

排除FTD上常見的AnyConnect通訊問題

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[建議的故障排除過程](#)

[AnyConnect客戶端無法訪問內部資源](#)

[AnyConnect客戶端不能訪問Internet](#)

[AnyConnect客戶端無法相互通訊](#)

[AnyConnect客戶端無法建立電話呼叫](#)

[AnyConnect客戶端可以建立電話呼叫，但是呼叫沒有音訊](#)

[相關資訊](#)

簡介

本文描述當使用Firepower威脅防禦(FTD)的Cisco AnyConnect安全移動客戶端(FTD)的安全套接字層(SSL)或網際網路金鑰交換版本2(IKEv2)時，如何解決一些最常見的通訊問題。

作者：Angel Ortiz和Fernando Jimenez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco AnyConnect Security Mobility Solution — 遠端存取。
- Cisco FTD。
- Cisco Firepower Management Center(FMC)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 由FMC 6.4.0管理的FTD。
- AnyConnect 4.8。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

建議的故障排除過程

本指南說明如何排解AnyConnect使用者端將FTD用作遠端存取虛擬私人網路(VPN)閘道時的一些常見通訊問題。以下各節針對以下問題提供解決方案：

- AnyConnect客戶端無法訪問內部資源。
- AnyConnect客戶端不能訪問Internet。
- AnyConnect客戶端無法相互通訊。
- AnyConnect客戶端無法建立電話呼叫。
- AnyConnect客戶端可以建立電話呼叫。但是，呼叫中沒有音訊。

AnyConnect客戶端無法訪問內部資源

請完成以下步驟：

步驟1.驗證分割隧道配置。

- 導航到AnyConnect客戶端所連線的連線配置檔案：**Devices > VPN > Remote Access > Connection Profile > Select the Profile.**
- 導航到分配給該Profile: 的組策略**編輯組策略>常規。**
- 檢查分割隧道配置，如下圖所示。

Edit Group Policy

The screenshot shows the 'Edit Group Policy' window with the following configuration:

- Name: Anyconnect_GroupPolicy
- Description: (empty)
- General tab selected
- VPN Protocols: (empty)
- IP Address Pools: (empty)
- Banner: (empty)
- DNS/WINS: (empty)
- Split Tunneling:
 - IPv4 Split Tunneling: Tunnel networks specified below
 - IPv6 Split Tunneling: Tunnel networks specified below
 - Split Tunnel Network List Type: Standard Access List Extended Access List
 - Standard Access List: Split-tunnel-ACL
 - DNS Request Split Tunneling:
 - DNS Requests: Send DNS requests as per split tunnel policy
 - Domain List: (empty)

- 如果將其設定為如下**指定的通道網路**，請確認存取控制清單(ACL)組態：
導航到**Objects > Object Management > Access List > Edit the Access List for Split tunneling.**
- 確保您嘗試從AnyConnect VPN客戶端到達的網路列在該訪問清單中，如下圖所示。

Edit Standard Access List Object

? X

Name: Split-tunnel-ACL

Entries (1)

Sequence No	Action	Network
1	✓ Allow	InternalNetwork1 InternalNetwork2 InternalNetwork3

Allow Overrides

Save Cancel

步驟2. 驗證網路地址轉換(NAT)免除配置。

請記住，我們必須配置NAT免除規則以避免將流量轉換為介面IP地址，該介面通常配置為用於網際網路訪問(使用埠地址轉換(PAT))。

- 導航到NAT配置：**Devices > NAT**。
- 確保為正確的源（內部）和目標（AnyConnect VPN池）網路配置NAT免除規則。此外，請確認是否已選取正確的來源介面和目的地介面，如下圖所示。

#..	Dire...	Ty...	Original Packet		Translated Packet		T.. Options S..		
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations		O... Translated S... Sources	Translated Destinations
1	Sta...		Inside_interface	outside_interface	InternalNetworksGroup	Anyconnect_Pool	InternalNetworksGroup	Anyconnect_Pool	Dns:false route-lookup no-proxy-arp

附註：配置NAT免除規則時，請檢查no-proxy-arp並執行route-lookup選項作為最佳實踐。

步驟3. 驗證訪問控制策略。

根據您的訪問控制策略配置，確保允許來自AnyConnect客戶端的流量到達選定的內部網路，如下圖所示。



AnyConnect客戶端不能訪問Internet

此問題有兩種可能情況。

1. 目的地為網際網路的流量不得通過VPN隧道。

請確保將組策略配置為將隧道分割為隧道網路，如下指定，不配置為允許所有流量通過隧道，如下圖所示。

Edit Group Policy

Name: * Anyconnect_GroupPolicy

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling: Tunnel networks specified below

IPv6 Split Tunneling: Tunnel networks specified below

Split Tunnel Network List Type: Standard Access List Extended Access List

Standard Access List: Split-tunnel-ACL

DNS Request Split Tunneling

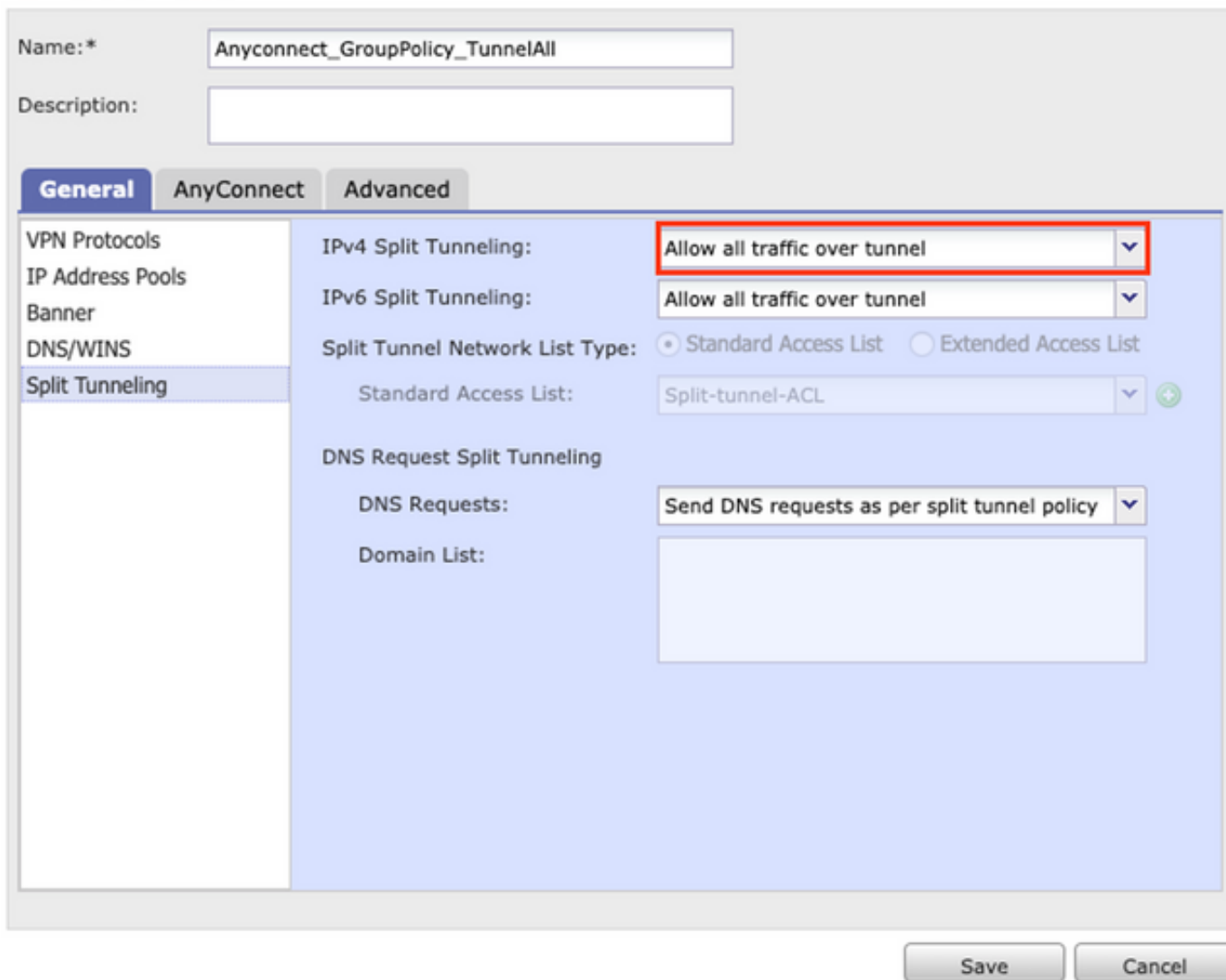
DNS Requests: Send DNS requests as per split tunnel policy

Domain List:

Save Cancel

2. 目的地為Internet的流量必須通過VPN隧道。

在這種情況下，拆分隧道的最常見組策略配置是選擇Allow all traffic over tunnel，如下圖所示。



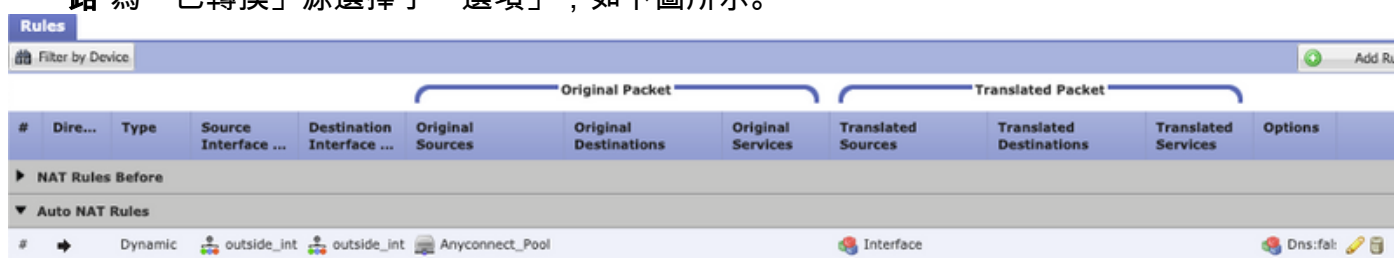
步驟1.檢驗NAT免除配置以實現內部網路連通性。

請記住，我們仍然必須配置NAT免除規則才能訪問內部網路。請檢視第2步，共同 AnyConnect客戶端無法訪問內部資源 部分。

步驟2.驗證動態轉換的迴轉連線配置。

為了使AnyConnect客戶端能夠通過VPN隧道訪問網際網路，我們需要確保髮夾NAT配置正確，以便流量轉換為介面的IP地址。

- 導航到NAT配置： Devices > NAT。
- 確保為作為源和目標（迴轉傳輸）的正確介面(網際網路服務提供商(ISP)鏈路)配置了動態 NAT規則。 還要檢查是否已在原始源和目標介面IP中選擇了用於AnyConnect VPN地址池的網路為「已轉換」源選擇了「選項」，如下圖所示。



步驟3. 驗證訪問控制策略。

根據您的訪問控制策略配置，確保允許來自AnyConnect客戶端的流量訪問外部資源，如下圖所示。

#	Name	Source ...	Dest ...	Source Networks	Dest Networks	VL...	Users	Ap...	Sou...	Des...	URLs	ISE...	Ac...	
▼ Mandatory - Policy1 (1-5)														
▶ External (1-2)														
▼ AnyconnectPolicy (3-5)														
3	Anyconnect-to-internet	Outside	Outside	Anyconnect_Pool	Any		Any	Any	Any	Any	Any	Any	Any	0
4	Internet-to-Anyconnect	Outside	Outside	Any	Anyconnect_Pool		Any	Any	Any	Any	Any	Any	Any	0

AnyConnect客戶端無法相互通訊

此問題有兩種可能情況：

1. AnyConnect客戶端 允許所有流量通過隧道 配置到位。
2. AnyConnect客戶端 下面指定的隧道網路 配置到位。

1. AnyConnect客戶端 允許所有流量通過隧道 配置到位。

When 允許所有流量通過隧道 配置為AnyConnect意味著所有流量（內部和外部流量）都應轉發到AnyConnect頭端，當您擁有用於公共Internet訪問的NAT時，這將成為一個問題，因為來自發往其他AnyConnect客戶端的AnyConnect客戶端的流量將轉換為介面IP地址，因此通訊失敗。

步驟1. 檢驗NAT免除配置。

為了解決此問題，必須配置手動NAT免除規則以允許在AnyConnect客戶端內進行雙向通訊。

- 導航到NAT配置： **Devices > NAT**。
- 確保為正確的源（AnyConnect VPN池）和目標配置NAT免除規則。（AnyConnect VPN池）網路。此外，請檢查是否安裝了正確的髮夾配置，如圖所示。

#	Dir...	Type	Source Interface ...	Destination Interface ...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1		Static	outside_int	outside_int	Anyconnect_Pool	Anyconnect_Pool		Anyconnect_Pool	Anyconnect_Pool		Dns:fail, route-lc, no-prox

步驟2. 驗證存取控制原則。

根據您的訪問控制策略配置，確保允許來自AnyConnect客戶端的流量，如下圖所示。

#	Name	Source ...	Dest ...	Source Networks	Dest Networks	VL...	Users	Ap...	Sou...	Des...	URLs	ISE...	Ac...	
▼ Mandatory - Policy1 (1-6)														
▶ External (1-2)														
▼ AnyconnectPolicy (3-6)														
3	Anyconnect-intra	Outside	Outside	Anyconnect_Pool	Anyconnect_Pool		Any	Any	Any	Any	Any	Any	Any	0

2. Anyconnect客戶端 下面指定的隧道網路 配置到位。

使用下面指定的隧道網路為AnyConnect客戶端配置的僅特定流量通過VPN隧道轉發到。但是，我們需要確保頭端具有正確的配置，以允許在AnyConnect客戶端內進行通訊。

步驟1. 檢驗NAT免除配置。

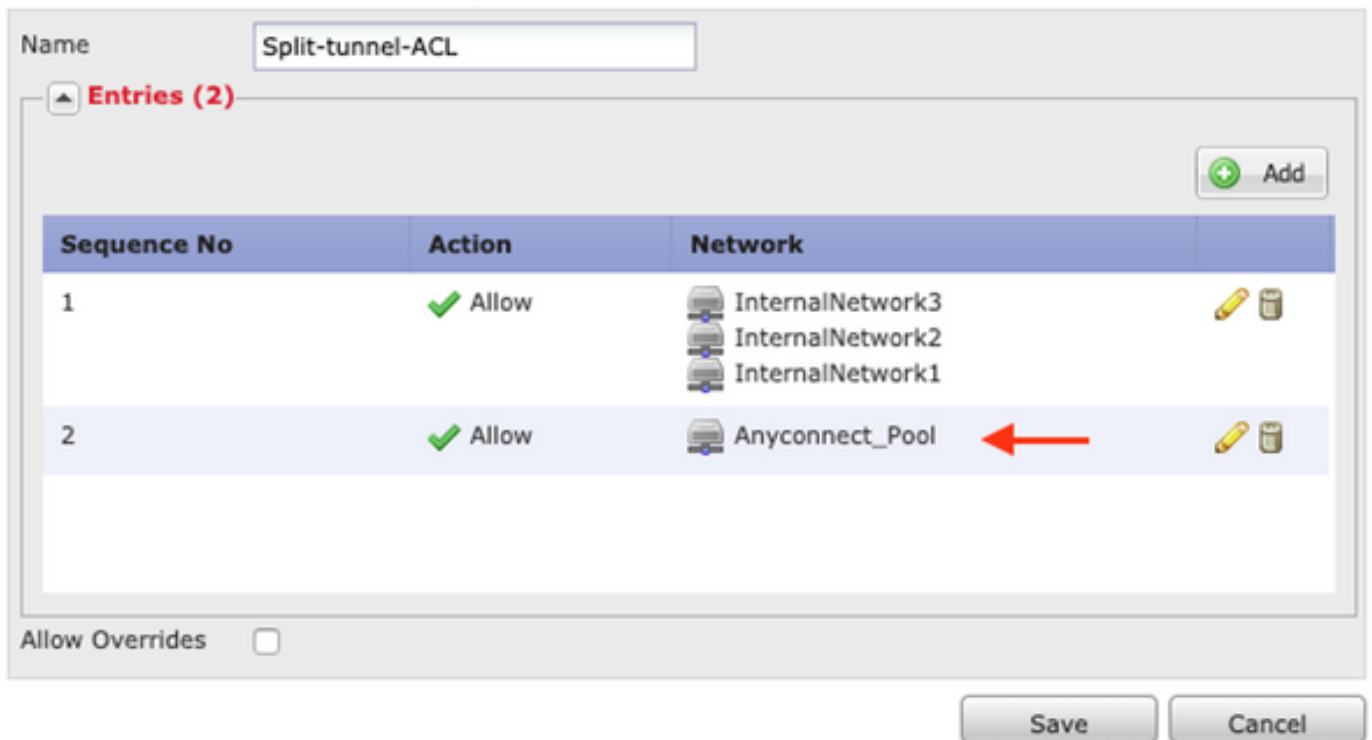
請檢查允許所有流量通過通道部分中的步驟1。

步驟2. 驗證分割隧道配置。

要使AnyConnect客戶端之間通訊，我們需要將VPN池地址新增到拆分隧道ACL中。

- 請按照的步驟1 AnyConnect客戶端無法訪問內部資源 部分。
- 確保AnyConnect VPN池網路列在Split tunneling Access List中，如圖所示。

Edit Standard Access List Object



附註：如果有多個IP池用於AnyConnect客戶端，並且需要在不同的池之間進行通訊，請確保在拆分隧道ACL中新增所有池，並為所需的IP池新增NAT免除規則。

步驟3. 驗證訪問控制策略。

確保允許來自AnyConnect客戶端的流量，如下圖所示。



AnyConnect客戶端無法建立電話呼叫

在某些情況下，AnyConnect客戶端需要通過VPN建立電話呼叫和視訊會議。

AnyConnect客戶端可以連線到AnyConnect頭端，而不會出現任何問題。它們可以訪問內部和外部資源，但電話呼叫無法建立。

對於這種情況，我們需要考慮以下幾點：

- 語音的網路拓撲。
- 涉及的協定。即作業階段啟動通訊協定(SIP)、快速跨距樹狀目錄通訊協定(RSTP)等。
- VPN電話如何連線到Cisco Unified Communications Manager(CUCM)。

預設情況下，FTD和ASA在其全域性策略對映中預設啟用應用程式檢查。

在大多數情況下，VPN電話無法與CUCM建立可靠的通訊，因為AnyConnect頭端已啟用修改訊號和語音流量的應用檢測。

有關可在其中應用應用檢測的語音和影片應用的詳細資訊，請參閱以下文檔：

[章節：語音和視訊通訊協定的檢查](#)

為了確認全域性策略對映是否丟棄或修改了應用程式流量，我們可以使用**show service-policy** 命令，如下所示。

```
firepower#show service-policy
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: inspection_default
```

```
.
```

```
.
```

```
Inspect: sip , packet 792114, lock fail 0, drop 10670, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
```

```
.
```

在此案例中，我們可以看到SIP檢測如何丟棄流量。

此外，SIP檢測還可以轉換負載內部的IP地址，而不是IP報頭中的IP地址，這會導致不同的問題，因此建議當我們希望通過AnyConnect VPN使用語音服務時禁用該檢測。

若要停用它，我們需要完成以下步驟：

步驟1.進入特權執行模式。

有關如何訪問此模式的詳細資訊，請參閱以下文檔：

[章節：使用命令列介面\(CLI\)](#)

步驟2.驗證全域性策略對映。

運行下一個命令並驗證SIP檢測是否已啟用。


```
firepower#show running-config policy-map
```

```
.
```

```
.
```

```
policy-map global_policy
```

```
class inspection_default
```

```
inspect dns preset_dns_map
```

```
inspect ftp
```

```
inspect h323 h225
```

```
inspect h323 ras
```

```
inspect rsh
```

```
inspect rtsp
```

```
inspect sqlnet
```

```
inspect skinny
```

```
inspect sunrpc
```

```
inspect xdmcp
```

```
inspect sip
```

```
inspect netbios
```

```
inspect tftp
```

```
inspect ip-options
```

```
inspect icmp
```

```
inspect icmp error
```

```
inspect esmtp
```

步驟3.禁用SIP檢測。

如果已啟用SIP檢測，請從點選提示符關閉以下運行命令：

```
> configure inspection sip disable
```

步驟4. 再次驗證全域性策略對映。

確保從全域性策略對映禁用SIP檢測：

```
firepower#show running-config policy-map
```

```
.
```

```
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect netbios
inspect tftp
inspect ip-options
inspect icmp
inspect icmp error
inspect esmtp
```

AnyConnect客戶端可以建立電話呼叫，但是呼叫沒有音訊

如上一節所述，AnyConnect客戶端的一個非常普遍的需求是在連線到VPN時建立電話呼叫。在某些情況下，可以建立呼叫，但客戶端可能遇到缺乏音訊的情況。這適用於以下情形：

- AnyConnect客戶端與外部號碼之間的呼叫無音訊。
- AnyConnect客戶端和另一個AnyConnect客戶端之間的呼叫沒有音訊。

為了修復此問題，我們可以執行以下步驟：

步驟1. 驗證分割隧道配置。

- 導航到用於連線的連線配置檔案：**Devices > VPN > Remote Access > Connection Profile > Select the Profile.**
- 導航到分配給該Profile: 的組策略**編輯組策略>常規。**
- 檢查分割隧道配置，如下圖所示。

Edit Group Policy

? X

Name:* Anyconnect_GroupPolicy

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling: Tunnel networks specified below

IPv6 Split Tunneling: Tunnel networks specified below

Split Tunnel Network List Type: Standard Access List Extended Access List

Standard Access List: Split-tunnel-ACL

DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split tunnel policy

Domain List:

Save Cancel

- 如果配置為 下面指定的隧道網路，驗證訪問清單配置：Objects > Object Management > Access List > Edit the Access List for Split tunneling。
- 確保在Split tunneling Access List中列出語音伺服器和AnyConnect IP池網路，如下圖所示。

Edit Standard Access List Object



Name: Split-tunnel-ACL

Entries (2)

Sequence No	Action	Network
1	✓ Allow	InternalNetwork3 InternalNetwork2 InternalNetwork1
2	✓ Allow	VoiceServers Anyconnect_Pool

Allow Overrides

Save Cancel

步驟2.檢驗NAT免除配置。

必須配置NAT免除規則以免除從AnyConnect VPN網路到語音伺服器網路的流量，並允許AnyConnect客戶端內的雙向通訊。

- 導航到NAT配置：**Devices > NAT**。
- 確保為正確的源（語音伺服器）和目標（AnyConnect VPN池）網路配置了NAT免除規則，並且已經有了允許AnyConnect客戶端與AnyConnect客戶端通訊的髮夾NAT規則。此外，請根據您的網路設計，檢查每個規則的入站和出站介面配置是否正確，如下圖所示。

Rules

Filter by Device

#..	Dir...	T...	Original Packet				Translated Packet				Options
			Source Interface Ob...	Destination Interface Obj...	Original Sources	Original Destinations	O... S...	Translated Sources	Translated Destinations	T... S...	
▼ NAT Rules Before											
1	↔	S...	Inside_interfac	outside_interface	InternalNetworksGroup	Anyconnect_Pool	InternalNetworksGroup	Anyconnect_Pool		Dns:false route-foo no-proxy	
2	↔	S...	Inside_interfac	outside_interface	VoiceServers	Anyconnect_Pool	VoiceServers	Anyconnect_Pool		Dns:false route-foo no-proxy	
3	↔	S...	outside_interfa	outside_interface	Anyconnect_Pool	Anyconnect_Pool	Anyconnect_Pool	Anyconnect_Pool		Dns:false route-foo no-proxy	

步驟3.驗證SIP檢查是否已禁用。

請查閱上一節 AnyConnect客戶端無法建立電話呼叫 瞭解如何禁用SIP檢測。

步驟4.驗證訪問控制策略。

根據您的訪問控制策略配置，確保允許來自AnyConnect客戶端的流量到達語音伺服器和相關的網路，如下圖所示。

The screenshot shows the Cisco ASA configuration interface for the 'Rules' section. The 'Mandatory - Policy1' is expanded to show three rules. The first rule, 'Anyconnect-intra', is selected. The configuration table is as follows:

#	Name	Source ...	Dest ...	Source Networks	Dest Networks	VL...	Users	Ap...	Sou...	Des...	URLs	ISE...	Ac...	
3	Anyconnect-intra	Outside	Outside	Anyconnect_Pool	Anyconnect_Pool	Any	Any	Any	Any	Any	Any	Any	✓ Allow	0
4	Anyconnect-to-voice-servr	Outside	Inside	Anyconnect_Pool	VoiceServers	Any	Any	Any	Any	Any	Any	Any	✓ Allow	0

相關資訊

- 此影片提供本文所述不同問題的組態範例。
- 如需其他協助，請聯絡技術協助中心(TAC)。需要有效的支援合約：[思科全球支援聯絡人](#)。
- 您還可以訪問Cisco VPN社群 [此處](#)。