

SWA-verbinding met internet controleren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[KRULLEN](#)

[Verificatie](#)

[SSLTOOL](#)

[Telnet](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven voor het testen van de internetverbinding in Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot de Command Line Interface (CLI) van SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

KRULLEN

Stap 1. Log in op de CLI van de SWA.

Stap 2. Typ curl en druk op enter.

Stap 3. Kies DIRECT om de SWA-internettoegang te testen zonder dat er een proxybeleid op het verkeer wordt toegepast.

Stap 4. Typ "y" als antwoord op Wilt u een bepaalde interface van het toestel kiezen? en druk op Enter.

Stap 5. Typ het nummer dat is gekoppeld aan de interface met internettoegang.

Stap 6. Voer de URL in voor het testen en druk op Enter.



Opmerking: zorg ervoor dat de URL begint met HTTP:// of 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
```

Verificatie

U kunt de HTTP-antwoordcode bekijken. In dit voorbeeld is de HTTP-antwoordcode 200, wat betekent dat de verbinding tot stand is gebracht.

```
% Total    % Received % Xferd  Average Speed   Time    Time       Time  Current
           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: 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
15:34:55.056723 * Connection #0 to host www.cisco.com left intact

```

In dit voorbeeld kunt u zien dat SWA geen toegang had tot de 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

De `ssltool` is de CLI-versie van `openssl s_client` opdracht. Het maakt rechtstreeks verbinding met een externe host met behulp van SSL/TLS zonder het proxybeleid van Secure Web Appliance te gebruiken.

Stap 1. Log in op de CLI van de SWA.

Stap 2. Typ `ssltool` en druk op enter.

Stap 3. Typ `SCLIENT` en druk op enter

Stap 4. Typ `COMMAND` en druk op enter.



Tip: U kunt `HELP` typen en op Enter drukken om meer informatie over deze opdracht te lezen.

Stap 5. Voer uw `openssl`-opdracht in en druk op 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



Opmerking: De telnet-opdracht is verwijderd uit SWA versie 15.0 en nieuwer.

Stap 1. Log in op de CLI van de SWA.

Stap 2. Typ telnet en druk op enter.

Stap 3. Typ het nummer dat is gekoppeld aan de interface met internettoegang.

Stap 4. Voer de externe hostnaam of het IP-adres in.

Stap 5. u kunt 80 of 443 typen in het antwoord om de externe poort in te voeren, om de TCP-connectiviteit met de HTTP- of HTTPS-poort van de externe host te testen.

Stap 6. Om het telnet af te sluiten houdt u de Control-toets ingedrukt en drukt u op ] .

```
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 '^]'.
```

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance](#)

- [Beveiligde eerste installatie van webtoestel](#)
- [Installatiehandleiding voor Cisco Secure Email and Web Virtual Appliance](#)
- [Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco](#)
- [Best practices voor veilige webapparaten gebruiken](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.