Verify SWA Connectivity to the Internet

Contents

Introduction

Prerequisites

- Requirements
- Components Used

CURL

- Verification

SSLTOOL

Telnet

Related Information

Introduction

This document describes the steps to test the Internet connectivity in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Access ToCommand Line Interface (CLI)of SWA.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

CURL

Step 1. Log in to the **CLI** of the SWA.

Step 2. Type **curl** and press enter.

Step 3. Choose **DIRECT**, to test the SWA Internet access without any proxy policy being applied to the traffic.

Step 4. Type "**y**" as the answer to **Do you wish to choose particular interface of appliance?** and press **Enter**.

Step 5. Type the number associated to the interface that has Internet access.

Step 6. Enter the URL for testing and press **Enter**.

Note: Make sure the URL starts with **HTTP://** or **HTTPS://**

```
SWA_CLI> curl

Choose the operation you want to perform:
- DIRECT - URL access going direct
- APPLIANCE - URL access through the Appliance
[]> DIRECT

Do you wish to choose particular interface of appliance?
[N]> y

1. Management
2. P1
3. P2
Enter the interface number:
[1]> 3

Enter URL to make request to
[]> http://www.cisco.com
```

Verification

You can review the HTTP response code. In this example the HTTP response code is 200, which means the connection was established.

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     015:34:55.026472 *   Tryin
15:34:55.026645 * Local Interface nic0 is ip 10.1.1.1 using address family 2
15:34:55.026676 * Local port: 0
15:34:55.035164 * Connected to www.cisco.com (10.18.27.120) port 80 (#0)
15:34:55.035202 > HEAD / HTTP/1.1
15:34:55.035202 > Host: www.cisco.com
15:34:55.035202 > User-Agent: curl/7.74.0
15:34:55.035202 > Accept: */*
15:34:55.035202 >
15:34:55.056382 * Mark bundle as not supporting multiuse
15:34:55.056397 < HTTP/1.1 200 OK
15:34:55.056429 < Date: Thu, 19 Mar 2026 19:34:54 GMT
15:34:55.056451 < Content-Type: text/html
15:34:55.056474 < Connection: keep-alive
15:34:55.056490 < CF-RAY: 9deeead18c0b253f-ORD
15:34:55.056515 < Last-Modified: Wed, 18 Mar 2026 19:14:43 GMT
15:34:55.056538 < Allow: GET, HEAD
15:34:55.056562 < Accept-Ranges: bytes
15:34:55.056583 < Age: 2119
15:34:55.056606 < cf-cache-status: HIT
15:34:55.056619 < Server: cloudflare
15:34:55.056639 <
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

```
15:34:55.056723 * Connection #0 to host www.cisco.com left intact
```

In this example you can see SWA was not able to access the URL.

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     015:38:29.520762 *   Tryin
15:38:29.520927 *   Trying 10.18.26.120:443...

15:38:29.521068 * Closing connection 0
curl: (7) Couldn't connect to server
```

SSLTOOL

The **ssltool,** is CLI version of **openssl s_client** command. It connects to a remote host using SSL/TLS directly without using Secure Web Appliance proxy policies.

Step 1. Log in to the CLI of the SWA.

Step 2. Type **ssltool** and press enter.

Step 3. Type **SCLIENT** and press enter

Step 4. Type **COMMAND** and press enter.

Tip: You can type HELP and press enter to read more information about this command.

Step 5. Enter your **openssl** command and press **Enter**.

```
SWA_CLI> ssltool

Choose the operation you want to perform:
- SCLIENT - This is CLI version of openssl s_client command. It will connect to a remote host using SSL
- CLEARLOGS - Delete all logs generated by ssltool
[]> SCLIENT

Choose the operation you want to perform:
- COMMAND - Execute an openssl s_client command
- HELP - Help information about this command
[]> COMMAND

Enter an openssl command for example: 'openssl s_client -connect www.cisco.com:443' or hit enter to go
[]>
```

Telnet

Note: The **telnet** command has been removed from SWA version 15.0 and newer.

Step 1. Log in to the CLI of the SWA.

Step 2. Type **telnet** and press enter.

Step 3. Type the number associated to the interface that has Internet access.

Step 4. Enter the remote hostname or IP address.

Step 5. you can type 80 or 443 in the answer to **Enter the remote port**, to test the TCP connectivity to HTTP or HTTPS port of the remote host.

Step 6. To exit the **telnet** hold the Control key and press **]** .

```
SWA_CLI> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (10.48.48.183/24: man-wsa125.amojarra.local)
3. P1 (10.10.10.10/24: p1-wsa125.amojarra.local)
4. P2 (10.20.20.20/24: p2-wsa125.amojarra.local)
[1]>4

Enter the remote hostname or IP address.
[]> cisco.com

Enter the remote port.
[23]> 8443

Trying 10.20.3.15...
Connected to 10.20.3.15.
Escape character is '^]'.
```

Related Information

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance
- Secure Web Appliance Initial Setup
- Cisco Secure Email and Web Virtual Appliance Installation Guide
- Configure Custom URL Categories in Secure Web Appliance - Cisco
- Use Secure Web Appliance Best Practices