思科ESA/WSA/SMA遠端訪問常見問題技術說明

目錄

簡介

本文檔回答了有關思科內容安全裝置上的思科技術支援使用遠端訪問的常見問題。 其中包括思科電子郵件安全裝置(ESA)、思科網路安全裝置(WSA)和思科安全管理裝置(SMA)。

必要條件

採用元件

本文檔中的資訊基於運行任何AsyncOS版本的思科內容安全裝置。

什麼是遠端訪問？

遠端訪問是從思科內容安全裝置到思科安全主機的安全外殼(SSH)連線。 啟用遠端會話後，只有思科客戶協助才能訪問裝置。 遠端訪問允許思科客戶支援分析裝置。 支援人員通過此過程在裝置和upgrades.ironport.com伺服器之間建立的SSH隧道訪問裝置。

遠端訪問的工作原理

當遠端訪問連線啟動時，裝置會通過裝置上的SSH連線開啟一個安全、隨機、高源埠，該埠連線到以下思科內容安全伺服器之一已配置/選定的埠：

IP 位址	主機名	使用
63.251.108.107	upgrades.ironport.com	所有內容安全裝置
63.251.108.107	c.tunnels.ironport.com	C系列裝置(ESA)
63.251.108.107	x.tunnels.ironport.com	X系列裝置(ESA)
63.251.108.107	m.tunnels.ironport.com	M系列裝置(SMA)
63.251.108.107	s.tunnels.ironport.com	S系列裝置(WSA)

必須注意的是，可能需要將客戶防火牆配置為允許到上面列出的其中一個伺服器的出站連線。如果防火牆已啟用SMTP協定檢查，則不會建立通道。思科將接受來自裝置的連線以進行遠端訪問的埠包括：

- 22
- 25（預設）
- 53
- 80
- 443
- 4766

遠端訪問連線到主機名而不是硬編碼IP地址。 這要求在裝置上配置域名伺服器(DNS)以建立出站連線。

在客戶網路中，由於協定/埠不匹配，某些協定感知網路裝置可能會阻止此連線。 某些感知簡單郵件傳輸協定(SMTP)的裝置也可能中斷連線。在有協定感知裝置或出站連線被阻塞的情況下，可能需要使用除預設埠(25)之外的埠。只有思科客戶支援才能訪問隧道的遠端端。 在嘗試建立裝置的遠端訪問連線或對其進行故障排除時，請確保檢視防火牆/網路的出站連線。

> **附註**：思科客戶支援工程師通過遠端訪問連線到裝置時，裝置上的系統提示符會顯示*(SERVICE)*。

如何啟用遠端訪問

> **附註**：請務必檢視裝置和AsyncOS版本的使用手冊，瞭解有關「為思科技術支援人員啟用遠端訪問」的說明。

> **附註**：透過電子郵件傳送至attach@cisco.com的附件可能在傳送過程中不安全。支援案件管理器是思科將資訊上傳到案件的首選安全選項。要瞭解有關其他檔案上傳選項的安全性和大小限制的更多資訊，請執行以下操作：客戶檔案上傳至 Cisco 技術援助中心

確定可以從Internet訪問的埠。預設值為埠25，在大多數環境中均可使用，因為系統還需要通過該埠進行常規訪問才能傳送電子郵件。大多數防火牆配置都允許通過此埠進行連線。

CLI

要通過CLI建立遠端訪問連線，請以管理員使用者身份完成以下步驟：

1. 輸入**techsupport**命令
2. 選擇**TUNNEL**
3. 選擇生成或*輸入*隨機種子字串

4. 指定連線的埠號
5. 回覆「Y」以啟用服務訪問

此時將啟用遠端訪問。 裝置現在用於建立與思科安全防禦主機的安全連線。 提供裝置序列號以及向支援您的案例的TAC工程師生成的種子字串。

GUI

為了通過GUI建立遠端訪問連線，請以管理員使用者的身份完成以下步驟：

1. 導航到**幫助和支援>遠端訪問**（對於ESA、SMA）、支援和幫助>遠端訪問（**對於WSA**），**導航到Help and Support（對於WSA）**
2. 按一下**「Enable」**
3. 選擇種子字串的方法
4. 確保選中*Initiate connection via secure tunnel*覈取方塊並指定連線的埠號
5. 按一下**Submit**

此時將啟用遠端訪問。 裝置現在用於建立與思科安全防禦主機的安全連線。 提供裝置序列號以及向支援您的案例的TAC工程師生成的種子字串。

如何禁用遠端訪問

CLI

1. 輸入**techsupport**命令
2. 選擇**DISABLE**
3. 在提示「Are you sure to disable service access？」時回覆「Y」

GUI

1. 導航到**幫助和支援>遠端訪問**（對於ESA、SMA）、支援和幫助>遠端訪問（**對於WSA**）。
2. 按一下**「Disable」**
3. GUI輸出將顯示「Success — Remote Access has been disabled」

如何測試遠端訪問連線

使用以下示例對從裝置到思科的連線執行初始測試：

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

可對上面列出的任何埠進行連通性測試：22、25、53、80、443或4766。 如果連線失敗，您可能需要運行資料包捕獲，檢視從您的裝置/網路進行連線的故障位置。

為什麼遠端訪問在SMA上不起作用？

如果SMA位於本地網路中，不能直接訪問網際網路，則可能無法在SMA上啟用遠端訪問。 例如，可以在ESA或WSA上啟用遠端訪問，並且可以在SMA上啟用SSH訪問。這樣，思科支援人員可以首先通過遠端訪問連線到ESA/WSA，然後通過SSH從ESA/WSA連線到SMA。 這將需要連線埠22上的ESA/WSA和SMA。

> **附註**：請務必檢視裝置使用手冊和AsyncOS版本，瞭解有關「啟用對沒有直接網際網路連線的裝置的遠端訪問」的說明。

CLI

要通過CLI建立遠端訪問連線，請以管理員使用者身份完成以下步驟：

1. 輸入**techsupport**命令
2. 選擇**SSHACCESS**
3. 選擇生成或*輸入*隨機種子字串
4. 回覆「**Y**」以啟用服務訪問

此時將啟用遠端訪問。 CLI輸出將顯示種子字串。 請將此資料提供給思科客戶支援工程師。 CLI輸出還將顯示連線狀態和遠端訪問詳細資訊，包括裝置序列號。 請將此序列號提供給客戶客戶支援工程師。

GUI

為了通過GUI建立遠端訪問連線，請以管理員使用者的身份完成以下步驟：

1. 導航到**幫助和支援>遠端訪問**（對於ESA、SMA）、支援和幫助>遠端訪問（**對於WSA**），**導航到Help and Support（對於WSA）**
2. 按一下**「Enable」**
3. 選擇種子字串的方法
4. 請勿選中*Initiate connection via secure tunnel*覈取方塊
5. 按一下**Submit**

此時將啟用遠端訪問。 GUI輸出將顯示成功消息和裝置的種子字串。 請將此資料提供給思科客戶支援工程師。 GUI輸出還將顯示連線狀態和遠端訪問詳細資訊，包括裝置序列號。 請將此序列號提供給客戶客戶支援工程師。

如何為SSHACCESS啟用時禁用遠端訪問

為SSHACCESS禁用遠端訪問與上面提供的步驟相同。

疑難排解

如果裝置無法啟用遠端訪問並通過列出的埠之一連線到upgrades.ironport.com，則需要直接從裝置運行資料包捕獲，以檢視導致出站連線失敗的原因。

> **附註**：請務必檢視裝置使用手冊和AsyncOS版本，以瞭解有關「運行資料包捕獲」的說明。

思科客戶支援工程師可能要求提供.pcap檔案，以便檢視和協助進行疑難排解。

相關資訊

- ESA常見問題：ESA提供哪些管理訪問級別？
- 思科電子郵件安全裝置產品支援
- Cisco Web Security產品支援
- 思科內容安全管理裝置產品支援
- 技術支援與文件 - Cisco Systems