

FTD에서 일반적인 AnyConnect 통신 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[권장 문제 해결 프로세스](#)

[AnyConnect 클라이언트가 내부 리소스에 액세스할 수 없음](#)

[AnyConnect 클라이언트에 인터넷 액세스가 없습니다.](#)

[AnyConnect 클라이언트는 서로 통신할 수 없습니다.](#)

[AnyConnect 클라이언트가 전화 통화를 설정할 수 없습니다.](#)

[AnyConnect 클라이언트는 전화 통화를 설정할 수 있지만 통화에 오디오가 없습니다.](#)

[관련 정보](#)

소개

이 문서에서는 SSL(Secure Socket Layer) 또는 IKEv2(Internet Key Exchange version 2)를 사용할 때 Cisco FTD(AnyConnect Secure Mobility Client on Firepower Threat Defense)에서 가장 일반적인 몇 가지 통신 문제를 해결하는 방법에 대해 설명합니다.

기고자: Angel Ortiz 및 Fernando Jimenez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AnyConnect Secure Mobility Client.
- Cisco FTD
- Cisco FMC(Firepower Management Center).

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMC 6.4.0에서 관리하는 FTD.
- AnyConnect 4.8.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

권장 문제 해결 프로세스

이 설명서에서는 FTD를 VPN(Remote Access Virtual Private Network) 게이트웨이로 사용할 때

AnyConnect 클라이언트에서 발생하는 몇 가지 일반적인 통신 문제를 해결하는 방법을 설명합니다. 이 섹션에서는 아래 문제에 대해 설명하고 해결책을 제시합니다.

- AnyConnect 클라이언트는 내부 리소스에 액세스할 수 없습니다.
- AnyConnect 클라이언트에는 인터넷 액세스가 없습니다.
- AnyConnect 클라이언트는 서로 통신할 수 없습니다.
- AnyConnect 클라이언트는 전화 통화를 설정할 수 없습니다.
- AnyConnect 클라이언트는 전화 통화를 설정할 수 있습니다. 그러나 통화에 오디오가 없습니다

AnyConnect 클라이언트가 내부 리소스에 액세스할 수 없음

다음 단계를 완료하십시오.

1단계. 스플릿 터널 컨피그레이션을 확인합니다.

- AnyConnect 클라이언트가 연결된 연결 프로파일로 이동합니다. **Devices(디바이스) > VPN > Remote Access(원격 액세스) > Connection Profile(연결 프로파일) > Select the Profile(프로필 선택)**.
- 해당 프로파일에 할당된 Group-Policy(그룹 정책 수정) > **General(일반)**으로 이동합니다.
- 이미지에 표시된 대로 스플릿 터널링 컨피그레이션을 확인합니다.

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:

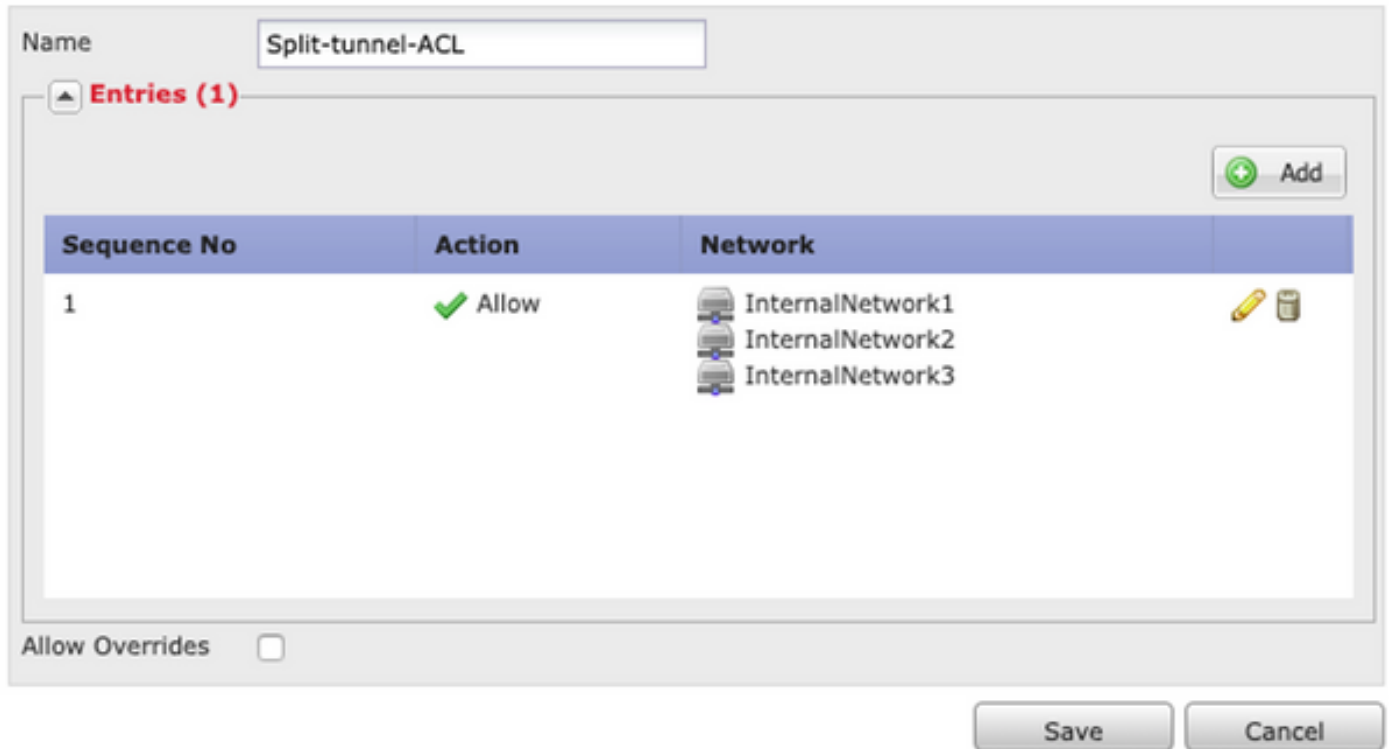
Save Cancel

- 아래에 지정된 터널 네트워크로 구성된 경우 ACL(Access Control List) 컨피그레이션을 확인합니다.

Objects(개체) > Object Management(개체 관리) > Access List(액세스 목록) > Edit the Access List for Split tunneling(스플릿 터널링에 대한 액세스 목록 편집)으로 이동합니다.

- 이미지에 표시된 대로 AnyConnect VPN 클라이언트에서 연결하려는 네트워크가 해당 액세스 목록에 나열되어 있는지 확인합니다.

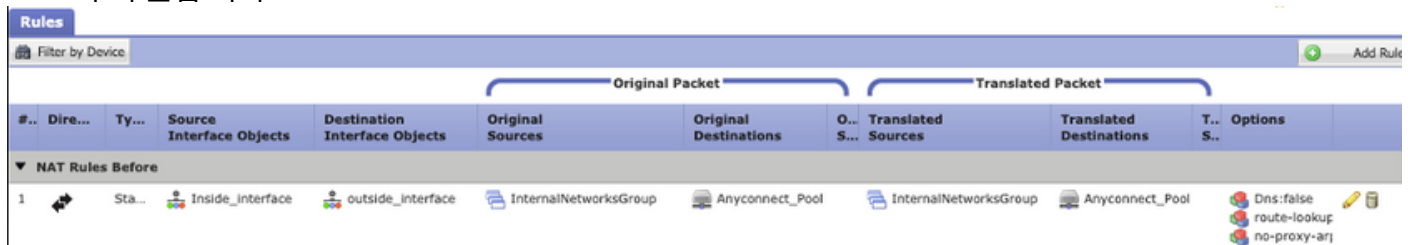
Edit Standard Access List Object



2단계. NAT(Network Address Translation) 예외 컨피그레이션을 확인합니다.

일반적으로 인터넷 액세스를 위해 구성된 인터페이스 IP 주소(PAT(Port Address Translation)로 트래픽을 변환하지 않도록 NAT 예외 규칙을 구성해야 합니다.

- NAT 컨피그레이션으로 이동합니다. **Devices(디바이스) > NAT.**
- 올바른 소스(내부) 및 대상(AnyConnect VPN 풀) 네트워크에 대해 NAT 예외 규칙이 구성되어 있는지 확인합니다. 또한 이미지에 표시된 대로 올바른 소스 및 대상 인터페이스가 선택되었는지 확인합니다.



참고: NAT 예외 규칙이 구성된 경우 no-proxy-arp를 확인하고 경로 조회 옵션을 모범 사례로서 수행합니다.

3단계. 액세스 제어 정책을 확인합니다.

액세스 제어 정책 컨피그레이션에 따라 이미지에 표시된 대로 AnyConnect 클라이언트의 트래픽이 선택한 내부 네트워크에 도달할 수 있는지 확인합니다.



AnyConnect 클라이언트에 인터넷 액세스가 없습니다.

이 문제에 대한 두 가지 가능한 시나리오가 있습니다.

1. 인터넷으로 향하는 트래픽은 VPN 터널을 통과해서는 안 됩니다.

그룹 정책이 아래에 지정된 터널 네트워크로 스플릿 터널링에 대해 구성되고 이미지에 표시된 대로 터널을 통한 모든 트래픽을 허용하지 않도록 합니다.

Edit Group Policy

A screenshot of the 'Edit Group Policy' dialog box in Cisco ISE. The 'Advanced' tab is selected. The 'Split Tunneling' section is expanded. The 'IPv4 Split Tunneling' dropdown is set to 'Tunnel networks specified below' (highlighted with a red box). The 'IPv6 Split Tunneling' dropdown is also set to 'Tunnel networks specified below'. The 'Split Tunnel Network List Type' is set to 'Standard Access List'. The 'Standard Access List' dropdown is set to 'Split-tunnel-ACL'. The 'DNS Request Split Tunneling' section is also visible, with 'DNS Requests' set to 'Send DNS requests as per split tunnel policy'.

2. 인터넷을 목적지로 하는 트래픽은 VPN 터널을 통과해야 합니다.

이 경우 스플릿 터널링에 대한 가장 일반적인 그룹 정책 컨피그레이션은 이미지에 표시된 대로

Allow all traffic over tunnel(터널을 통한 모든 트래픽 허용)을 선택하는 것입니다.

Edit Group Policy

? X

Name: * Anyconnect_GroupPolicy_TunnelAll

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling: Allow all traffic over tunnel

IPv6 Split Tunneling: Allow all traffic over tunnel

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

1단계. 내부 네트워크 연결성에 대한 NAT 예외 컨피그레이션을 확인합니다.

내부 네트워크에 액세스할 수 있도록 NAT 예외 규칙을 구성해야 합니다. 의 2단계를 검토하십시오. AnyConnect 클라이언트가 내부 리소스에 액세스할 수 없음 섹션을 참조하십시오.

2단계. 동적 변환에 대한 헤어피닝 구성을 확인합니다.

AnyConnect 클라이언트가 VPN 터널을 통해 인터넷에 액세스할 수 있도록 하려면 헤어피닝 NAT 컨피그레이션이 인터페이스의 IP 주소로 트래픽이 변환될 수 있는지 확인해야 합니다.

- NAT 컨피그레이션으로 이동합니다. **Devices(디바이스) > NAT.**
- 동적 NAT 규칙이 소스 및 대상(헤어피닝)으로 올바른 인터페이스(ISP(Internet Service Provider) 링크)에 대해 구성되어 있는지 확인합니다. 또한 AnyConnect VPN 주소 풀에 사용된 네트워크가 원래 소스 및 대상 **인터페이스 IP**에서 선택되었는지 확인합니다. 이 옵션은 이미지에 표시된 대로 [변환된 소스]에 대해 선택됩니다.

#	Dir...	Type	Source Interface ...	Destination Interface ...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before											
Auto NAT Rules											
#	→	Dynamic	outside_int	outside_int	Anyconnect_Pool				Interface		Dns: fal

3단계. 액세스 제어 정책을 확인합니다.

액세스 제어 정책 컨피그레이션에 따라 이미지에 표시된 대로 AnyConnect 클라이언트의 트래픽이 외부 리소스에 도달할 수 있는지 확인합니다.

#	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	✓ Allo
4	Internet-to-Anyconnect	Outside	Outside	Any	Anyconnect_Pool	Any	Any	Any	Any	Any	Any	Any	✓ Allo

AnyConnect 클라이언트는 서로 통신할 수 없습니다.

이 문제에 대한 두 가지 시나리오가 있습니다.

1. AnyConnect 클라이언트 터널을 통한 모든 트래픽 허용 구성.
2. AnyConnect 클라이언트 아래에 지정된 터널 네트워크 구성.

1. AnyConnect 클라이언트 터널을 통한 모든 트래픽 허용 구성.

언제 터널을 통한 모든 트래픽 허용 AnyConnect에 대해 구성되었다는 것은 내부 및 외부 모든 트래픽을 AnyConnect 헤드엔드로 전달해야 한다는 것을 의미합니다. 공용 인터넷 액세스를 위한 NAT가 있는 경우, 다른 AnyConnect 클라이언트로 향하는 트래픽이 인터페이스 IP 주소로 변환되므로 통신이 실패합니다.

1단계. NAT 예외 컨피그레이션을 확인합니다.

이 문제를 해결하려면 AnyConnect 클라이언트 내에서 양방향 통신을 허용하도록 수동 NAT 예외 규칙을 구성해야 합니다.

- NAT 컨피그레이션으로 이동합니다. **Devices(디바이스) > NAT.**
- 올바른 소스(AnyConnect VPN 풀) 및 대상에 대해 NAT 예외 규칙이 구성되어 있는지 확인합니다. (AnyConnect VPN 풀) 네트워크. 또한 이미지에 표시된 대로 올바른 헤어핀 컨피그레이션이 있는지 확인합니다.

#	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: fal, route-1c, no-prox

2단계. 액세스 제어 정책을 확인합니다.

액세스 제어 정책 컨피그레이션에 따라 이미지에 표시된 대로 AnyConnect 클라이언트의 트래픽이 허용되는지 확인합니다.



2. AnyConnect 클라이언트 아래에 지정된 터널 네트워크 구성.

사용 아래에 지정된 터널 네트워크 AnyConnect 클라이언트에 대해 구성된 특정 트래픽만 VPN 터널을 통해 로 전달됩니다. 그러나 헤드엔드에 AnyConnect 클라이언트 내의 통신을 허용하는 적절한 컨피그레이션이 있는지 확인해야 합니다.

1단계. NAT 예외 컨피그레이션을 확인합니다.

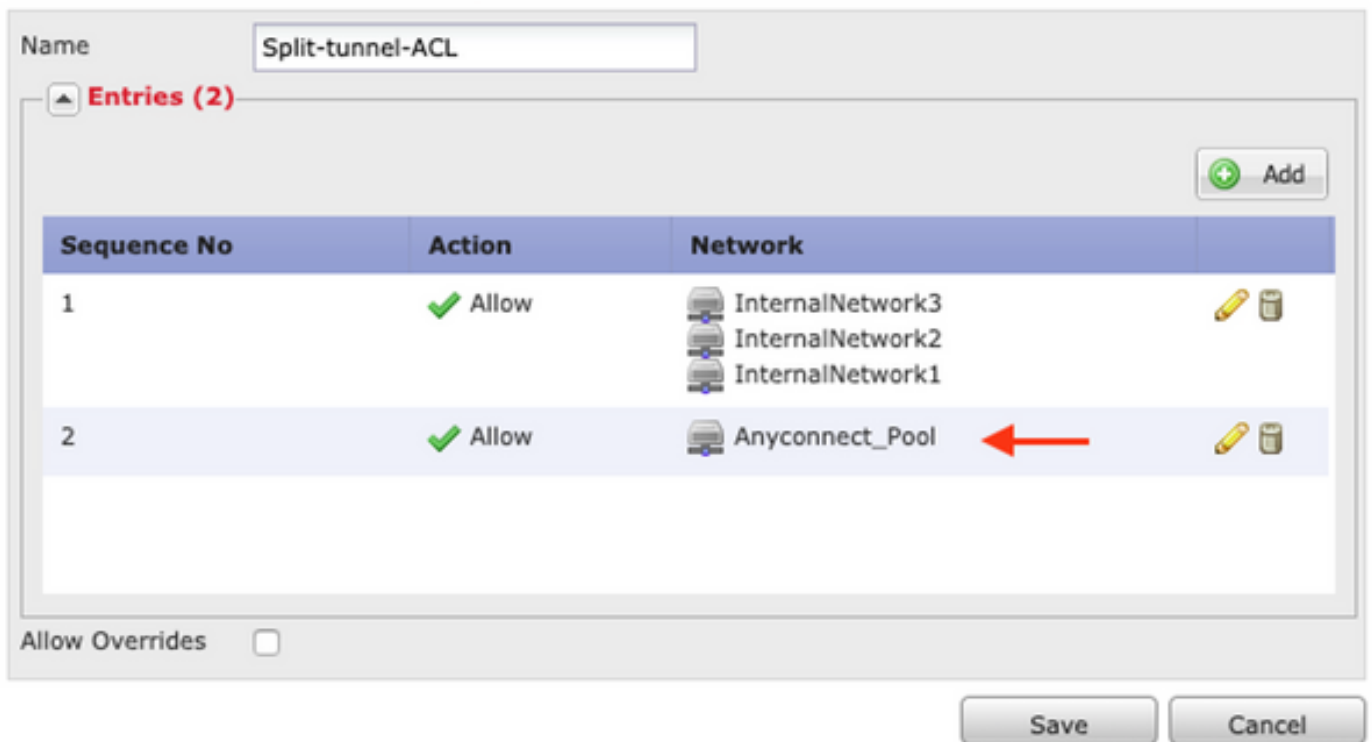
Allow all traffic over tunnel 섹션에서 1단계를 확인하십시오.

2단계. 스플릿 터널링 컨피그레이션을 확인합니다.

AnyConnect 클라이언트가 서로 통신하려면 스플릿 터널 ACL에 VPN 풀 주소를 추가해야 합니다.

- 다음 단계 1을 따르십시오. AnyConnect 클라이언트가 내부 리소스에 액세스할 수 없음 섹션을 참조하십시오.
- 이미지에 표시된 대로 AnyConnect VPN 풀 네트워크가 스플릿 터널링 액세스 목록에 나열되어 있는지 확인합니다.

Edit Standard Access List Object



참고: AnyConnect 클라이언트에 대해 둘 이상의 IP 풀이 있고 다른 풀 간의 통신이 필요한 경우 스플릿 터널링 ACL에 모든 풀을 추가해야 하며 필요한 IP 풀에 대해 NAT 예외 규칙을 추가

하십시오.

3단계. 액세스 제어 정책을 확인합니다.

이미지에 표시된 대로 AnyConnect 클라이언트의 트래픽이 허용되는지 확인합니다.



AnyConnect 클라이언트가 전화 통화를 설정할 수 없습니다.

AnyConnect 클라이언트가 VPN을 통해 전화 통화 및 화상 회의를 설정해야 하는 몇 가지 시나리오가 있습니다.

AnyConnect 클라이언트는 문제 없이 AnyConnect 헤드엔드에 연결할 수 있습니다. 내부 및 외부 리소스에 연결할 수 있지만 전화 통화를 설정할 수 없습니다.

이 경우 다음 사항을 고려해야 합니다.

- 음성 네트워크 토폴로지
 - 관련된 프로토콜입니다. SIP(Session Initiation Protocol), RSTP(Rapid Spanning Tree Protocol) 등
 - VPN 전화기가 Cisco CUCM(Unified Communications Manager)에 연결되는 방법
- 기본적으로 FTD 및 ASA는 전역 정책 맵에서 기본적으로 애플리케이션 검사를 활성화합니다.

대부분의 경우 AnyConnect 헤드엔드에 신호 및 음성 트래픽을 수정하는 애플리케이션 검사가 활성화되어 있기 때문에 VPN 전화기는 CUCM과의 안정적인 통신을 설정할 수 없습니다.

애플리케이션 검사를 적용할 수 있는 음성 및 비디오 애플리케이션에 대한 자세한 내용은 다음 문서를 참조하십시오.

[장: 음성 및 비디오 프로토콜 검사](#)

애플리케이션 트래픽이 전역 정책 맵에 의해 삭제 또는 수정되는지 확인하기 위해 아래와 같이 **show service-policy** 명령을 사용할 수 있습니다.

```
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
```


이 경우 SIP 검사가 트래픽을 삭제하는 방법을 확인할 수 있습니다.

또한 SIP 검사는 IP 헤더가 아닌 페이로드 내부의 IP 주소를 변환할 수 있으므로 다른 문제가 발생하므로 AnyConnect VPN을 통해 음성 서비스를 사용하려는 경우 이를 비활성화하는 것이 좋습니다

비활성화하려면 다음 단계를 완료해야 합니다.

1단계. 특별 권한 EXEC 모드를 시작합니다.

이 모드에 액세스하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오.

[장: CLI\(Command Line Interface\) 사용](#)

2단계. 전역 정책 맵을 확인합니다.

다음 명령을 실행하고 SIP 검사가 활성화되었는지 확인합니다.

```
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
```

3단계. SIP 검사를 비활성화합니다.

SIP 검사가 활성화된 경우 호출 프롬프트에서 아래의 실행 명령을 해제합니다.

```
> configure inspection sip disable
```

4단계. 전역 정책 맵을 다시 확인합니다.

SIP 검사가 전역 정책 맵에서 비활성화되었는지 확인합니다.

```
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 클라이언트는 전화 통화를 설정할 수 있지만 통화에 오디오가 없습니다.

이전 섹션에서 언급한 대로, AnyConnect 클라이언트가 VPN에 연결될 때 전화 통화를 설정하는 것이 매우 일반적입니다. 경우에 따라 통화를 설정할 수 있지만, 클라이언트에 오디오가 없을 수 있습니다. 이는 다음 시나리오에 적용됩니다.

- AnyConnect 클라이언트와 외부 번호 간의 통화에 오디오가 없습니다.
- AnyConnect 클라이언트와 다른 AnyConnect 클라이언트 간의 통화에 오디오가 없습니다.

이 문제를 해결하려면 다음 단계를 수행하십시오.

1단계. 스플릿 터널링 컨피그레이션을 확인합니다.

- Connection Profile(연결 프로파일)을 사용하여 다음으로 이동합니다. **Devices(디바이스) > VPN > Remote Access(원격 액세스) > Connection Profile(연결 프로파일) > Select the Profile(프로필 선택)**.
- 해당 프로파일에 할당된 Group-Policy(그룹 정책 수정) > **General(일반)**으로 이동합니다.
- 이미지에 표시된 대로 스플릿 터널링 컨피그레이션을 확인합니다.

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:

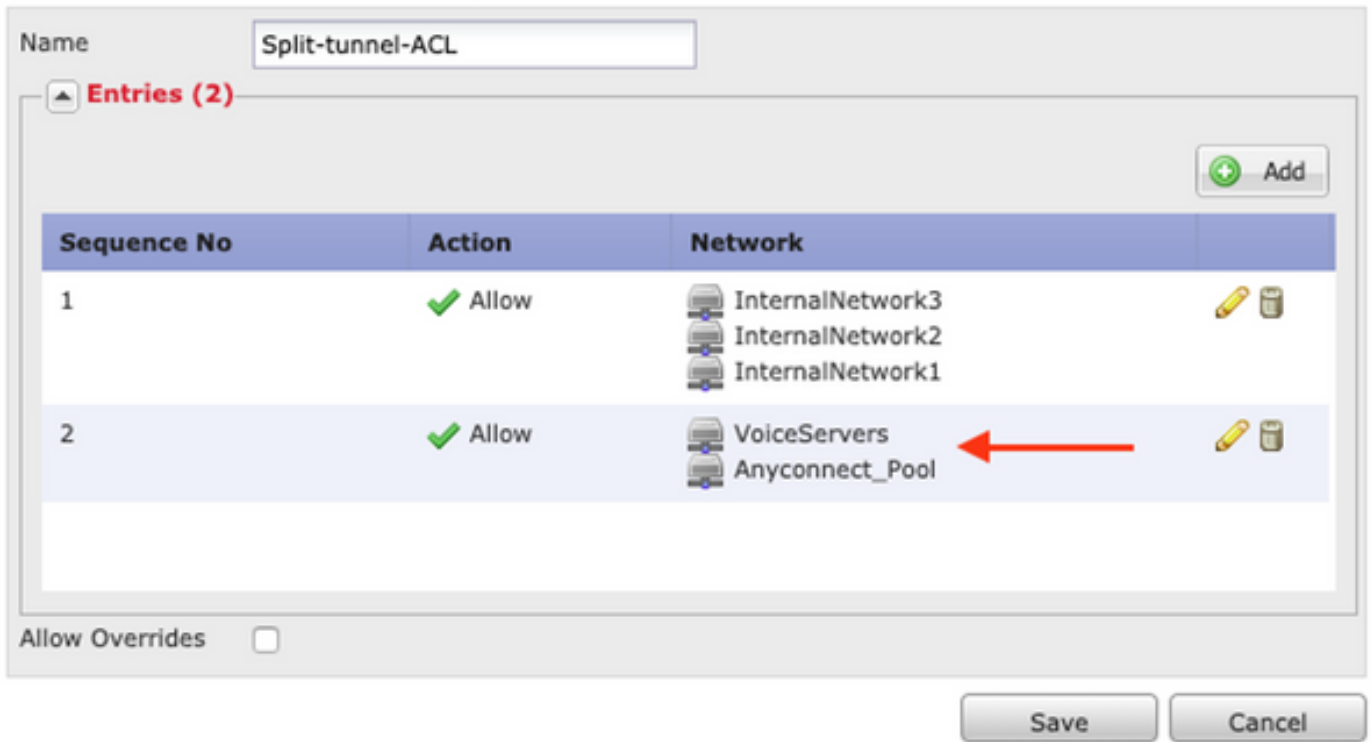
Save Cancel

- 다음으로 구성된 경우 아래에 지정된 터널 네트워크, 액세스 목록 컨피그레이션을 확인합니

다. Objects(개체) > Object Management(개체 관리) > Access List(액세스 목록) > Edit the Access List for Split tunneling(스플릿 터널링에 대한 액세스 목록 편집)

- 이미지에 표시된 대로 Split tunneling Access List(스플릿 터널링 액세스 목록)에 음성 서버 및 AnyConnect IP 풀 네트워크가 나열되어 있는지 확인합니다.

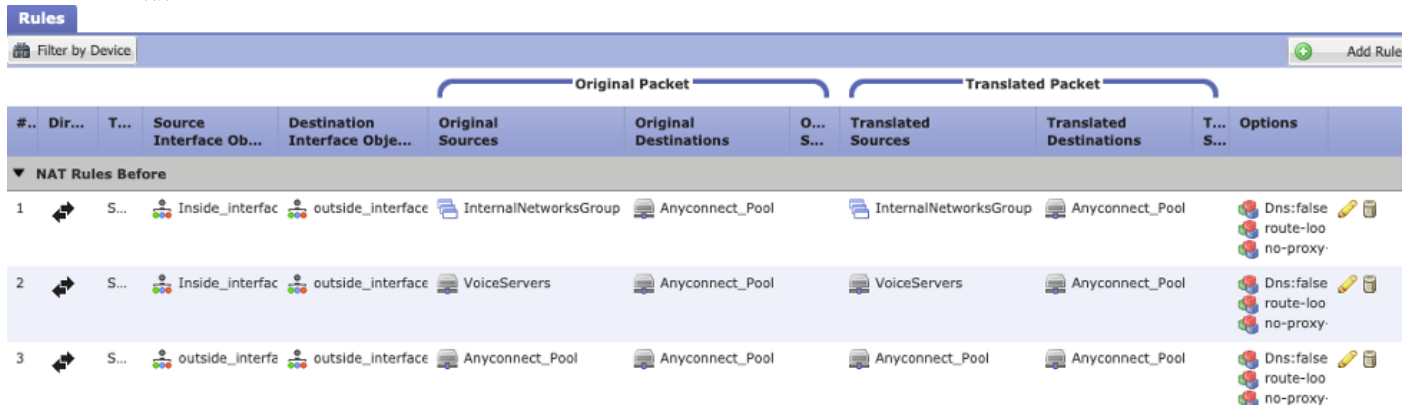
Edit Standard Access List Object



2단계. NAT 예외 컨피그레이션을 확인합니다.

AnyConnect VPN 네트워크에서 음성 서버 네트워크로 가는 트래픽을 면제하고 AnyConnect 클라이언트 내에서 양방향 통신을 허용하도록 NAT 예외 규칙을 구성해야 합니다.

- NAT 컨피그레이션으로 이동합니다. **Devices(디바이스) > NAT.**
- 올바른 소스(음성 서버) 및 대상(AnyConnect VPN 풀) 네트워크에 대해 NAT 예외 규칙이 구성되었는지 확인하고, AnyConnect 클라이언트에서 AnyConnect 클라이언트 통신을 허용하도록 헤어핀 NAT 규칙이 적용되었는지 확인합니다. 또한 이미지에 표시된 대로 네트워크 설계에 따라 각 규칙에 대해 올바른 인바운드 및 아웃바운드 인터페이스 컨피그레이션이 적용되었는지 확인합니다.



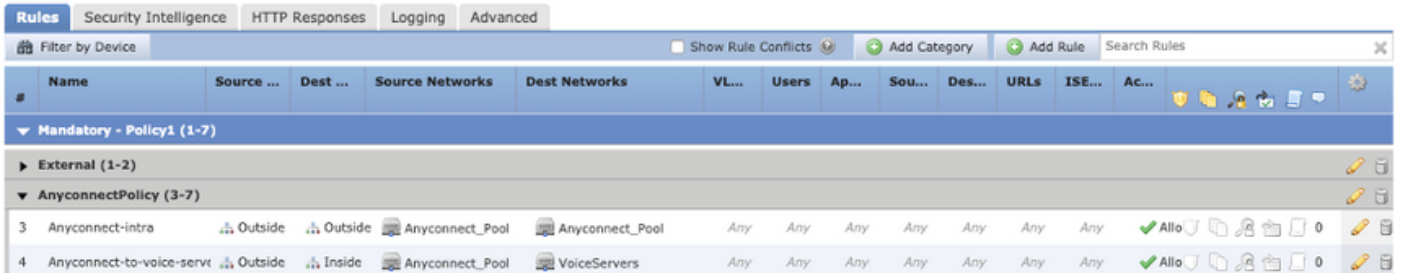
3단계. SIP 검사가 비활성화되었는지 확인합니다.

이전 섹션을 검토하십시오. AnyConnect 클라이언트가 전화 통화를 설정할 수 없습니다. SIP 검사

를 비활성화하는 방법을 알아보겠습니다.

4단계. 액세스 제어 정책을 확인합니다.

액세스 제어 정책 컨피그레이션에 따라 이미지에 표시된 대로 AnyConnect 클라이언트의 트래픽이 음성 서버 및 관련 네트워크에 연결되도록 허용되는지 확인합니다.



#	Name	Source ...	Dest ...	Source Networks	Dest Networks	VL...	Users	Ap...	Sou...	Des...	URLs	ISE...	Ac...	
▼ Mandatory - Policy1 (1-7)														
▶ External (1-2)														
▼ AnyconnectPolicy (3-7)														
3	Anyconnect-intra	Outside	Outside	Anyconnect_Pool	Anyconnect_Pool	Any	Any	Any	Any	Any	Any	Any	✓ Allow	0
4	Anyconnect-to-voice-servt	Outside	Inside	Anyconnect_Pool	VoiceServers	Any	Any	Any	Any	Any	Any	Any	✓ Allow	0

관련 정보

- 이 비디오에서는 이 문서에서 설명하는 여러 문제에 대한 구성 예제를 제공합니다.
- 추가 지원이 필요한 경우 기술 지원 센터(TAC)에 문의하십시오. 유효한 지원 계약이 필요합니다. [Cisco 전 세계 지원 문의처](#).
- 또한 Cisco VPN Community를 방문하여 [여기](#).