UNREACHABLE) for last 12 secs,
tried to connect 0 times
Backup: proxy666.scansafe.net (NOT RESOLVED) (UNREACHABLE) for last 12 secs,
tried to connect 0 times
```

You can also establish a Telnet connection to the CWS proxy to test for connectivity. Use a TCP ping to connect the IP address or the fully qualified domain name of the proxy using the port you specified in your configuration. A success rate greater than zero means you have connectivity to the tower; if the success rate is zero, there is no connectivity.

! Connectivity between ASA and ScanSafe Tower
ping tcp proxy197.scansafe.net 8080
Type escape sequence to abort.
No source specified. Pinging from identity interface.

```
Sending 5 TCP SYN requests to 72.37.244.115 port 8080
from xxx.xxx.xxx, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 21/22/23 ms
! No connectivity between ASA and ScanSafe Tower
```

```
# ping tcp proxy197.scansafe.net 8080
```

```
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 72.37.244.115 port 8080
from xxx.xxx.xxx, timeout is 2 seconds:
????
Success rate is 0 percent (0/5)
```

Next Steps:

- Check your routing to make sure your network is able to reach the CWS proxy.
- Make sure there are no firewalls blocking access to the tower.
- If you need to contact support, open a case with the Cisco Technical Assistance Center at: <u>Cisco TAC</u>.

Distinguishing Between ASA and CWS Proxy Problems

If you have verified both proxies are accessible and you can connect with TCP to the proxies but you are getting blank pages when browsing, try to determine if the problem is with the ASA or the CWS proxy. If you need to open a support case, you will receive faster resolution reporting the case to the proper contact (either on the ASA side or the CWS side). To determine the origin of any problems, configure the proxy IP directly on the browser proxy settings to bypass the ASA. This bypass will allow you to determine whether you have an ASA or a proxy problem.

Because you will be bypassing the ASA and thus not using the license configured on it, the tower will not recognize you as an authorized user. To allow the CWS proxy to still recognize the traffic as authorized, you must first add your egress IP address to the list of scanning IPs in ScanCenter. You can find your egress IP address by going to www.whatismyip.com on your computer or client. The following example shows how to add the egress IP address to the CWS list of scanning IPs.

1. In ScanCenter, click the Admin tab, and under the Your account menu, select Scanning IPs.

CISCO Cisco Clou	d Web Sec	urity							Help Logou
	Home	Dashboard	Web Virus	Spyware	Web Filtering	Dead	Admin	Reports	Support
Your account 🔹 Authent	cation 🛃 Man	agement	Audit	4		_	A	-	
Account Details									
Change Password									
Scanning IPs	ore details need to	he amonded also	aca channa ha	low and click	'Enur'				
Admin users	ese details need to	be amended pre	ease change be	IOW and CICK	Jave				
	ACCOUNT OCTAILS						1		

2. Enter the egress IP address in the list with the subnet mask, and click **Submit**.

		Suppo
our account • Au	hentication 4 Management 4 Audit 4	
Request Scanning Ips		
	Enter the IP addresses to scan	
	This form is used to enter and submit updates to be changed for your service IP addresses to be scanned by the service. IP addresses should have format non-non-noninetmask, for example	
	62.56.62.250/255.255.255.255.	
	Be aware that IP addresses in the form of 192.168.*, 10.*, 172.16.* or 169.254* are internal addresses. Note only	
	trame nom external addresses can de scamed.	
	10.1.1.1/255.255.255.255	
	a)	
	a) Reset	
	Reset Sove 1	

3. You will get a confirmation message that the Scanning IPs have been changed.

Your account		Authentication
Scanning IPs		
Scanning IPs have	beer	ı changed

The following example shows how to configure a proxy with Internet Explorer (IE). Steps may vary for other browser versions.

1. On IE, go to **Tools** \rightarrow **Internet Options**.



2. Under the **Connections** tab, click **LAN settings**.

Internet Options	?						
General Security Privacy Content Connections	Programs Advanced						
To set up an Internet connection, click Setup Setup.							
Dial-up and Virtual Private Network settings							
3G Connection	Add						
	Add VPN						
	Remove						
Choose Settings if you need to configure a proxy server for a connection.	Settings						
Never dial a connection							
Dial whenever a network connection is not prese	ent						
Always dial my default connection							
Current None	Set default						
Local Area Network (LAN) settings							
LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.	LAN settings						
Some <u>settings</u> are managed by your system administrator.							
OK Cancel Apply							

3. Under the **Proxy Server** section, check the "Use a proxy server for your LAN" checkbox. Enter the IP address of the CWS proxy under **Address** and the port number under **Port**, and click OK when done.

utomatic coni se of manual	figuration may over settings, disable au	ride man utomatic d	ual setting: configuratio	s. To ensure th
Automatica	ally detect settings			
Use automa	atic configuration <u>s</u> e	ript		
Address]
roxy server	L			
roxy server Use a pro <u>x</u> dial-up or V	y server for your Li /PN connections).	AN (These	e settings (will not apply to
roxy server Use a pro <u>x</u> dial-up or V Addr <u>e</u> ss:	y server for your L/ /PN connections). 72.37.244.115	AN (These Por <u>t</u> :	e settings v 8080	vill not apply to
Toxy server Use a pro <u>x</u> dial-up or V Addr <u>e</u> ss:	y server for your L/ /PN connections). 72.37.244.115 proxy server for lo	AN (These Por <u>t</u> : cal addre	e settings v 8080 Isses	will not apply to

Try browsing to a website now that you are bypassing the ASA. If you are able to browse properly, the problem is most likely with the ASA. Check your configurations and routing. If you are unable to browse, the problem is most likely with the CWS proxy, and you will have to contact your Cisco representatives.

Note: If some users are complaining that their pages are not loading but other users are fine, check to see if the users whose pages are not loading are using a different proxy server instead of going through CWS.

Next Steps:

- If you are able to browse after configuring a proxy on your browser, the problem resides on the ASA side. If you need to contact support, open a case with <u>Cisco TAC</u>.
- If you are unable to browse after configuring a proxy on your browser, the problem resides on the CWS proxy side. If you need to contact support, open a case with <u>Cisco TAC</u>.

License Problems

If you have an invalid CWS license, the **show scansafe server** command may still show REACHABLE for connections to the tower. However, if you have a license problem, when you are browsing you will get a **403 Forbidden** error message similar to the following:



Next Steps:

 Verify that you entered the correct license key information on the ASA with the key provided on the Cisco ScanCenter portal.

- You can also generate and send a new key from ScanCenter in case your key was misconfigured. Details about how to generate and send a key are available in the <u>ScanCenter Administrator Guide</u>.
- If you are unable to obtain a working license or key, contact <u>Cisco TAC</u>.

Cisco Cloud Web Security Functions

This section examines other situations in which users cannot reach websites. We assume in this section that the ASA has connectivity to the CWS proxy. Please refer to the section "Connectivity to the Cloud Web Security Proxy" if you are not certain about the connection.

Remember that you will get a block or warning message from CWS if you are trying to access a blocked or warned site. Displaying this message is one of the Cloud Web Security functions.

A CWS blocked message follows:



A CWS warning message follows; clicking "Accept" allows you to continue to the site.



If users are instead reporting that their webpages are not loading at all (for example, all they see is a blank page), check for the errors described in the following section.

Mismatched Time Zones

Because CWS uses time-based policies, users will not be able to access websites if the time zone on the ASA does not match the time zone on the CWS proxy.

Next Steps:

 The simplest way to solve this problem is to configure the ASA to use a Network Time Protocol (NTP) server:

ntp server 10.0.0.1 source outside prefer

Session Flows

Taking a closer look at session flows can help determine if CWS is redirecting traffic properly. To see the total number of redirected sessions as well as white-listed sessions (which bypass the CWS connector on ASA), use the **show scansafe statistics** command:

show scansafe statistics

```
Current HTTP sessions : 12

Current HTTPS sessions : 0

Total HTTP Sessions : 102

Total HTTPS Sessions : 0

Total Fail HTTP sessions : 0

Total Fail HTTPS sessions : 0

Total Bytes In : 6532 Bytes

Total Bytes Out : 66622 Bytes

HTTP session Connect Latency in ms(min/max/avg) : 0/0/0

HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

As seen in bold in the example configuration, CWS is indeed redirecting traffic to the tower.

show service-policy inspect scansafe

This command shows the number of connections redirected or white-listed by a particular policy. Example output follows:

```
ciscoasa(config)# show service-policy inspect scansafe
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Interface inside:
Service-policy: scansafe-pmap
Class-map: scansafe-cmap
Inspect: scansafe p-scansafe fail-open, packet 0, drop 0, reset-drop 0, v6-fail-
close 0
Number of whitelisted connections: 0
```

```
Number of connections allowed without scansafe inspection because of "fail-open"
config: 0
Number of connections dropped because of "fail-close" config: 0
Number of HTTP connections inspected: 0
Number of HTTPS connections dropped because of errors: 0
Number of HTTPS connections dropped because of errors: 0
```

Next Steps:

As a final check to determine if individual users or entire usergroups are reaching the CWS proxy
properly, ask users to go to http://whoami.scansafe.net/ on their browsers. If CWS is working, they should
see an output with details of their usergroup account obtained from the CWS proxy. An example of the
output follows:

🏉 http://whoami.scansafe.net/ - Windows Internet E	xplorer provided by Cisco	
🔾 🗢 🖻 http://whoami.scansafe.net/	🔹 🗟 😽 🗙 🚰 Google	• م
🚖 Favorites 🏾 🌈 http://whoami.scansafe.net/	🚺 🔹 🖾 👻 🖶 🕈 Page 🕶	Safety 🕶 Tools 🕶 🔞 🕶 🎬
		*
authUserName: ciscouser		
authenticated: true		
companyName: Cisco Systems		
countryCode: US		
externalIp: 76.21.95.1		
groupNames:		
- Demo		
logicalToverNumber: 197		
staticGroupNames:		
- Demo		
- "LDAP://ciscogroup"		
userName: ciscouser		
		*
Done	Internet Protected Mode: Off	
		11

- If redirection to CWS is working and users are still unable to load webpages, you should perform
 debugging on the CWS proxy side, because the connector on the ASA is already functioning properly. If
 you need to contact support, open a case with <u>Cisco TAC</u>.
- If redirection to CWS is not working, you should perform debugging on the ASA side. If you need to contact support, open a case with <u>Cisco TAC</u>.



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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.

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: www.cisco.com/go/trademarks. 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. (1110R)

Printed in USA

Page 13 of 13