

Überprüfen der SWA-Internetverbindung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[CURL](#)

[Verifizierung](#)

[WERKZEUG](#)

[Telnet](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte zum Testen der Internetverbindung in der Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die Befehlszeilenschnittstelle (CLI) von SWA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

CURL

Schritt 1: Melden Sie sich bei der CLI der SWA an.

Schritt 2. Geben Sie curl ein, und drücken Sie die Eingabetaste.

Schritt 3: Wählen Sie DIRECT aus, um den SWA-Internetzugriff zu testen, ohne dass eine Proxy-Richtlinie auf den Datenverkehr angewendet wird.

Schritt 4. Geben Sie "y" als Antwort auf Möchten Sie eine bestimmte Schnittstelle der Appliance auswählen? und drücke die Eingabetaste.

Schritt 5: Geben Sie die Nummer ein, die der Schnittstelle mit Internetzugang zugeordnet ist.

Schritt 6: Geben Sie die URL für den Test ein und drücken Sie die Eingabetaste.



Anmerkung: Stellen Sie sicher, dass die URL mit HTTP:// oder HTTPS:// beginnt.

```
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
```

Verifizierung

Sie können den HTTP-Antwortcode überprüfen. In diesem Beispiel lautet der HTTP-Antwortcode 200, was bedeutet, dass die Verbindung hergestellt wurde.

```
% Total    % Received % Xferd  Average Speed   Time    Time       Time  Current
           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 diesem Beispiel sehen Sie, dass SWA nicht auf die URL zugreifen konnte.

```

% 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

```

WERKZEUG

Das `ssltool` ist die CLI-Version des Befehls `openssl s_client`. Er stellt über SSL/TLS eine direkte Verbindung zu einem Remote-Host her, ohne die Proxyrichtlinien der sicheren Webappliance zu verwenden.

Schritt 1: Melden Sie sich bei der CLI der SWA an.

Schritt 2. Geben Sie `ssltool` ein, und drücken Sie die Eingabetaste.

Schritt 3. Geben Sie `SCLIENT` ein, und drücken Sie die Eingabetaste.

Schritt 4. Geben Sie `COMMAND` ein, und drücken Sie die Eingabetaste.

 **Tipp:** Sie können `HELP` eingeben und die Eingabetaste drücken, um weitere Informationen zu diesem Befehl anzuzeigen.

Schritt 5: Geben Sie den Befehl `openssl` ein, und drücken Sie die Eingabetaste.

```
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

---

 Hinweis: Der Telnet-Befehl wurde aus SWA Version 15.0 und neueren Versionen entfernt.

---

Schritt 1: Melden Sie sich bei der CLI der SWA an.

Schritt 2. Geben Sie telnet ein, und drücken Sie die Eingabetaste.

Schritt 3: Geben Sie die Nummer ein, die der Schnittstelle mit Internetzugang zugeordnet ist.

Schritt 4: Geben Sie den Namen oder die IP-Adresse des Remote-Hosts ein.

Schritt 5. Sie können 80 oder 443 in die Antwort Geben Sie den Remote-Port ein eingeben, um die TCP-Verbindung zum HTTP- oder HTTPS-Port des Remote-Hosts zu testen.

Schritt 6: Um das Telnet zu verlassen, halten Sie die Strg -Taste gedrückt und drücken Sie ] .

```
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 '^]'.
```

Zugehörige Informationen

- [Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance](#)

- [Ersteinrichtung der sicheren Web-Appliance](#)
- [Installationsleitfaden für die Cisco Secure Email und Web Virtual Appliance](#)
- [Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco](#)
- [Best Practices für sichere Web-Appliances](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.