检验SWA与Internet的连接

目录

简介

先决条件

- 要求
- 使用的组件

卷曲

- 确认

ssltool

Telnet

相关信息

简介

本文档介绍在安全Web设备(SWA)中测试Internet连接的步骤。

先决条件

要求

思科建议了解以下主题：

- 访问SWA的命令行界面(CLI)。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

卷曲

步骤1.登录到SWA的CLI。

步骤2.键入curl并按Enter。

第3步：选择DIRECT，以测试SWA Internet访问，而不对流量应用任何代理策略。

步骤4.键入y作为Do you want to choose specific interface of appliance?并按Enter。

步骤5.键入与能访问Internet的接口关联的编号。

步骤6.输入用于测试的URL，然后按Enter键。

注意：输入以http://或https://开头的URL。

```
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
```

确认

您可以查看HTTP响应代码。在本示例中，HTTP响应代码为200，这意味着已建立连接。

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  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: 9deeead18c0b253f-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
```

在本示例中，您可以看到SWA无法访问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

ssltool是openssl s_client命令的CLI版本。它使用SSL/TLS直接连接到远程主机，而不使用安全Web设备代理策略。

步骤1.登录到SWA的CLI。

步骤2.键入ssltool并按Enter。

步骤3.键入SCLIENT，然后按Enter

步骤4.键入COMMAND并按Enter。

提示：您可以键入HELP并按enter阅读有关此命令的详细信息。

步骤5.键入openssl命令并按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

注意：telnet命令已从SWA版本15.0及更高版本中删除。

步骤1.登录到SWA的CLI。

步骤2.键入telnet并按Enter。

步骤3.键入与能访问Internet的接口关联的编号。

步骤4.输入remote hostname或IP地址。

步骤5.可以在Enter the remote port提示符处输入80或443，以测试通过HTTP或HTTPS到远程主机的TCP连接。

步骤6.要退出telnet，请按住Control键并按enter。

```
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 '^]'.
```

相关信息

思科安全Web设备AsyncOS 15.2用户指南

安全Web设备初始设置

思科安全邮件和Web虚拟设备安装指南

在安全Web设备中配置自定义URL类别 — 思科

使用安全Web设备最佳实践

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。