

Fehlerbehebung bei häufigen AnyConnect-Kommunikationsproblemen in FTD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Empfohlener Fehlerbehebungsprozess](#)

[AnyConnect-Clients können nicht auf interne Ressourcen zugreifen](#)

[AnyConnect-Clients haben keinen Internetzugang](#)

[AnyConnect-Clients können nicht miteinander kommunizieren](#)

[AnyConnect-Clients können keine Telefonanrufe herstellen](#)

[AnyConnect-Clients können Telefonanrufe herstellen, es ist jedoch kein Audio bei den Anrufen vorhanden.](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie einige der häufigsten Kommunikationsprobleme des Cisco AnyConnect Secure Mobility Client auf Firepower Threat Defense (FTD) beheben können, wenn dieser entweder Secure Socket Layer (SSL) oder Internet Key Exchange Version 2 (IKEv2) verwendet.

Unterstützt von Angel Ortiz und Fernando Jimenez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTD verwaltet durch FMC 6.4.0.
- AnyConnect 4.8

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Empfohlener Fehlerbehebungsprozess

In diesem Leitfaden wird erläutert, wie Sie einige häufige Kommunikationsprobleme von AnyConnect-Clients beheben können, wenn die FTD als VPN-Gateway (Remote Access Virtual Private Network) verwendet wird. In diesen Abschnitten werden die folgenden Probleme behandelt und erläutert:

- AnyConnect-Clients können nicht auf interne Ressourcen zugreifen.
- AnyConnect-Clients haben keinen Internetzugang.
- AnyConnect-Clients können nicht miteinander kommunizieren.
- AnyConnect-Clients können keine Telefonanrufe herstellen.
- AnyConnect-Clients können Telefonanrufe herstellen. Es ist jedoch kein Audio bei den Anrufen verfügbar.

AnyConnect-Clients können nicht auf interne Ressourcen zugreifen

Führen Sie diese Schritte aus:

Schritt 1: Überprüfen der Split-Tunnelkonfiguration

- Navigieren Sie zum Verbindungsprofil, mit dem AnyConnect-Clients verbunden sind: **Geräte > VPN > Remote Access > Connection Profile > Select the Profile (Profil auswählen)**
- Navigieren Sie zu der Gruppenrichtlinie, die dieser Profile: **Gruppenrichtlinie > Allgemein** zugewiesen ist.
- Überprüfen Sie die Split Tunneling-Konfiguration, wie im Bild gezeigt.

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

- Wenn es als **Tunnelnetzwerke** konfiguriert ist, **wie unten angegeben**, überprüfen Sie die Konfiguration der Zugriffssteuerungsliste (ACL):

Navigieren Sie zu **Objekte > Objektverwaltung > Zugriffsliste > Zugriffsliste bearbeiten für das Getrennte-Tunneling**.

- Stellen Sie sicher, dass die Netzwerke, auf die Sie über den AnyConnect VPN-Client zugreifen möchten, in dieser Zugriffsliste aufgeführt sind, wie im Bild gezeigt.

Edit Standard Access List Object



Name: Split-tunnel-ACL

Entries (1)

Sequence No	Action	Network
1	✓ Allow	InternalNetwork1 InternalNetwork2 InternalNetwork3

Allow Overrides

Save Cancel

Schritt 2: Verifizieren der Network Address Translation (NAT)-Ausnahmekonfiguration.

Denken Sie daran, dass wir eine NAT-Freistellungsregel konfigurieren müssen, um zu verhindern, dass Datenverkehr in die IP-Adresse der Schnittstelle übersetzt wird, die normalerweise für den Internetzugriff konfiguriert ist (mit Port Address Translation (PAT)).

- Navigieren Sie zur NAT-Konfiguration: **Geräte > NAT**.
- Stellen Sie sicher, dass die NAT-Freistellungsregel für die richtigen Quell- (internen) und Zielnetzwerke (AnyConnect VPN Pool) konfiguriert ist. Überprüfen Sie außerdem, ob die richtige Quell- und Zielschnittstelle ausgewählt wurde, wie im Bild gezeigt.

Rules

Filter by Device

Original Packet Translated Packet

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

Anmerkung: Wenn NAT-Freistellungsregeln konfiguriert sind, überprüfen Sie **no-proxy-arp** und führen Sie **Route-Lookup**-Optionen als Best Practice durch.

Schritt 3: Überprüfen der Zugriffskontrollrichtlinie

Stellen Sie gemäß der Konfiguration der Zugriffskontrollrichtlinie sicher, dass der Datenverkehr von den AnyConnect-Clients die ausgewählten internen Netzwerke erreichen darf, wie im Bild gezeigt.

#	Name	Source ...	Dest ...	Source Networks	Dest Networks	VL...	Users	Ap...	Sou...	Des...	URLs	ISE...	Ac...
Mandatory - Policy1 (1-3)													
External (1-2)													
AnyconnectPolicy (3-3)													
3	Anyconnect-to-internal	Outside	Inside	Anyconnect_Pool	InternalNetworksGroup	Any	Any	Any	Any	Any	Any	Any	Any

AnyConnect-Clients haben keinen Internetzugang

Für dieses Problem gibt es zwei mögliche Szenarien.

1. Der für das Internet bestimmte Datenverkehr darf nicht durch den VPN-Tunnel geleitet werden.

Stellen Sie sicher, dass die Gruppenrichtlinie für das Split-Tunneling als **Tunnelnetzwerke** konfiguriert ist, **die unten angegeben sind** und NICHT als **Zulassen des gesamten Datenverkehrs über Tunnel**, wie im Bild gezeigt.

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. Der für das Internet bestimmte Datenverkehr muss den VPN-Tunnel durchlaufen.

In diesem Fall ist die häufigste Gruppenrichtlinien-Konfiguration für Split-Tunneling die Option **Gesamten Datenverkehr über Tunnel zulassen**, wie im Bild gezeigt.

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

Schritt 1: Überprüfung der NAT-Ausnahmekonfiguration für die Erreichbarkeit des internen Netzwerks

Denken Sie daran, dass wir weiterhin eine NAT-Freistellungsregel konfigurieren müssen, um Zugriff auf das interne Netzwerk zu erhalten. Bitte lesen Sie **Schritt 2** des **AnyConnect-Clients können nicht auf interne Ressourcen zugreifen** Abschnitt.

Schritt 2: Überprüfen der Hairpinning-Konfiguration für dynamische Übersetzungen

Damit AnyConnect-Clients über den VPN-Tunnel auf das Internet zugreifen können, müssen wir sicherstellen, dass die Hairpinning NAT-Konfiguration für den Datenverkehr korrekt ist, der in die IP-Adresse der Schnittstelle übersetzt werden soll.

- Navigieren Sie zur NAT-Konfiguration: **Geräte > NAT**.
- Stellen Sie sicher, dass die Dynamic NAT-Regel für die richtige Schnittstelle (Internet Service Provider (ISP)-Verbindung) als Quelle und Ziel (Hairpinning) konfiguriert ist. Überprüfen Sie außerdem, ob das Netzwerk, das für den AnyConnect VPN-Adresspool verwendet wird, in der Original-Quelle und der Ziel-**Schnittstellen-IP** ausgewählt ist. ist für Translated source ausgewählt, wie im Bild gezeigt.

#	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!

Schritt 3: Überprüfen der Zugriffskontrollrichtlinie

Stellen Sie gemäß der Konfiguration der Zugriffskontrollrichtlinie sicher, dass der Datenverkehr von den AnyConnect-Clients die externen Ressourcen erreichen darf, wie im Bild gezeigt.

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

AnyConnect-Clients können nicht miteinander kommunizieren

Es gibt zwei mögliche Szenarien für dieses Problem:

1. AnyConnect-Clients mit **Zulassen des gesamten Datenverkehrs über Tunnel** Konfiguration implementiert.
 2. AnyConnect-Clients mit **Tunnel-Netzwerke weiter unten spezifiziert** Konfiguration implementiert.
1. AnyConnect-Clients mit **Zulassen des gesamten Datenverkehrs über Tunnel** Konfiguration implementiert.

Wann **Zulassen des gesamten Datenverkehrs über Tunnel** ist für AnyConnect konfiguriert, bedeutet, dass der gesamte interne und externe Datenverkehr an das AnyConnect-Headend weitergeleitet werden muss. Dies wird zu einem Problem, wenn Sie über NAT für den öffentlichen Internetzugriff verfügen, da der Datenverkehr von einem AnyConnect-Client, der an einen anderen AnyConnect-Client gerichtet ist, in die IP-Adresse der Schnittstelle umgewandelt wird und daher die Kommunikation fehlschlägt.

Schritt 1: Überprüfen der Konfiguration der NAT-Ausnahme

Um dieses Problem zu beheben, muss eine manuelle NAT-Ausnahmeregel konfiguriert werden, die eine bidirektionale Kommunikation innerhalb der AnyConnect-Clients ermöglicht.

- Navigieren Sie zur NAT-Konfiguration: **Geräte > NAT**.
- Stellen Sie sicher, dass die NAT-Freistellungsregel für die richtige Quelle (AnyConnect VPN Pool) und das richtige Ziel konfiguriert ist. (AnyConnect VPN Pool)-Netzwerke. Überprüfen Sie auch, ob die richtige Haarnadelkonfiguration vorhanden ist, wie im Bild gezeigt.

#	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-ic no-proxy

Schritt 2: Überprüfen der Zugriffskontrollrichtlinie

Stellen Sie gemäß der Konfiguration der Zugriffskontrollrichtlinie sicher, dass Datenverkehr von den AnyConnect-Clients zulässig ist, wie im Bild gezeigt.

#	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

2. AnyConnect-Clients **Tunnel-Netzwerke weiter unten spezifiziert** Konfiguration implementiert.

Mit **Tunnel-Netzwerke weiter unten spezifiziert** für die AnyConnect-Clients konfiguriert, wird nur der spezifische Datenverkehr durch den VPN-Tunnel weitergeleitet. Wir müssen jedoch sicherstellen, dass das Headend über die richtige Konfiguration verfügt, um die Kommunikation innerhalb der AnyConnect-Clients zu ermöglichen.

Schritt 1: Überprüfen der Konfiguration der NAT-Ausnahme

Aktivieren Sie **Schritt 1** im Abschnitt **Zulassen des gesamten Datenverkehrs über Tunnel**.

Schritt 2: Überprüfen der Split-Tunneling-Konfiguration

Damit AnyConnect-Clients miteinander kommunizieren können, müssen die Adressen des VPN-Pools der Split-Tunnel-ACL hinzugefügt werden.


- Befolgen Sie **Schritt 1** des **AnyConnect-Clients können nicht auf interne Ressourcen zugreifen** Abschnitt.
- Stellen Sie sicher, dass das AnyConnect VPN Pool-Netzwerk in der Zugriffsliste für Split-Tunneling aufgeführt ist, wie im Bild gezeigt.









Edit Standard Access List Object

? X

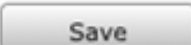
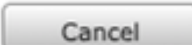
Name

▲ Entries (2)



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

Allow Overrides

Anmerkung: Wenn mehr als ein IP-Pool für AnyConnect-Clients vorhanden ist und eine Kommunikation zwischen den verschiedenen Pools erforderlich ist, stellen Sie sicher, dass alle Pools in der Split-Tunneling-ACL hinzugefügt werden. Fügen Sie außerdem eine NAT-Freistellungsregel für die erforderlichen IP-Pools hinzu.

Schritt 3: Überprüfen der Zugriffskontrollrichtlinie

Stellen Sie sicher, dass Datenverkehr von den AnyConnect-Clients wie im Bild gezeigt zulässig ist.



The screenshot shows the Cisco ISE Policy Editor interface. The 'Rules' tab is active, and the 'AnyconnectPolicy (3-6)' is expanded. A rule named 'Anyconnect-intra' is visible with the following configuration:

#	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	 

AnyConnect-Clients können keine Telefonanrufe herstellen

Es gibt einige Szenarien, in denen AnyConnect-Clients Telefonanrufe und Videokonferenzen über VPN einrichten müssen.

AnyConnect-Clients können problemlos eine Verbindung mit dem AnyConnect-Headend herstellen. Sie können interne und externe Ressourcen erreichen, Telefonanrufe können jedoch nicht eingerichtet werden.

In diesem Fall müssen folgende Punkte berücksichtigt werden:

- Netzwerktopologie für Sprache.

- Hierbei handelt es sich um Protokolle. z. B. Session Initiation Protocol (SIP), Rapid Spanning Tree Protocol (RSTP) usw.
- Verbindung der VPN-Telefone mit dem Cisco Unified Communications Manager (CUCM)

In der globalen Richtlinienzuweisung ist die Anwendungsinspektion für FTD und ASA standardmäßig aktiviert.

In den meisten Fällen können die VPN-Telefone keine zuverlässige Kommunikation mit dem CUCM herstellen, da für das AnyConnect-Headend eine Anwendungsinspektion aktiviert ist, die den Signal- und Sprachverkehr ändert.

Weitere Informationen zur Sprach- und Videoanwendung, in der Sie die Anwendungsprüfung durchführen können, finden Sie im folgenden Dokument:

[Kapitel: Überprüfung auf Sprach- und Videoprotokolle](#)

Um zu überprüfen, ob ein Anwendungsdatenverkehr durch die globale Richtlinienzuordnung verworfen oder geändert wird, können Sie den folgenden Befehl **show service-policy** verwenden.

```
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 diesem Fall sehen wir, wie die SIP-Inspektion den Datenverkehr verwirft.

Darüber hinaus kann die SIP-Prüfung auch IP-Adressen innerhalb der Nutzlast übersetzen, nicht im IP-Header. Daher wird empfohlen, diese zu deaktivieren, wenn Sprachdienste über AnyConnect VPN verwendet werden sollen.

Um diese Funktion zu deaktivieren, müssen die nächsten Schritte ausgeführt werden:

Schritt 1: Wechseln Sie in den privilegierten EXEC-Modus.

Weitere Informationen zum Zugriff auf diesen Modus finden Sie im folgenden Dokument:

[Kapitel: Verwenden der Befehlszeilenschnittstelle \(CLI\)](#)

Schritt 2: Überprüfen Sie die globale Richtlinienzuweisung.

Führen Sie den nächsten Befehl aus, und überprüfen Sie, ob SIP Inspection aktiviert ist.

```
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
```

Schritt 3: Deaktivieren Sie die SIP-Prüfung.

Wenn die SIP-Inspektion aktiviert ist, deaktivieren Sie den folgenden Befehl von der Eingabeaufforderung aus:

```
> configure inspection sip disable
```

Schritt 4: Überprüfen Sie erneut die globale Richtlinienzuweisung.

Stellen Sie sicher, dass die SIP-Inspektion in der globalen Richtlinienzuordnung deaktiviert ist:

```
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-Clients können Telefonanrufe herstellen, es ist jedoch kein Audio bei den Anrufen vorhanden.

Wie im vorherigen Abschnitt erwähnt, besteht eine sehr häufige Anforderung für AnyConnect-Clients darin, Anrufe herzustellen, wenn eine Verbindung mit dem VPN hergestellt wird. In einigen Fällen kann der Anruf eingerichtet werden, es kann jedoch zu Audioausfällen beim Kunden kommen. Dies gilt für die folgenden Szenarien:

- Keine Audioverbindung zwischen einem AnyConnect-Client und einer externen Rufnummer.
- Zwischen einem AnyConnect-Client und einem anderen AnyConnect-Client besteht kein Audio.

Um dies zu beheben, können wir die folgenden Schritte ausführen:

Schritt 1: Überprüfen der Split-Tunneling-Konfiguration

- Navigieren Sie zur Connection Profile-Funktion, mit der Sie eine Verbindung herstellen können: **Geräte > VPN > Remote Access > Connection Profile > Select the Profile (Profil auswählen)**
- Navigieren Sie zu der Gruppenrichtlinie, die dieser Profile: **Gruppenrichtlinie > Allgemein**

zugewiesen ist.

- Überprüfen Sie die Split Tunneling-Konfiguration, wie im Bild gezeigt.

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

- Wird konfiguriert als **Tunnel-Netzwerke weiter unten spezifiziert**überprüfen Sie die Konfiguration der Zugriffsliste: **Objekte > Objektverwaltung > Zugriffsliste > Zugriffsliste bearbeiten für Split-Tunneling.**
- Stellen Sie sicher, dass die Sprachserver und die AnyConnect IP Pool-Netzwerke in der Zugriffsliste für Split-Tunneling aufgeführt sind, wie im Bild gezeigt.

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

Schritt 2: Überprüfen der Konfiguration der NAT-Ausnahme

NAT-Freistellungsregeln müssen so konfiguriert werden, dass der Datenverkehr vom AnyConnect VPN-Netzwerk zum Sprach-Server-Netzwerk sowie die bidirektionale Kommunikation innerhalb der AnyConnect-Clients ausgeschlossen werden.

- Navigieren Sie zur NAT-Konfiguration: **Geräte > NAT**.
- Stellen Sie sicher, dass die NAT-Freistellungsregel für die richtigen Quell- (Voice Server) und Zielnetzwerke (AnyConnect VPN Pool) und die Hairpin-NAT-Regel konfiguriert ist, um die Kommunikation zwischen dem AnyConnect-Client und dem AnyConnect-Client zuzulassen. Überprüfen Sie außerdem, ob für jede Regel die richtige Konfiguration der ein- und ausgehenden Schnittstellen gemäß Ihrem Netzwerkdesign vorhanden ist (siehe Bild).

Rules

Filter by Device

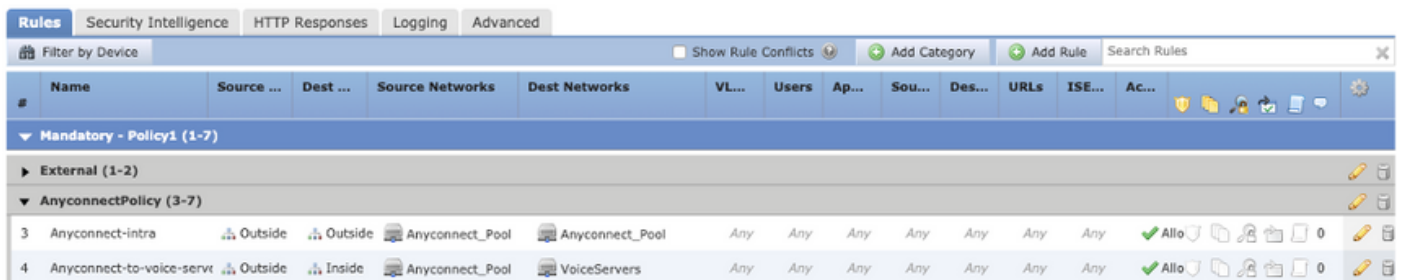
#..	Dir...	T...	Original Packet				Translated Packet				Options
			Source Interface Ob...	Destination Interface Obj...	Original Sources	Original Destinations	O... S...	Translated Sources	Translated Destinations	T... S...	
▼ NAT Rules Before											
1	↔	S...	Inside_interfac	outside_interface	InternalNetworksGroup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

Schritt 3: Überprüfen Sie, ob die SIP-Inspektion deaktiviert ist.

Lesen Sie den vorherigen Abschnitt. AnyConnect-Clients können keine Telefonanrufe herstellen um zu erfahren, wie die SIP-Inspektion deaktiviert wird.

Schritt 4: Überprüfen der Zugriffskontrollrichtlinie

Stellen Sie gemäß der Konfiguration der Zugriffskontrollrichtlinie sicher, dass Datenverkehr von den AnyConnect-Clients die Sprachserver und die beteiligten Netzwerke erreichen darf, wie im Bild gezeigt.



#	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	Any	✓ Allow				0
4	Anyconnect-to-voice-servr	Outside	Inside	Anyconnect_Pool	VoiceServers	Any	Any	Any	Any	Any	Any	Any	Any	✓ Allow				0

Zugehörige Informationen

- Dieses Video enthält das Konfigurationsbeispiel für die verschiedenen in diesem Dokument besprochenen Probleme.
- Weitere Unterstützung erhalten Sie vom Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: [Weltweiter Kontakt zum Cisco Support](#).
- Sie können auch die Cisco VPN Community besuchen. [hier](#).