

Vérification de la connectivité SWA à Internet

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[BOUCLER](#)

[Vérification](#)

[OUTIL À CLAPET](#)

[Telnet](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes à suivre pour tester la connectivité Internet dans Secure Web Appliance (SWA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface de ligne de commande (CLI) de SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

BOUCLER

Étape 1. Connectez-vous à l'interface CLI du SWA.

Étape 2. Tapez curl et appuyez sur Entrée.

Étape 3. Choisissez DIRECT, pour tester l'accès Internet SWA sans qu'aucune stratégie de proxy ne soit appliquée au trafic.

Étape 4. Entrez « y » comme réponse à la question « Souhaitez-vous choisir une interface particulière de l'appliance ? et appuyez sur Entrée.

Étape 5. Tapez le numéro associé à l'interface disposant d'un accès Internet.

Étape 6. Entrez l'URL de test et appuyez sur Entrée.



Remarque : Assurez-vous que l'URL commence par HTTP:// ou 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
```

Vérification

Vous pouvez consulter le code de réponse HTTP. Dans cet exemple, le code de réponse HTTP est 200, ce qui signifie que la connexion a été établie.

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

```

Dans cet exemple, vous pouvez voir que SWA n'a pas pu accéder à l'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  015:38:29.520762 *    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

```

OUTIL À CLAPET

Le `ssltool` est la version CLI de la commande `openssl s_client`. Il se connecte directement à un hôte distant à l'aide de SSL/TLS sans utiliser de stratégies proxy Secure Web Appliance.

Étape 1. Connectez-vous à l'interface de ligne de commande du SWA.

Étape 2. Tapez `ssltool` et appuyez sur Entrée.

Étape 3. Tapez `SCLIENT` et appuyez sur Entrée

Étape 4. Tapez `COMMAND` et appuyez sur Entrée.

 Conseil : Vous pouvez taper `HELP` et appuyer sur Entrée pour obtenir plus d'informations sur cette commande.

Étape 5. Entrez la commande `openssl` et appuyez sur Entrée.

```
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



Remarque : la commande telnet a été supprimée de SWA version 15.0 et ultérieure.

Étape 1. Connectez-vous à l'interface de ligne de commande du SWA.

Étape 2. Tapez telnet et appuyez sur Entrée.

Étape 3. Tapez le numéro associé à l'interface disposant d'un accès Internet.

Étape 4. Entrez le nom d'hôte ou l'adresse IP distante.

Étape 5. Vous pouvez taper 80 ou 443 dans la réponse à Enter the remote port, pour tester la connectivité TCP au port HTTP ou HTTPS de l'hôte distant.

Étape 6. Pour quitter telnet, maintenez la touche Ctrl enfoncée et appuyez sur] .

```
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 '^['.
```

Informations connexes

- [Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance](#)
- [Configuration initiale de Secure Web Appliance](#)

- [Guide d'installation de l'appliance virtuelle Cisco Secure Email and Web](#)
- [Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco](#)
- [Utilisation des meilleures pratiques de sécurisation des appliances Web](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.