

Verificar la conectividad de SWA a Internet

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[RIZAR](#)

[Verificación](#)

[SSLTOOL](#)

[TELNET](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos para probar la conectividad a Internet en Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz de línea de comandos (CLI) de SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

RIZAR

Paso 1. Inicie sesión en la CLI del SWA.

Paso 2. Escriba curl y presione Enter.

Paso 3. Elija DIRECT, para probar el acceso a Internet SWA sin aplicar ninguna política de proxy

al tráfico.

Paso 4. Escriba "y" como respuesta a ¿Desea elegir una interfaz concreta del dispositivo? y pulse Intro.

Paso 5. Escriba el número asociado a la interfaz que tiene acceso a Internet.

Paso 6. Introduzca la URL para la prueba y pulse Intro.



Nota: Asegúrese de que la URL comienza con HTTP:// o 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
```

Verificación

Puede revisar el código de respuesta HTTP. En este ejemplo, el código de respuesta HTTP es 200, lo que significa que se estableció la conexión.

```
% Total    % Received % Xferd  Average Speed   Time    Time       Time  Current
           0         0         0             0      0:00:00     0:00:00     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

```

En este ejemplo, puede ver que SWA no pudo acceder a la URL.

```

% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
  0      0      0      0      0      0      0      0  --:--:--  --:--:--  --:--:--      0  15:38:29.520762 * Trying
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

La `ssltool`, es la versión CLI del comando `openssl s_client`. Se conecta a un host remoto mediante SSL/TLS directamente sin utilizar las políticas de proxy del dispositivo web seguro.

Paso 1. Inicie sesión en la CLI del SWA.

Paso 2. Escriba `ssltool` y presione Enter.

Paso 3. Escriba `SCLIENT` y presione Intro

Paso 4. Escriba `COMMAND` y presione Enter.

 Consejo: Puede escribir AYUDA y presionar Entrar para obtener más información acerca de este comando.

Paso 5. Ingrese su comando `openssl` y presione 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



Nota: El comando telnet se ha eliminado de la versión SWA 15.0 y posterior.

Paso 1. Inicie sesión en la CLI del SWA.

Paso 2. Escriba telnet y presione Intro.

Paso 3. Escriba el número asociado a la interfaz que tiene acceso a Internet.

Paso 4. Introduzca el nombre de host remoto o la dirección IP.

Paso 5. puede escribir 80 o 443 en la respuesta para Ingrese el puerto remoto, para probar la conectividad TCP con el puerto HTTP o HTTPS del host remoto.

Paso 6. Para salir de telnet, mantenga presionada la tecla Control y presione] .

```
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 '^'.

Información Relacionada

- [Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Configuración inicial del dispositivo web seguro](#)
- [Guía de instalación de Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco](#)
- [Uso de las prácticas recomendadas de Secure Web Appliance](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).