

Dépannage des problèmes courants de communication AnyConnect sur FTD

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Processus de dépannage recommandé](#)

[Les clients AnyConnect ne peuvent pas accéder aux ressources internes](#)

[Les clients AnyConnect n'ont pas d'accès à Internet](#)

[Les clients AnyConnect ne peuvent pas communiquer entre eux](#)

[Les clients AnyConnect ne peuvent pas établir d'appels téléphoniques](#)

[Les clients AnyConnect peuvent établir des appels téléphoniques, mais il n'y a pas d'audio sur les appels](#)

[Informations connexes](#)

Introduction

Ce document décrit comment résoudre certains des problèmes de communication les plus courants du client Cisco AnyConnect Secure Mobility sur Firepower Threat Defense (FTD) lorsqu'il utilise SSL (Secure Socket Layer) ou IKEv2 (Internet Key Exchange version 2).

Contribution d'Angel Ortiz et Fernando Jimenez, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Client de mobilité sécurisée Cisco AnyConnect.
- Cisco FTD.
- Cisco Firepower Management Center (FMC).

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FTD géré par FMC 6.4.0.
- AnyConnect 4.8.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Processus de dépannage recommandé

Ce guide explique comment résoudre certains problèmes de communication courants que rencontrent les clients AnyConnect lorsque le FTD est utilisé comme passerelle de réseau privé virtuel (VPN) d'accès distant. Ces sections traitent des problèmes ci-dessous et leur apportent des solutions :

- Les clients AnyConnect ne peuvent pas accéder aux ressources internes.
- Les clients AnyConnect ne disposent pas d'accès à Internet.
- Les clients AnyConnect ne peuvent pas communiquer entre eux.
- Les clients AnyConnect ne peuvent pas établir d'appels téléphoniques.
- Les clients AnyConnect peuvent établir des appels téléphoniques. Cependant, il n'y a pas d'audio sur les appels.

Les clients AnyConnect ne peuvent pas accéder aux ressources internes

Procédez comme suit :

Étape 1. Vérifiez la configuration du tunnel partagé.

- Accédez au profil de connexion auquel les clients AnyConnect sont connectés : **Devices > VPN > Remote Access > Connection Profile > Sélectionnez le profil.**
- Accédez à la stratégie de groupe affectée à cette **stratégie de groupe** Profile: **> Général.**
- Vérifiez la configuration du fractionnement en canaux, comme illustré dans l'image.

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:

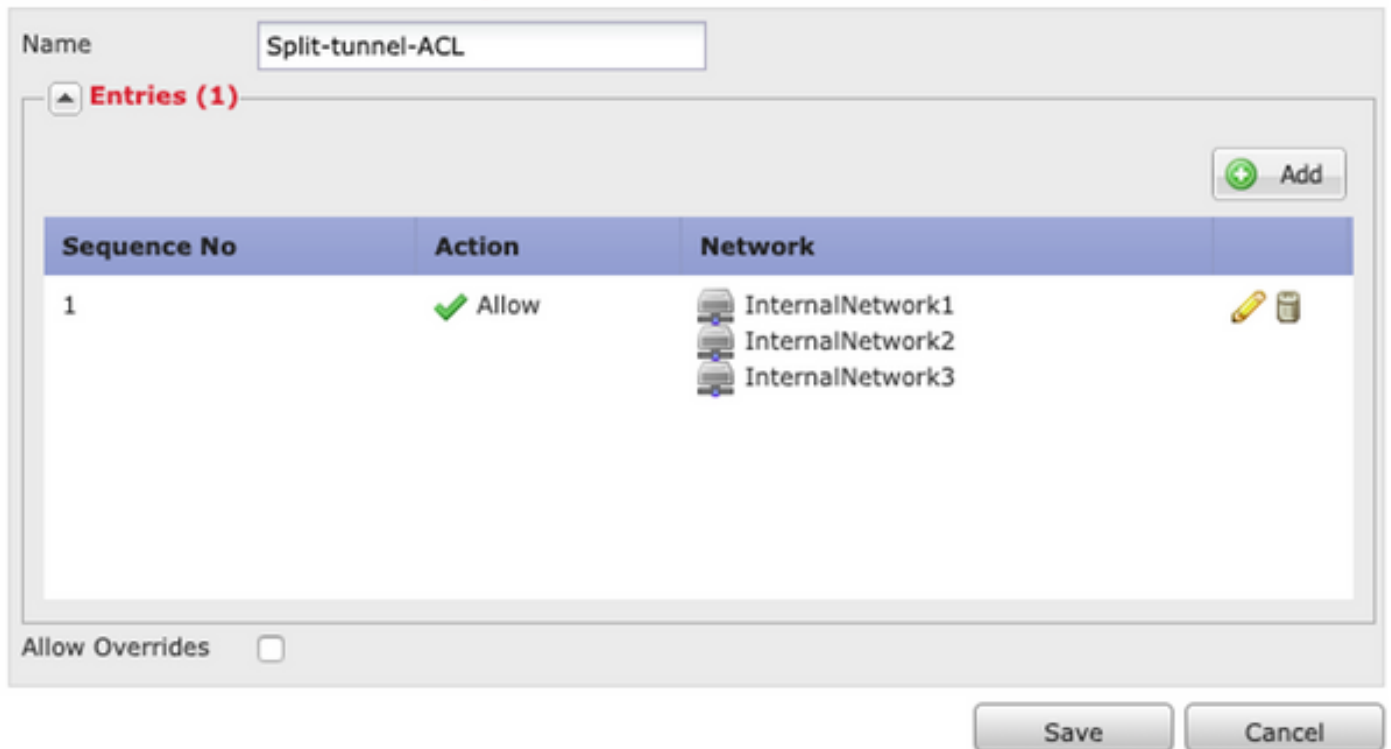
Save Cancel

- S'il est configuré en tant que **réseaux de tunnel spécifiés** ci-dessous, vérifiez la configuration de la liste de contrôle d'accès (ACL) :

Accédez à **Objets > Gestion des objets > Liste d'accès > Modifier la liste d'accès pour la transmission tunnel partagée.**

- Assurez-vous que les réseaux que vous essayez d'atteindre à partir du client VPN AnyConnect figurent dans cette liste d'accès, comme l'illustre l'image.

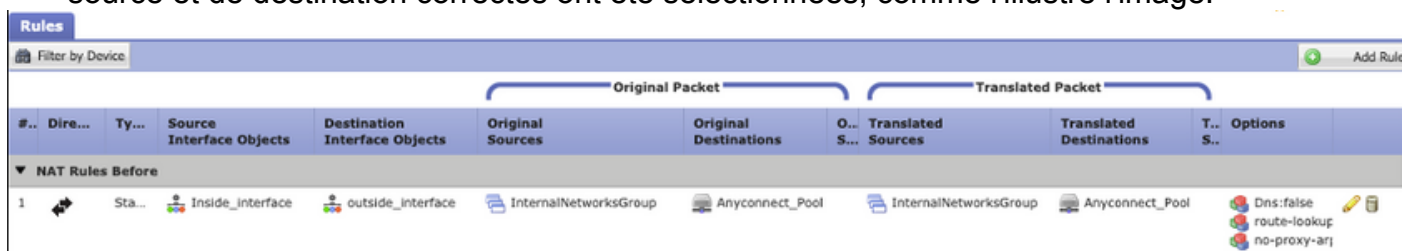
Edit Standard Access List Object



Étape 2. Vérifiez la configuration de l'exemption NAT (Network Address Translation).

N'oubliez pas que nous devons configurer une règle d'exemption NAT pour éviter que le trafic ne soit traduit en adresse IP d'interface, généralement configurée pour l'accès Internet (avec traduction d'adresses de port (PAT)).

- Accédez à la configuration NAT : **Périphériques > NAT**.
- Assurez-vous que la règle d'exemption NAT est configurée pour les réseaux source (interne) et de destination corrects (pool VPN AnyConnect). Vérifiez également que les interfaces source et de destination correctes ont été sélectionnées, comme l'illustre l'image.



Note: Lorsque des règles d'exemption NAT sont configurées, vérifiez le **no-proxy-arp** et exécutez des options de **recherche de route** comme meilleure pratique.

Étape 3. Vérifiez la stratégie de contrôle d'accès.

Conformément à votre configuration de stratégie de contrôle d'accès, assurez-vous que le trafic provenant des clients AnyConnect est autorisé à atteindre les réseaux internes sélectionnés, comme l'illustre l'image.

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

Les clients AnyConnect n'ont pas d'accès à Internet

Il existe deux scénarios possibles pour ce problème.

1. Le trafic destiné à Internet ne doit pas passer par le tunnel VPN.

Assurez-vous que la stratégie de groupe est configurée pour la transmission tunnel partagée en tant que **réseaux de tunnel spécifiés ci-dessous** et NON comme **Autoriser tout le trafic sur le tunnel**, comme illustré dans l'image.

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. Le trafic destiné à Internet doit passer par le tunnel VPN.

Dans ce cas, la configuration de stratégie de groupe la plus courante pour la transmission tunnel partagée serait de sélectionner **Autoriser tout le trafic sur le tunnel**, comme illustré dans l'image.

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

Étape 1. Vérifiez la configuration de l'exemption NAT pour l'accessibilité du réseau interne.

N'oubliez pas que nous devons toujours configurer une règle d'exemption NAT pour avoir accès au réseau interne. Veuillez passer en revue l'étape 2 du **Les clients AnyConnect ne peuvent pas accéder aux ressources internes** de la section.

Étape 2. Vérifier la configuration de la reconnexion pour les traductions dynamiques.

Pour que les clients AnyConnect puissent accéder à Internet via le tunnel VPN, nous devons nous assurer que la configuration NAT de renvoi est correcte pour que le trafic soit traduit vers l'adresse IP de l'interface.

- Accédez à la configuration NAT : **Périphériques > NAT**.
- Assurez-vous que la règle NAT dynamique est configurée pour l'interface correcte (liaison du fournisseur d'accès à Internet) comme source et destination (renvoi). Vérifiez également que le réseau utilisé pour le pool d'adresses VPN AnyConnect est sélectionné dans la source d'origine et l'**adresse IP** de l'**interface** de destination est sélectionnée pour la source traduite, comme l'illustre l'image.

#	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

Étape 3. Vérifiez la stratégie de contrôle d'accès.

Conformément à votre configuration de stratégie de contrôle d'accès, assurez-vous que le trafic provenant des clients AnyConnect est autorisé à atteindre les ressources externes, comme l'illustre l'image.

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

Les clients AnyConnect ne peuvent pas communiquer entre eux

Il existe deux scénarios possibles pour ce problème :

1. Clients AnyConnect avec **Autoriser tout le trafic sur le tunnel** configuration en place.
2. Clients AnyConnect avec **Réseaux de tunnel spécifiés ci-dessous** configuration en place.

1. Clients AnyConnect avec **Autoriser tout le trafic sur le tunnel** configuration en place.

Quand **Autoriser tout le trafic sur le tunnel** est configuré pour AnyConnect signifie que tout le trafic, interne et externe, doit être transféré à la tête de réseau AnyConnect. Cela devient un problème lorsque vous avez NAT pour l'accès Internet public, puisque le trafic provient d'un client AnyConnect destiné à un autre client AnyConnect est traduit en adresse IP d'interface et par conséquent la communication échoue.

Étape 1. Vérifiez la configuration de l'exemption NAT.

Afin de résoudre ce problème, une règle d'exemption NAT manuelle doit être configurée pour permettre la communication bidirectionnelle au sein des clients AnyConnect.

- Accédez à la configuration NAT : **Périphériques > NAT**.
- Assurez-vous que la règle d'exemption NAT est configurée pour la source (pool VPN AnyConnect) et la destination correctes. (AnyConnect VPN Pool). Vérifiez également que la configuration de la broche à oreilles est correcte, comme l'illustre l'image.

#	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-lc no-prox

Étape 2. Vérifiez la stratégie de contrôle d'accès.

Conformément à votre configuration de stratégie de contrôle d'accès, assurez-vous que le trafic en provenance des clients AnyConnect est autorisé, comme l'illustre l'image.



2. Anyconnect clients avec **Réseaux de tunnel spécifiés ci-dessous** configuration en place.

Avec **Réseaux de tunnel spécifiés ci-dessous** configuré pour les clients AnyConnect, seul le trafic spécifique est transféré vers via le tunnel VPN. Cependant, nous devons nous assurer que la tête de réseau a la configuration appropriée pour permettre la communication au sein des clients AnyConnect.

Étape 1. Vérifiez la configuration de l'exemption NAT.

Cochez **Étape 1**, dans la section **Autoriser tout le trafic sur le tunnel**.

Étape 2. Vérifiez la configuration de la transmission tunnel partagée.

Pour que les clients AnyConnect puissent communiquer entre eux, nous devons ajouter les adresses du pool VPN dans la liste de contrôle d'accès Split-Tunnel.

- Suivez l'étape 1 du **Les clients AnyConnect ne peuvent pas accéder aux ressources internes** de la section.
- Assurez-vous que le réseau du pool de VPN AnyConnect figure dans la liste d'accès à la transmission tunnel partagée, comme l'illustre l'image.

Edit Standard Access List Object

? X

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

Note: S'il existe plusieurs pools d'adresses IP pour les clients AnyConnect et qu'une communication entre les différents pools est nécessaire, assurez-vous d'ajouter tous les pools dans la liste de contrôle d'accès de tunnelisation fractionnée et ajoutez également une règle d'exemption NAT pour les pools d'adresses IP nécessaires.

Étape 3. Vérifiez la stratégie de contrôle d'accès.

Assurez-vous que le trafic provenant des clients AnyConnect est autorisé, comme le montre l'image.

#	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

Les clients AnyConnect ne peuvent pas établir d'appels téléphoniques

Il existe certains scénarios dans lesquels les clients AnyConnect doivent établir des appels téléphoniques et des vidéoconférences sur VPN.

Les clients AnyConnect peuvent se connecter à la tête de réseau AnyConnect sans problème. Ils peuvent atteindre des ressources internes et externes, mais les appels téléphoniques ne peuvent pas être établis.

Dans ce cas, nous devons examiner les points suivants :

- Topologie réseau pour la voix.

- Protocoles impliqués. C'est-à-dire le protocole SIP (Session Initiation Protocol), le protocole Spanning Tree rapide (RSTP), etc.
- Comment les téléphones VPN se connectent à Cisco Unified Communications Manager (CUCM).

Par défaut, FTD et ASA ont activé l'inspection des applications par défaut dans leur carte de stratégie globale.

Dans la plupart des cas, les téléphones VPN ne sont pas en mesure d'établir une communication fiable avec le CUCM, car l'inspection des applications activée sur la tête de réseau AnyConnect modifie le trafic voix et signal.

Pour plus d'informations sur l'application voix et vidéo dans laquelle vous pouvez appliquer l'inspection d'application, reportez-vous au document suivant :

[Chapitre : Inspection des protocoles voix et vidéo](#)

Afin de confirmer si un trafic d'application est abandonné ou modifié par la carte-politique globale, nous pouvons utiliser la commande **show service-policy** comme indiqué ci-dessous.

```
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
```

```
.
```

Dans ce cas, nous pouvons voir comment l'inspection SIP supprime le trafic.

En outre, l'inspection SIP peut également traduire des adresses IP à l'intérieur de la charge utile, et non dans l'en-tête IP, cause des problèmes différents, il est donc recommandé de la désactiver lorsque nous voulons utiliser des services vocaux sur AnyConnect VPN.

Pour la désactiver, nous devons effectuer les étapes suivantes :

Étape 1. Passez en mode privilégié.

Pour plus d'informations sur l'accès à ce mode, reportez-vous au document suivant :

[Chapitre : Utiliser l'interface de ligne de commande \(CLI\)](#)

Étape 2. Vérifiez la carte de stratégie globale.

Exécutez la commande suivante et vérifiez si l'inspection SIP est activée.

```
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

Étape 3. Désactivez l'inspection SIP.

Si l'inspection SIP est activée, désactivez la commande en cours ci-dessous à partir de l'invite de conclusion :

> configure inspection sip disable

Étape 4. Vérifiez à nouveau la carte de stratégie globale.

Assurez-vous que l'inspection SIP est désactivée à partir de la carte de stratégie globale :

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
```

Les clients AnyConnect peuvent établir des appels téléphoniques, mais il n'y a pas d'audio sur les appels

Comme indiqué dans la section précédente, un besoin très courant pour les clients AnyConnect est d'établir des appels téléphoniques lorsqu'ils sont connectés au VPN. Dans certains cas, l'appel peut être établi, mais les clients peuvent ne pas avoir accès à l'audio. Cela s'applique aux scénarios suivants :

- Aucun son sur l'appel entre un client AnyConnect et un numéro externe.
- Aucun son sur l'appel entre un client AnyConnect et un autre client AnyConnect.

Afin de résoudre ce problème, nous pouvons suivre les étapes suivantes :

Étape 1. Vérifiez la configuration de la transmission tunnel partagée.

- Accédez au profil de connexion utilisé pour vous connecter à : **Devices > VPN > Remote Access > Connection Profile > Sélectionnez le profil.**
- Accédez à la stratégie de groupe affectée à cette **stratégie de groupe Profile: > Général.**

- Vérifiez la configuration du fractionnement en canaux, comme illustré dans l'image.

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

- Si configuré comme **Réseaux de tunnel spécifiés ci-dessous**, vérifiez la configuration de la liste d'accès : **Objets > Gestion des objets > Liste d'accès > Modifier la liste d'accès pour la transmission tunnel partagée**.
- Assurez-vous que les serveurs vocaux et les réseaux du pool d'adresses IP AnyConnect sont répertoriés dans la liste d'accès à la transmission tunnel partagée, comme illustré dans l'image.

Edit Standard Access List Object



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

Étape 2. Vérifiez la configuration de l'exemption NAT.

Les règles d'exemption NAT doivent être configurées pour exempter le trafic du réseau VPN AnyConnect vers le réseau des serveurs voix et pour permettre la communication bidirectionnelle au sein des clients AnyConnect.

- Accédez à la configuration NAT : **Périphériques > NAT**.
- assurez-vous que la règle d'exemption NAT est configurée pour les réseaux source (serveurs voix) et de destination corrects (pool VPN AnyConnect), et que la règle NAT hairpin pour permettre la communication entre le client AnyConnect et le client AnyConnect est en place. De plus, vérifiez que la configuration correcte des interfaces entrantes et sortantes est en place pour chaque règle, conformément à la conception de votre réseau, comme l'illustre l'image.

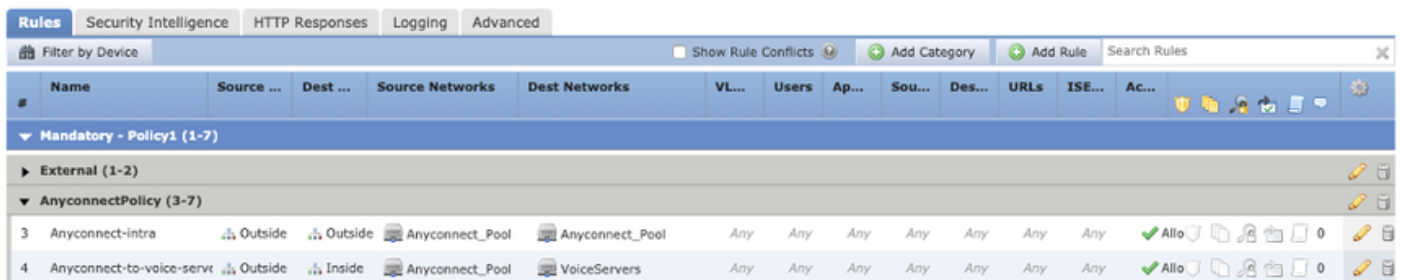
#..	Dir...	T...	Source Interface Ob...	Destination Interface Obje...	Original Sources	Original Destinations	O... S...	Translated Sources	Translated Destinations	T... S...	Options
1	↔	S...	Inside_interfac	outside_interface	InternalNetworksGroup	Anyconnect_Pool	InternalNetworksGroup	Anyconnect_Pool	Anyconnect_Pool	Anyconnect_Pool	Dns:false route-lookup no-proxy
2	↔	S...	Inside_interfac	outside_interface	VoiceServers	Anyconnect_Pool	VoiceServers	Anyconnect_Pool	Anyconnect_Pool	Anyconnect_Pool	Dns:false route-lookup no-proxy
3	↔	S...	outside_interfa	outside_interface	Anyconnect_Pool	Anyconnect_Pool	Anyconnect_Pool	Anyconnect_Pool	Anyconnect_Pool	Anyconnect_Pool	Dns:false route-lookup no-proxy

Étape 3. Vérifiez que l'inspection SIP est désactivée.

Veuillez consulter la section précédente **Les clients AnyConnect ne peuvent pas établir d'appels téléphoniques** pour savoir comment désactiver l'inspection SIP.

Étape 4. Vérifiez la stratégie de contrôle d'accès.

Conformément à votre configuration de stratégie de contrôle d'accès, assurez-vous que le trafic provenant des clients AnyConnect est autorisé à atteindre les serveurs voix et les réseaux concernés, comme l'illustre l'image.



The screenshot shows the Cisco ISE Policy Administration console. The 'Rules' tab is active, and the 'AnyconnectPolicy' category is expanded. The table below represents the data visible in the console.

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

Informations connexes

- Cette vidéo fournit un exemple de configuration pour les différents problèmes abordés dans ce document.
- Pour obtenir de l'aide supplémentaire, veuillez contacter le centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : [Coordonnées du service d'assistance Cisco à l'échelle mondiale.](#)
- Vous pouvez également visiter la communauté VPN Cisco [ici](#).