

Solución de problemas comunes de comunicación de AnyConnect en FTD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Proceso recomendado de resolución de problemas](#)

[Los clientes de AnyConnect no pueden acceder a los recursos internos](#)

[Los clientes de AnyConnect no tienen acceso a Internet](#)

[Los clientes de AnyConnect no pueden comunicarse entre sí](#)

[Los clientes de AnyConnect no pueden establecer llamadas telefónicas](#)

[Los clientes de AnyConnect pueden establecer llamadas telefónicas, aunque no haya audio en las llamadas](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo resolver algunos de los problemas de comunicación más comunes de Cisco AnyConnect Secure Mobility Client en Firepower Threat Defense (FTD) cuando utiliza Secure Socket Layer (SSL) o Internet Key Exchange versión 2 (IKEv2).

Contribuido por Angel Ortiz y Fernando Jiménez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTD gestionado por 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Proceso recomendado de resolución de problemas

Esta guía explica cómo resolver algunos problemas de comunicación comunes que tienen los clientes de AnyConnect cuando el FTD se utiliza como gateway de red privada virtual (VPN) de acceso remoto. Estas secciones abordan y proporcionan soluciones a los problemas siguientes:

- Los clientes de AnyConnect no pueden acceder a los recursos internos.
- Los clientes de AnyConnect no tienen acceso a Internet.
- Los clientes de AnyConnect no pueden comunicarse entre sí.
- Los clientes de AnyConnect no pueden establecer llamadas telefónicas.
- Los clientes de AnyConnect pueden establecer llamadas telefónicas. Sin embargo, no hay audio en las llamadas.

Los clientes de AnyConnect no pueden acceder a los recursos internos

Complete estos pasos:

Paso 1. Verifique la configuración del túnel dividido.

- Vaya al perfil de conexión al que están conectados los clientes de AnyConnect: **Devices > VPN > Remote Access > Connection Profile > Select the Profile** .
- Navegue hasta la política de grupo asignada a ese Profile: **Edit Group Policy > General**.
- Verifique la configuración de la Tunelización Dividida, como se muestra en la imagen.

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:

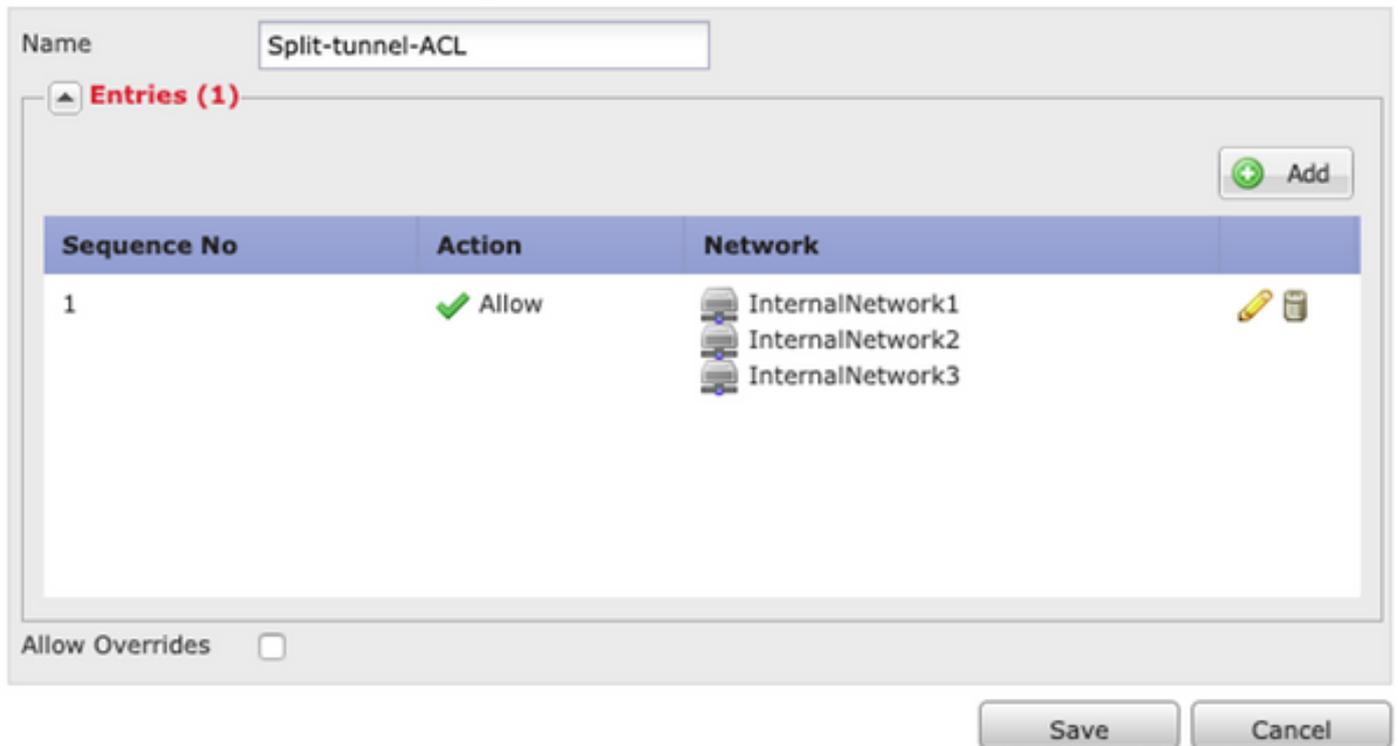
Save Cancel

- Si se configura como **redes de túnel especificadas** a continuación, verifique la configuración de la Lista de control de acceso (ACL):

Navegue hasta **Objetos > Administración de objetos > Lista de acceso > Editar lista de acceso para tunelización dividida**.

- Asegúrese de que las redes a las que intenta llegar desde el cliente AnyConnect VPN aparezcan en esa lista de acceso, como se muestra en la imagen.

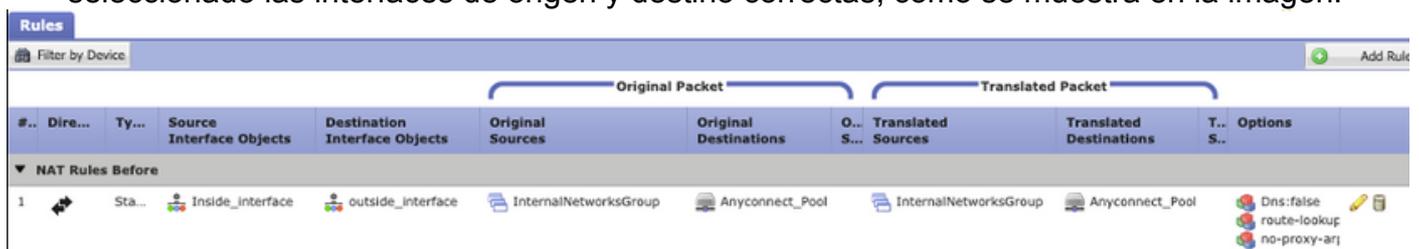
Edit Standard Access List Object



Paso 2. Verifique la configuración de la exención de traducción de direcciones de red (NAT).

Recuerde que debemos configurar una regla de exención de NAT para evitar que el tráfico se traduzca a la dirección IP de la interfaz, normalmente configurada para el acceso a Internet (con Traducción de dirección de puerto (PAT)).

- Vaya a la configuración NAT: **Devices > NAT**.
- Asegúrese de que la regla de exención de NAT esté configurada para las redes de origen (interna) y destino (AnyConnect VPN Pool) correctas. Verifique también que se hayan seleccionado las interfaces de origen y destino correctas, como se muestra en la imagen.



Nota: Cuando se configuran las reglas de exención de NAT, verifique las opciones **no-proxy-arp** y realice **route-lookup** como práctica recomendada.

Paso 3. Verifique la política de control de acceso.

De acuerdo con la configuración de la política de control de acceso, asegúrese de que el tráfico de los clientes de AnyConnect pueda llegar a las redes internas seleccionadas, como se muestra en la imagen.



Los clientes de AnyConnect no tienen acceso a Internet

Hay dos escenarios posibles para esta cuestión.

1. El tráfico destinado a Internet no debe atravesar el túnel VPN.

Asegúrese de que la política de grupo esté configurada para la tunelización dividida como **redes de túnel especificadas a continuación** y NO como **Permitir todo el tráfico sobre el túnel**, como se muestra en la imagen.

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. El tráfico destinado a Internet debe atravesar el túnel VPN.

En este caso, la configuración de política de grupo más común para la tunelización dividida sería seleccionar **Permitir todo el tráfico sobre el túnel**, como se muestra en la imagen.

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

Paso 1. Verifique la configuración de la exención de NAT para el alcance de la red interna.

Recuerde que aún debemos configurar una regla de exención de NAT para tener acceso a la red interna. Revise el **paso 2** del **Los clientes de AnyConnect no pueden acceder al recurso interno** sección.

Paso 2. Verifique la configuración del hairpinning para las traducciones dinámicas.

Para que los clientes de AnyConnect tengan acceso a Internet a través del túnel VPN, necesitamos asegurarnos de que la configuración NAT de conexión es correcta para que el tráfico se traduzca a la dirección IP de la interfaz.

- Vaya a la configuración NAT: **Devices > NAT**.
- Asegúrese de que la regla NAT dinámica esté configurada para la interfaz correcta (enlace ISP) como origen y destino (hairpinning). Verifique también que la red utilizada para el conjunto de direcciones VPN de AnyConnect esté seleccionada en el origen original y en la **IP de la interfaz** de destino se selecciona para el origen traducido, como se muestra en la imagen.

#	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...

Paso 3. Verifique la política de control de acceso.

De acuerdo con la configuración de la política de control de acceso, asegúrese de que el tráfico de los clientes de AnyConnect pueda llegar a los recursos externos, como se muestra en la imagen.

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

Los clientes de AnyConnect no pueden comunicarse entre sí

Hay dos escenarios posibles para este problema:

1. Clientes AnyConnect con **Permitir todo el tráfico a través del túnel** configuración en su lugar.
2. Clientes AnyConnect con **Redes de túnel especificadas a continuación** configuración en su lugar.

1. Clientes AnyConnect con **Permitir todo el tráfico a través del túnel** configuración en su lugar. Fecha **Permitir todo el tráfico a través del túnel** está configurado para AnyConnect significa que todo el tráfico, interno y externo, debe reenviarse a la cabecera de AnyConnect. Esto se convierte en un problema cuando tiene NAT para el acceso público a Internet, ya que el tráfico proviene de un cliente de AnyConnect destinado a otro cliente de AnyConnect se traduce a la dirección IP de la interfaz y, por lo tanto, la comunicación falla.

Paso 1. Verifique la configuración de la exención de NAT.

Para superar este problema, se debe configurar una regla de exención de NAT manual para permitir la comunicación bidireccional dentro de los clientes de AnyConnect.

- Vaya a la configuración NAT: **Devices > NAT**.
- Asegúrese de que la regla de exención de NAT esté configurada para el origen correcto (AnyConnect VPN Pool) y el destino. (Conjunto VPN de AnyConnect). Verifique también que la configuración correcta del pin hairpin esté en su lugar, como se muestra en la imagen.

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

Paso 2. Verifique la política de control de acceso.

De acuerdo con la configuración de la política de control de acceso, asegúrese de que se permite el tráfico de los clientes de AnyConnect, como se muestra en la imagen.

#	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	Any

2. Clientes de Anyconnect con **Redes de túnel especificadas a continuación** configuración en su lugar.

Con **Redes de túnel especificadas a continuación** configurado para los clientes de AnyConnect, sólo se reenvía tráfico específico a través del túnel VPN. Sin embargo, debemos asegurarnos de que la cabecera tenga la configuración adecuada para permitir la comunicación dentro de los clientes de AnyConnect.

Paso 1. Verifique la configuración de la exención de NAT.

Verifique el paso 1, en la sección **Permitir todo el tráfico por el túnel**.

Paso 2. Verifique la configuración de la tunelización dividida.

Para que los clientes de AnyConnect se comuniquen entre ellos, necesitamos agregar las direcciones del conjunto de VPN a la ACL de túnel dividido.

- Siga el paso 1 del **Los clientes de AnyConnect no pueden acceder a los recursos internos** sección.
- Asegúrese de que la red del conjunto VPN de AnyConnect aparezca en la lista de acceso de tunelización dividida, como se muestra en la imagen.

Edit Standard Access List Object

? X

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

Nota: Si hay más de un grupo IP para los clientes AnyConnect y se necesita comunicación entre los diferentes grupos, asegúrese de agregar todos los grupos en la ACL de tunelización dividida, y también agregue una regla de exención de NAT para los grupos IP necesarios.

Paso 3. Verifique la política de control de acceso.

Asegúrese de que el tráfico de los clientes de AnyConnect esté permitido como se muestra en la imagen.

#	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

Los clientes de AnyConnect no pueden establecer llamadas telefónicas

Hay algunos escenarios en los que los clientes de AnyConnect necesitan establecer llamadas telefónicas y videoconferencias a través de VPN.

Los clientes de AnyConnect pueden conectarse a la cabecera de AnyConnect sin ningún problema. Pueden acceder a recursos internos y externos, pero no se pueden establecer llamadas telefónicas.

En estos casos, debemos tener en cuenta los siguientes aspectos:

- Topología de red para voz.

- Protocolos involucrados. Es decir, protocolo de inicio de sesión (SIP), protocolo de árbol de extensión rápido (RSTP), etc.
- Cómo se conectan los teléfonos VPN a Cisco Unified Communications Manager (CUCM).

De forma predeterminada, FTD y ASA tienen la inspección de aplicaciones habilitada de forma predeterminada en su mapa de políticas global.

En la mayoría de los casos, los teléfonos VPN no pueden establecer una comunicación fiable con CUCM porque la cabecera de AnyConnect tiene habilitada una inspección de aplicación que modifica el tráfico de señal y voz.

Para obtener más información sobre la aplicación de voz y vídeo en la que puede aplicar la inspección de aplicaciones, consulte el siguiente documento:

[Capítulo: Inspección de los protocolos de voz y vídeo](#)

Para confirmar si el policy-map global descarta o modifica el tráfico de una aplicación, podemos utilizar el comando **show service-policy** como se muestra a continuación.

```
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
```

```
.
```

En este caso, podemos ver cómo la inspección SIP descarta el tráfico.

Además, la inspección de SIP también puede traducir las direcciones IP dentro de la carga útil, no en el encabezado IP, causa diferentes problemas, por lo que se recomienda desactivarla cuando deseemos utilizar servicios de voz a través de AnyConnect VPN.

Para desactivarla, debemos completar los siguientes pasos:

Paso 1. Introduzca el modo EXEC privilegiado.

Para obtener más información sobre cómo acceder a este modo, consulte el siguiente documento:

[Capítulo: Utilizar la interfaz de línea de comandos \(CLI\)](#)

Paso 2. Verifique el policy-map global.

Ejecute el siguiente comando y verifique si la inspección SIP está habilitada.

```
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

Paso 3. Desactive la inspección SIP.

Si la inspección SIP está activada, desactive el siguiente comando de ejecución desde el mensaje de clish:

```
> configure inspection sip disable
```

Paso 4. Vuelva a verificar el mapa de política global.

Asegúrese de que la inspección SIP esté inhabilitada en el mapa de políticas global:

```
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
```

Los clientes de AnyConnect pueden establecer llamadas telefónicas, aunque no haya audio en las llamadas

Como se mencionó en la sección anterior, una necesidad muy común para los clientes de AnyConnect es establecer llamadas telefónicas cuando se conectan a la VPN. En algunos casos se puede establecer la llamada, sin embargo, los clientes pueden experimentar una falta de audio. Esto se aplica a los siguientes escenarios:

- No hay audio en la llamada entre un cliente AnyConnect y un número externo.
- No hay audio en la llamada entre un cliente AnyConnect y otro cliente AnyConnect.

Para corregir esto, podemos seguir estos pasos:

Paso 1. Verifique la configuración de la tunelización dividida.

- Vaya a Connection Profile use para conectarse a: **Devices > VPN > Remote Access > Connection Profile > Select the Profile** .
- Navegue hasta la política de grupo asignada a ese Profile: **Edit Group Policy > General**.

- Verifique la configuración de la Tunelización Dividida, como se muestra en la imagen.

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 está configurado como **Redes de túnel especificadas a continuación**, verifique la configuración de la lista de acceso: **Objects > Object Management > Access List > Edit the Access List for Split tunneling**.
- Asegúrese de que los servidores de voz y las redes del conjunto IP de AnyConnect se enumeran en la lista de acceso de tunelización dividida, como se muestra en la imagen.

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

Paso 2. Verifique la configuración de la exención de NAT.

Las reglas de exención de NAT se deben configurar para eximir el tráfico de la red VPN de AnyConnect a la red de servidores de voz y también para permitir la comunicación bidireccional dentro de los clientes de AnyConnect.

- Vaya a la configuración NAT: **Devices > NAT**.
- asegúrese de que la regla de exención de NAT esté configurada para las redes de origen (servidores de voz) y de destino (conjunto de VPN de AnyConnect) correctas, y que la regla de NAT de la horquilla para permitir que el cliente de AnyConnect pueda comunicarse con el cliente de AnyConnect esté en su lugar. Además, verifique que la configuración de interfaces entrantes y salientes correcta esté en su lugar para cada regla, según el diseño de red, como se muestra en la imagen.

Rules

Filter by Device

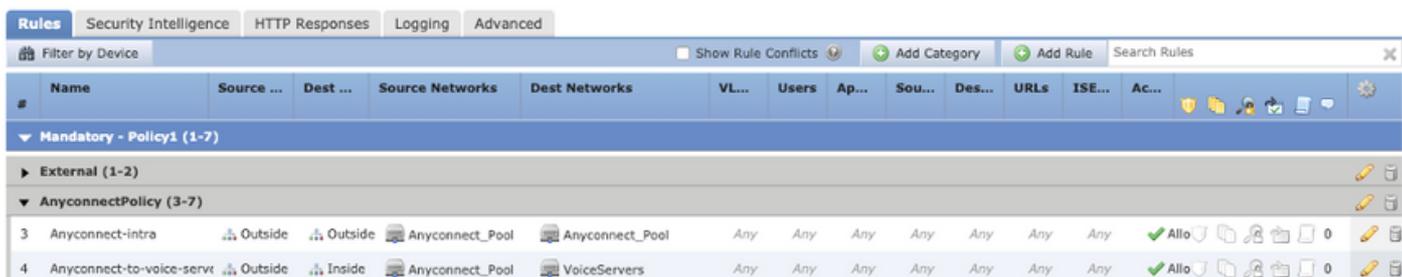
#..	Dir...	T...	Original Packet				Translated Packet				Options	
			Source Interface Ob...	Destination Interface Obje...	Original Sources	Original Destinations	O... S...	Translated Sources	Translated Destinations	T... S...		
▼ NAT Rules Before												
1	↔	S...	Inside_interfac	outside_interface	InternalNetworksGroup	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	

Paso 3. Verifique que la inspección SIP esté inhabilitada.

Revise la sección anterior **Los clientes de AnyConnect no pueden establecer llamadas telefónicas** para saber cómo desactivar la inspección SIP.

Paso 4. Verifique la política de control de acceso.

De acuerdo con la configuración de la política de control de acceso, asegúrese de que el tráfico de los clientes de AnyConnect pueda llegar a los servidores de voz y a las redes involucradas, como se muestra en la imagen.



The screenshot shows the Cisco ISE Rules configuration interface. The top navigation bar includes tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. Below the navigation bar, there are options for 'Filter by Device', 'Show Rule Conflicts', 'Add Category', 'Add Rule', and a search box for 'Search Rules'. The main content area displays a table of rules under the 'AnyconnectPolicy' category. The table has columns for '#', 'Name', 'Source ...', 'Dest ...', 'Source Networks', 'Dest Networks', 'VL...', 'Users', 'Ap...', 'Sou...', 'Des...', 'URLs', 'ISE...', 'Ac...', and a status column. Two rules are visible:

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

Información Relacionada

- Este vídeo proporciona el ejemplo de configuración para los diferentes problemas que se tratan en este documento.
- Para obtener asistencia adicional, póngase en contacto con el Centro de Asistencia Técnica (TAC). Se requiere un contrato de soporte válido: [Contactos de soporte a nivel mundial de Cisco](#).
- También puede visitar la comunidad Cisco VPN [aquí](#).