

Verificar a conectividade SWA com a Internet

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[CURL](#)

[Verificação](#)

[FERRAMENTAS](#)

[Telnet](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para testar a conectividade com a Internet no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface de linha de comando (CLI) do SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

CURL

Etapa 1. Faça login na CLI do SWA.

Etapa 2. Digite curl e pressione enter.

Etapa 3. Escolha DIRECT para testar o acesso SWA à Internet sem que nenhuma política de proxy seja aplicada ao tráfego.

Etapa 4. Digite "y" como a resposta para Você deseja escolher uma interface específica do dispositivo? e pressione Enter.

Etapa 5. Digite o número associado à interface que tem acesso à Internet.

Etapa 6. Insira o URL para teste e pressione Enter.



Note: Verifique se a URL começa com 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
```

Verificação

Você pode revisar o código de resposta HTTP. Neste exemplo, o código de resposta HTTP é 200, o que significa que a conexão foi estabelecida.

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

```

Neste exemplo, você pode ver que o SWA não pôde acessar a 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

```

FERRAMENTASSLN

O ssltool é uma versão CLI do comando openssl s_client. Ele se conecta a um host remoto usando SSL/TLS diretamente sem usar políticas de proxy do Secure Web Appliance.

Etapa 1. Efetue login no CLI do SWA.

Etapa 2. Digite ssltool e pressione enter.

Etapa 3. Digite SCLIENT e pressione enter

Etapa 4. Digite COMMAND e pressione enter.



Tip: Você pode digitar HELP e pressionar enter para ler mais informações sobre esse comando.

Etapa 5. Digite o comando openssl e pressione 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



Observação: o comando telnet foi removido do SWA versão 15.0 e mais recente.

Etapa 1. Efetue login no CLI do SWA.

Etapa 2. Digite telnet e pressione enter.

Etapa 3. Digite o número associado à interface que tem acesso à Internet.

Etapa 4. Digite o nome do host remoto ou o endereço IP.

Etapa 5. você pode digitar 80 ou 443 na resposta para Enter the remote port, para testar a conectividade TCP para a porta HTTP ou HTTPS do host remoto.

Etapa 6. Para sair do telnet mantenha pressionada a tecla Control e pressione].

```
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 '^['.
```

Informações Relacionadas

- [Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Configuração inicial do Secure Web Appliance](#)

- [Guia de instalação do Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco](#)
- [Use as práticas recomendadas de dispositivos da Web seguros](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.