

Verifica della connettività SWA a Internet

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[ARRICCIATURA](#)

[Verifica](#)

[SSLTOOL](#)

[Telnet](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come verificare la connettività Internet in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia della riga di comando (CLI) di SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

ARRICCIATURA

Passaggio 1. Accedere alla CLI dell'SWA.

2. Digitare curl e premere Invio.

Passaggio 3. Scegliere DIRECT per verificare l'accesso a Internet dell'SWA senza applicare alcuna policy proxy al traffico.

Passaggio 4. Digitare "y" come risposta per Scegliere una particolare interfaccia dell'accessorio? e premere Invio.

Passaggio 5. Digitare il numero associato all'interfaccia con accesso a Internet.

Passaggio 6. Immettere l'URL per il test e premere Invio.



Nota: Verificare che l'URL inizi 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
```

Verifica

È possibile esaminare il codice di risposta HTTP. In questo esempio, il codice di risposta HTTP è 200, che indica che la connessione è stata stabilita.

```
% Total    % Received % Xferd  Average Speed   Time    Time       Time  Current
           Dload  Upload   Total     Spent    Left     Speed

  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: 9deead18c0b253f-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 --:--:-- --:--:-- --:--:--    0
15:34:55.056723 * Connection #0 to host www.cisco.com left intact

```

Nell'esempio viene mostrato come SWA non sia in grado di accedere all'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

Il comando `ssltool`, è la versione CLI del comando `openssl s_client`. Si connette a un host remoto utilizzando direttamente SSL/TLS senza utilizzare i criteri proxy di Secure Web Appliance.

Passaggio 1. Accedere alla CLI dell'SWA.

Passaggio 2. Digitare `ssltool` e premere Invio.

Passaggio 3. Digitare `SCLIENT` e premere Invio

Passaggio 4. Digitare `COMMAND` e premere Invio.



Suggerimento: Per ulteriori informazioni sul comando, digitare `HELP` e premere invio.

Passaggio 5. Immettere il comando `openssl` e premere Invio.

```
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: il comando telnet è stato rimosso dalla versione SWA 15.0 e successive.

Passaggio 1. Accedere alla CLI dell'SWA.

Passaggio 2. Digitare telnet e premere Invio.

Passaggio 3. Digitare il numero associato all'interfaccia con accesso a Internet.

Passaggio 4. Immettere il nome host remoto o l'indirizzo IP.

Passaggio 5. È possibile digitare 80 o 443 nella risposta Immettere la porta remota, per verificare la connettività TCP alla porta HTTP o HTTPS dell'host remoto.

Passaggio 6. Per uscire dal telnet tenere premuto il tasto Ctrl e premere ] .

```
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 '^['.
```

## Informazioni correlate

- [Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance](#)
- [Installazione iniziale di Secure Web Appliance](#)

- [Guida all'installazione di Cisco Secure Email e Web Virtual Appliance](#)
- [Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco](#)
- [Utilizzare le procedure ottimali per Secure Web Appliance](#)

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).