

Probleemoplossing voor gebruikelijke AnyConnect-communicatieproblemen op FTD

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Aanbevolen proces voor probleemoplossing](#)

[AnyConnect-klanten hebben geen toegang tot interne bronnen](#)

[AnyConnect-klanten hebben geen internettoegang](#)

[AnyConnect-clients kunnen niet tussen elkaar communiceren](#)

[AnyConnect-klanten kunnen geen telefoongesprekken instellen](#)

[AnyConnect-klanten kunnen telefoonoproepen instellen, maar er is geen audio van de oproepen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een aantal van de meest gebruikelijke communicatieproblemen van Cisco AnyConnect Secure Mobility Client op Firepower Threat Defense (FTD) kunt oplossen wanneer dit gebruik maakt van Secure Socket Layer (SSL) of Internet Key Exchange versie 2 (IKEv2).

Bijgedragen door Angel Ortiz en Fernando Jimenez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco AnyConnect beveiligde mobiliteit-client
- Cisco FTD.
- Cisco Firepower Management Center (FMC).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FTD beheerd door FMC 6.4.0.
- AnyConnect 4.8.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Aanbevolen proces voor probleemoplossing

Deze handleiding legt uit hoe u problemen kunt oplossen bij het oplossen van bepaalde gebruikelijke communicatieproblemen die AnyConnect-klanten hebben wanneer de FTD wordt gebruikt als VPN-poort (Remote Access Virtual Private Network). In deze rubrieken worden de volgende problemen aangepakt en opgelost:

- AnyConnect-klanten hebben geen toegang tot interne bronnen.
- AnyConnect-klanten hebben geen internettoegang.
- AnyConnect-clients kunnen niet met elkaar communiceren.
- AnyConnect-klanten kunnen geen telefoongesprekken instellen.
- AnyConnect-klanten kunnen telefoongesprekken instellen. Er is echter geen geluid op de oproepen.

AnyConnect-klanten hebben geen toegang tot interne bronnen

Voer de volgende stappen uit:

Stap 1. Controleer de tunnelconfiguratie.

- Navigeer naar het verbindingsprofiel waarop AnyConnect-clients zijn aangesloten op: **Apparaten > VPN > Externe toegang > Connection Profile > Selecteren van het profiel.**
- Navigeer aan het groepsbeleid dat aan dat Profile: **Bewerken Groepsbeleid > Algemeen is toegewezen.**
- Controleer de configuratie van Split-tunneling, zoals in de afbeelding wordt getoond.

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

- Als deze is geconfigureerd als hieronder **gespecificeerde tunnelnetwerken**, verifieert u de configuratie van toegangscontrolelijst (ACL):

Navigeer aan **Exemplaar > Objectbeheer > Toegangslijst > Bewerken de Lijst voor Split tunneling**.

- Zorg ervoor dat de netwerken die u probeert te bereiken vanaf de AnyConnect VPN-client in die toegangslijst zijn opgenomen, zoals in de afbeelding.

Edit Standard Access List Object



Name: Split-tunnel-ACL

Entries (1)

| Sequence No | Action | Network |
|-------------|---------|--|
| 1 | ✓ Allow | InternalNetwork1 InternalNetwork2 InternalNetwork3 |

Allow Overrides

Buttons: Add, Save, Cancel

Stap 2. Controleer de NAT-configuratie (Network Address Translation).

Onthoud dat we een NAT-vrijstellingsregel moeten configureren om te voorkomen dat verkeer wordt vertaald naar het IP-interfaceadres, dat doorgaans is ingesteld voor internettoegang (met Port Address Translation (PAT)).

- Navigeren naar de NAT-configuratie: **Apparaten > NAT**.
- Zorg ervoor dat de NAT-vrijstellingsregel is ingesteld voor de juiste bron- (interne) en doelnetwerken (AnyConnect VPN Pool). Controleer ook of de juiste bron- en doelinterfaces zijn geselecteerd, zoals in de afbeelding.

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

Opmerking: Wanneer NAT-vrijstellingsregels worden geconfigureerd, controleert u de **no-proxy-arp** en voert u **route-lookup**-opties uit als beste praktijk.

Stap 3. Controleer het toegangscontrolebeleid.

Zorg er na uw configuratie voor dat het verkeer van de AnyConnect-clients naar de geselecteerde interne netwerken mag worden gebracht, zoals in de afbeelding.



AnyConnect-klienten hebben geen internettoegang

Er zijn twee mogelijke scenario's voor deze kwestie.

1. Het verkeer dat voor het internet is bestemd, mag niet door de VPN-tunnel gaan.

Zorg ervoor dat het Group-Policy is geconfigureerd voor Split-tunneling als **tunnelnetwerken die hieronder zijn gespecificeerd** en NIET als **All verkeer via tunnel** toestaat, zoals in de afbeelding wordt getoond.

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. Voor het internet bestemd verkeer moet door de VPN-tunnel gaan.

In dit geval, zou de meest algemene configuratie van het Groep-Beleid voor het Split tunneling zijn om **Alle verkeer via tunnel** te selecteren, zoals in het beeld getoond wordt.

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

Stap 1. Controleer de NAT-vrijstellingsconfiguratie voor interne netwerkbereikbaarheid.

Denk eraan dat we nog steeds een NAT-vrijstellingsregel moeten configureren om toegang tot het interne netwerk te hebben. Zie **Stap 2** van het **AnyConnect-klienten hebben geen toegang tot interne resources** deel.

Stap 2. Controleer de configuratie van het kapsel voor dynamische vertalingen.

Om ervoor te zorgen dat AnyConnect-klienten toegang tot internet hebben via de VPN-tunnel, moeten we ervoor zorgen dat de NAT-configuratie correct is zodat het verkeer kan worden vertaald naar het IP-adres van de interface.

- Navigeren naar de NAT-configuratie: **Apparaten > NAT**.
- Zorg ervoor dat de Dynamische NAT-regel is ingesteld voor de juiste interface (Internet Service Provider (ISP)-link) als bron en bestemming (kapsel). Controleer ook of het netwerk dat voor de AnyConnect VPN-adrespool wordt gebruikt, in de oorspronkelijke bron en de IP van de doelinterface is geselecteerd. De optie wordt geselecteerd voor Vertaalde bron, zoals in de afbeelding weergegeven.

| # | Dire... | 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:fa |

Stap 3. Controleer het beleid voor toegangscontrole.

Zorg er na uw configuratie voor dat het verkeer van de AnyConnect-klienten de externe bronnen mag bereiken, zoals in de afbeelding.

| # | 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-clients kunnen niet tussen elkaar communiceren

Er zijn twee mogelijke scenario's voor deze kwestie:

1. AnyConnect-klienten met **Alle verkeer via een tunnel toestaan** configuratie op zijn plaats.
2. AnyConnect-klienten met **hieronder gespecificeerde tunnelnetwerken** configuratie op zijn plaats.

1. AnyConnect-klienten met **Alle verkeer via een tunnel toestaan** configuratie op zijn plaats.

Wanneer **Alle verkeer via een tunnel toestaan** is geconfigureerd voor AnyConnect en dit betekent dat al het interne en externe verkeer naar het AnyConnect-head-end moet worden verzonden. Dit wordt een probleem wanneer u NAT voor de toegang tot het openbare internet hebt, aangezien het verkeer afkomstig is van een AnyConnect-client die bestemd is voor een andere AnyConnect-client, wordt vertaald naar het IP-interfaceadres en de communicatie mislukt.

Stap 1. Controleer de NAT-vrijstellingsconfiguratie.

Om dit probleem op te lossen moet een handmatige NAT-vrijstellingsregel zo worden geconfigureerd dat deze binnen de AnyConnect-klienten bidirectionele communicatie mogelijk maakt.

- Navigeren naar de NAT-configuratie: **Apparaten > NAT**.
- Zorg ervoor dat de NAT-vrijstellingsregel is ingesteld voor de juiste bron (AnyConnect VPN-pool) en de juiste bestemming. Alle (AnyConnect VPN-netwerken). Controleer ook of de juiste configuratie van de haarspelden is geïnstalleerd, zoals in de afbeelding wordt getoond.

| # | Dire... | Type | Source Interface ... | Destination Interface ... | Original Sources | Original Destinations | Original Services | Translated Sources | Translated Destinations | Translated Services | Options |
|---|---------|--------|----------------------|---------------------------|------------------|-----------------------|-------------------|--------------------|-------------------------|---------------------|----------------------------------|
| 1 | ↔ | Static | outside_int | outside_int | Anyconnect_Pool | Anyconnect_Pool | | Anyconnect_Pool | Anyconnect_Pool | | Dns:fail route-lc no-proxy |

Stap 2. Controleer het beleid voor toegangscontrole.

Zorg er na de configuratie van het toegangsbeleid voor dat verkeer vanaf de AnyConnect-clients is toegestaan, zoals in de afbeelding.

| # | 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 | Any | Allow |

2. AnyConnect-klienten met **hieronder gespecificeerde tunnelnetwerken** configuratie op zijn plaats.

Met **hieronder gespecificeerde tunnelnetwerken** Voor de AnyConnect-klienten wordt alleen specifiek verkeer doorgestuurd naar de VPN-tunnel. We moeten er echter voor zorgen dat het head-end beschikt over de juiste configuratie om communicatie binnen de AnyConnect-klienten mogelijk te maken.

Stap 1. Controleer de NAT-vrijstellingsconfiguratie.

Controleer **Stap 1** in de sectie **Toegestaan al verkeer via een tunnel**.

Stap 2. Controleer de configuratie van het tunneleffect.

Voor AnyConnect-klienten om tussen hen te communiceren, moeten we de VPN-pooladressen aan de Split-Tunnel ACL toevoegen.

- Volg **Stap 1** van het **AnyConnect-klienten hebben geen toegang tot interne bronnen** deel.
- Zorg ervoor dat het AnyConnect VPN-peernetwerk is opgenomen in de toegangslijst voor splitsen, zoals in de afbeelding.

Edit Standard Access List Object

? X

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

Opmerking: Als er meer dan één IP-pool is voor AnyConnect-clients en er behoefte is aan communicatie tussen de verschillende pools, zorg er dan voor dat u alle pools in de gesplitste tunneling ACL toevoegt, voegt u ook een NAT-vrijstellingsregel toe voor de benodigde IP-pools.

Stap 3. Controleer het beleid voor toegangscontrole.

Zorg ervoor dat verkeer van de AnyConnect-klanten is toegestaan zoals in de afbeelding.

| # | 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 | ✓ Allo |

AnyConnect-klanten kunnen geen telefoongesprekken instellen

Er zijn enkele scenario's waar AnyConnect-klanten telefoongesprekken en videoconferenties via VPN moeten opzetten.

AnyConnect-klanten kunnen zonder problemen verbinding maken met het AnyConnect-head-end. Ze kunnen interne en externe middelen bereiken, maar telefoongesprekken kunnen niet worden ingesteld.

In dit geval moeten we de volgende punten in overweging nemen:

- Netwerktopologie voor spraak.
- Betrokken protocollen. d.w.z. Session Initiation Protocol (SIP), Rapid Spanning Tree Protocol

(RSTP) enz.

- Hoe de VPN-telefoons aansluiten op de Cisco Unified Communications Manager (CUCM).

Standaard hebben FTD en ASA applicatie-inspectie die standaard ingeschakeld is in hun mondiale beleidskaart.

In de meeste gevallen zijn de VPN-telefoons niet in staat om een betrouwbare communicatie met de CUCM op te zetten omdat de AnyConnect-head-end een toepassingsinspectie heeft die het signaal- en spraakverkeer wijzigt.

Zie het volgende document voor meer informatie over de spraak- en videotoepping waarin u een toepassingsinspectie kunt uitvoeren:

[Hoofdstuk: Inspectie voor spraak- en videoprotocollen](#)

Om te bevestigen of een toepassingsverkeer door de globale beleidskaart wordt ingetrokken of gewijzigd kunnen we de **show service-beleid** opdracht gebruiken zoals hieronder wordt getoond.

```
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
```

```
.
```

In dit geval kunnen we zien hoe SIP-inspectie het verkeer vermindert.

Bovendien kan SIP-inspectie IP-adressen binnen de payload ook vertalen, niet in de IP-header, veroorzaakt verschillende problemen en wordt het aanbevolen om deze uit te schakelen wanneer we spraakservices via AnyConnect VPN willen gebruiken.

Om dit uit te schakelen, moeten we de volgende stappen uitvoeren:

Stap 1. Voer de geprivilegieerde EXEC-modus in.

Zie het volgende document voor meer informatie over de toegang tot deze modus:

[Hoofdstuk: Gebruik de opdrachtregel-interface \(CLI\)](#)

Stap 2. Controleer de algemene beleidskaart.

Start de volgende opdracht en controleer of SIP-inspectie is ingeschakeld.

```
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
```

Stap 3. Schakel SIP-inspectie uit.

Als de SIP-inspectie is ingeschakeld, schakelt u de opdracht hieronder uit vanaf de vloeiende melding:

```
> configure inspection sip disable
```

Stap 4. Controleer de Global Policy-map opnieuw.

Zorg ervoor dat de SIP-inspectie van de globale beleidslijn is uitgeschakeld:

```
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-klienten kunnen telefoonoproepen instellen, maar er is geen audio van de oproepen

Zoals vermeld in de vorige sectie, is het zeer vaak nodig voor AnyConnect-klienten om telefoongesprekken in te stellen wanneer verbonden met VPN. In sommige gevallen kan de oproep worden opgesteld, maar klanten kunnen er een gebrek aan audio op ervaren. Dit geldt voor de volgende scenario's:

- Geen audio op de verbinding tussen een AnyConnect-client en een extern nummer.
- Geen audio op de verbinding tussen een AnyConnect-client en een andere AnyConnect-client.

Om dit op te lossen, kunnen we de volgende stappen volgen:

Stap 1. Controleer de configuratie van het tunneleffect.

- Navigeren in naar het gebruik van het verbindingsprofiel om verbinding te maken met: **Apparaten > VPN > Externe toegang > Connection Profile > Selecteren van het profiel.**
- Navigeer aan het groepsbeleid dat aan dat Profile: **Bewerken Groepsbeleid > Algemeen is**

toegewezen.

- Controleer de configuratie van Split-tunneling, zoals in de afbeelding wordt getoond.

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

- Indien ingesteld als **hieronder gespecificeerde tunnelnetwerken** Controleer de configuratie van de toegangslijst: **Objecten > Objectbeheer > Toegangslijst > Bewerken voor Split-tunneling**.
- Zorg ervoor dat de spraakservers en de AnyConnect IP-peernetwerken zijn opgenomen in de toegangslijst voor splitsen, zoals in de afbeelding.

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

Stap 2. Controleer de NAT-vrijstellingsconfiguratie.

NAT-vrijstellingsregels moeten zo worden geconfigureerd dat zij het AnyConnect VPN-netwerk vrijstellen van het Spraakservernetwerk en dat zij tevens bidirectionele communicatie binnen de AnyConnect-klienten mogelijk maken.

- Navigeren naar de NAT-configuratie: **Apparaten > NAT**.
- Zorg ervoor dat de NAT-vrijstellingsregel is ingesteld voor de juiste bron- (spraakservers) en doelnetwerken (AnyConnect VPN-pool) en dat de NAT-regel is ingesteld om AnyConnect-client naar AnyConnect-client te laten communiceren. Bovendien, controleer dat de juiste binnen en uitgaande interfaceconfiguratie op zijn plaats is voor elke regel, per uw netwerkontwerp, zoals in het beeld getoond wordt.

Rules

Filter by Device

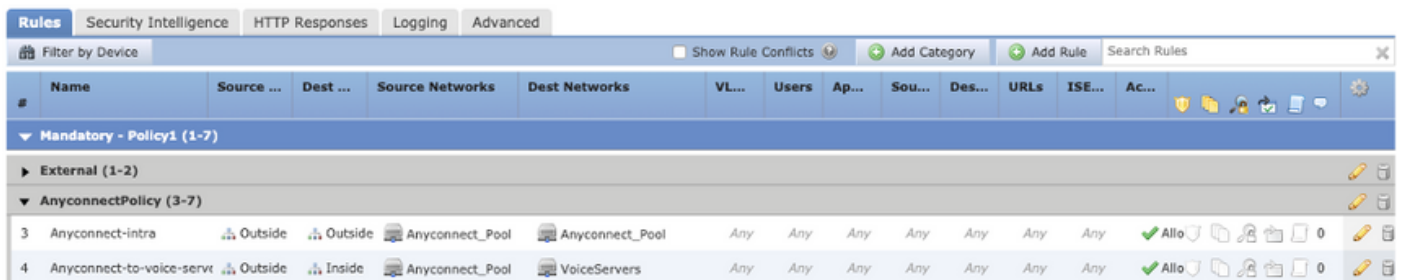
| #.. | Dir... | T... | Original Packet | | | | Translated Packet | | | | Options |
|--------------------|--------|------|------------------------|-------------------------------|-----------------------|-----------------------|-----------------------|--------------------|-------------------------|-----------|-------------------------------------|
| | | | Source Interface Ob... | Destination Interface Obje... | 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-look no-proxy |
| 2 | ↔ | S... | Inside_interfac | outside_interface | VoiceServers | Anyconnect_Pool | VoiceServers | Anyconnect_Pool | | | Dns:false route-look no-proxy |
| 3 | ↔ | S... | outside_interfa | outside_interface | Anyconnect_Pool | Anyconnect_Pool | Anyconnect_Pool | Anyconnect_Pool | | | Dns:false route-look no-proxy |

Stap 3. Controleer dat de SIP-inspectie is uitgeschakeld.

Bekijk de vorige sectie **AnyConnect-klienten kunnen geen telefoongesprekken instellen** om te weten hoe te om SIP inspectie uit te schakelen.

Stap 4. Controleer het beleid voor toegangscontrole.

Zorg er na uw configuratie voor toegangsbeleid voor dat het verkeer van de AnyConnect-clients wordt toegestaan om de spraakservers en de bijbehorende netwerken te bereiken, zoals in de afbeelding.



The screenshot shows the Cisco ASA configuration interface for rules. The 'Rules' tab is active, and the 'Mandatory - Policy1 (1-7)' policy is expanded to show the 'AnyconnectPolicy (3-7)' section. Two rules are visible:

| # | 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 | Any | Allo | | | | 0 |
| 4 | Anyconnect-to-voice-servr | Outside | Inside | Anyconnect_Pool | VoiceServers | Any | Any | Any | Any | Any | Any | Any | Any | Allo | | | | 0 |

Gerelateerde informatie

- Deze video geeft het configuratievoorbeeld voor de verschillende problemen die in dit document worden besproken.
- Voor extra hulp kunt u contact opnemen met het Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: [Cisco's wereldwijde contactgegevens voor ondersteuning](#).
- U kunt ook de Cisco VPN-community bezoeken [hier](#).