

# Troubleshoot Common AnyConnect Communication Issues on FTD

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Recommended troubleshoot process](#)

[AnyConnect clients cannot access internal resources](#)

[AnyConnect clients do not have internet access](#)

[AnyConnect clients cannot communicate between each other](#)

[AnyConnect clients cannot establish phone calls](#)

[AnyConnect clients can establish phone calls, however there is no audio on the calls](#)

[Related Information](#)

## Introduction

This document describes how to troubleshoot some of the most common communication issues of the Cisco AnyConnect Secure Mobility Client on Firepower Threat Defense (FTD) when it uses either Secure Socket Layer (SSL) or Internet Key Exchange version 2 (IKEv2).

Contributed by Angel Ortiz and Fernando Jimenez, Cisco TAC Engineers.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

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

### Components Used

The information in this document is based on these software and hardware versions:

- FTD managed by 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. If your network is live, ensure that you understand the potential impact of any command.

## Recommended troubleshoot process

This guide explains how to troubleshoot some common communication issues that AnyConnect clients have when the FTD is used as Remote Access Virtual Private Network (VPN) gateway. These sections address and provide solutions to problems below:

- AnyConnect clients cannot access internal resources.
- AnyConnect clients do not have internet access.
- AnyConnect clients cannot communicate between each other.
- AnyConnect clients cannot establish phone calls.
- AnyConnect clients can establish phone calls. However, there is no audio on the calls.

## AnyConnect clients cannot access internal resources

Complete these steps:

### Step 1. Verify Split tunnel configuration.

- Navigate to the Connection Profile that AnyConnect clients are connected to: **Devices > VPN > Remote Access > Connection Profile > Select the Profile.**
- Navigate to the Group-Policy assigned to that Profile: **Edit Group Policy > General.**
- Check the Split Tunneling configuration, as shown in the image.

#### Edit Group Policy

? X

The screenshot shows the 'Edit Group Policy' configuration window. The 'Name' field is 'Anyconnect\_GroupPolicy'. The 'Description' field is empty. The 'General' tab is selected, showing the 'Split Tunneling' section. The 'IPv4 Split Tunneling' dropdown is set to 'Tunnel networks specified below'. 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 visible, with 'DNS Requests' set to 'Send DNS requests as per split tunnel policy' and 'Domain List' empty. The 'Save' and 'Cancel' buttons are at the bottom right.

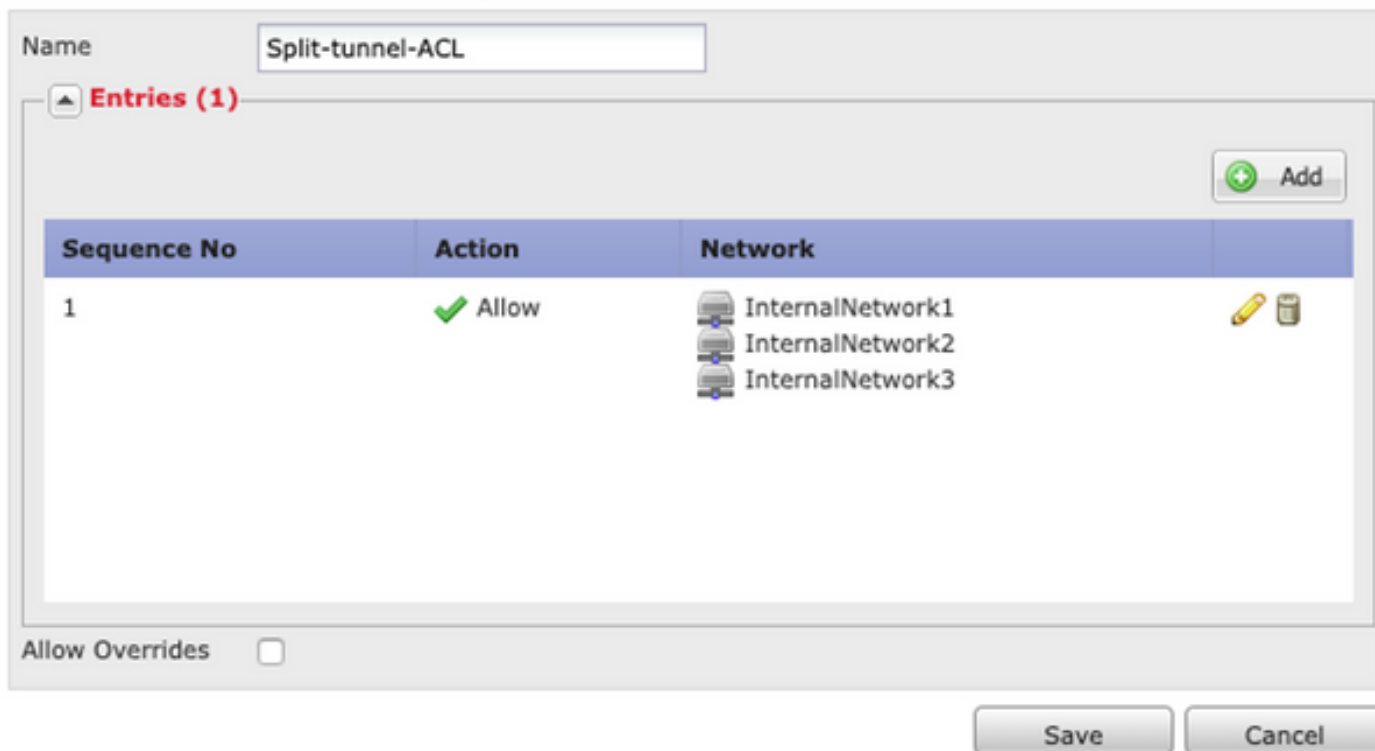
- If it's configured as **Tunnel networks specified below**, verify the Access Control List (ACL)

configuration:

Navigate to **Objects > Object Management > Access List > Edit the Access List for Split tunneling.**

- Ensure that the networks that you try to reach from the AnyConnect VPN client are listed in that Access List, as shown in the image.

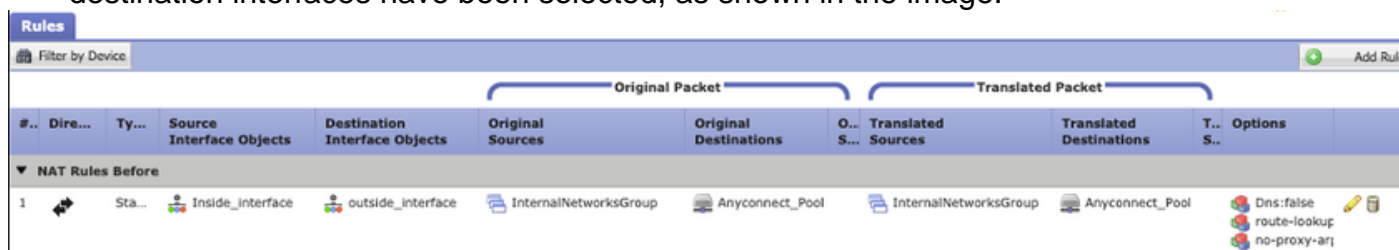
### Edit Standard Access List Object



**Step 2.** Verify Network Address Translation (NAT) exemption configuration.

Remember that we must configure a NAT exemption rule to avoid traffic to be translated to the interface IP address, usually configured for internet access (with Port Address Translation (PAT)).

- Navigate to the NAT configuration: **Devices > NAT.**
- Ensure that the NAT exemption rule is configured for the correct source (internal) and destination (AnyConnect VPN Pool) networks. Also check that the correct source and destination interfaces have been selected, as shown in the image.



**Note:** When NAT exemption rules are configured, check the **no-proxy-arp** and perform **route-lookup** options as a best practice.

**Step 3.** Verify Access Control Policy.

Per your Access Control Policy configuration, ensure that traffic from the AnyConnect clients is allowed to reach the selected internal networks, as shown in the image.

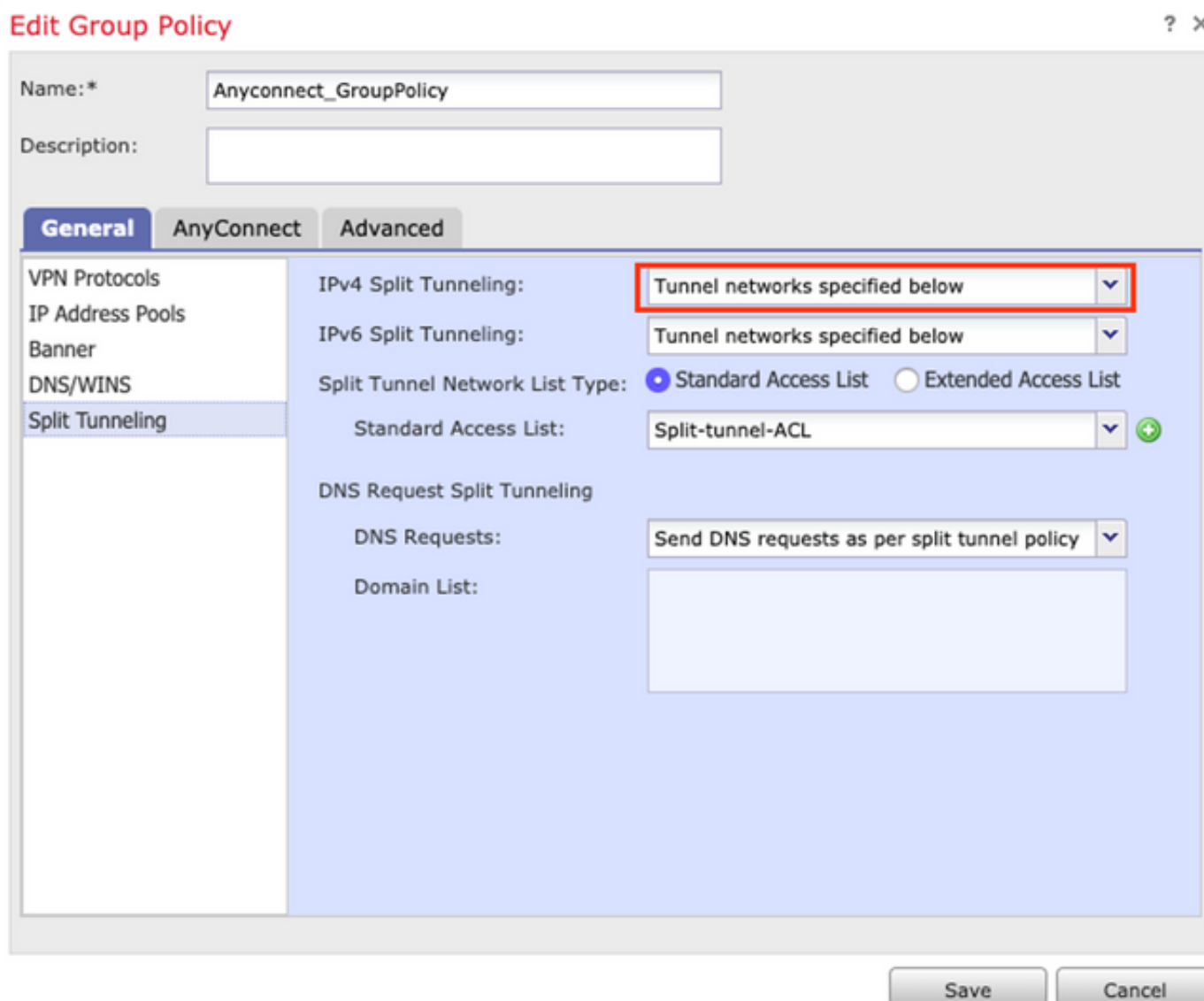


## AnyConnect clients do not have internet access

There are two possible scenarios for this issue.

1. Traffic destined for the internet must not go through the VPN tunnel.

Ensure that the Group-Policy is configured for Split tunneling as **Tunnel networks specified below** and NOT as **Allow all traffic over tunnel**, as shown in the image.



2. Traffic destined for the Internet must go through the VPN tunnel.

In this case, the most common Group-Policy configuration for Split tunneling would be to select

**Allow all traffic over tunnel**, as shown in the image.

### 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

#### Step 1. Verify NAT exemption configuration for internal network reachability.

Remember that we must still configure a NAT exemption rule to have access to the internal network. Please review **Step 2** of the **AnyConnect clients cannot access internal resource** section.

#### Step 2. Verify hairpinning configuration for dynamic translations.

In order for AnyConnect clients to have internet access through the VPN tunnel, we need to ensure that the hairpinning NAT configuration is correct for traffic to be translated to the interface's IP address.

- Navigate to the NAT configuration: **Devices > NAT**.
- Ensure that the Dynamic NAT rule is configured for the correct interface (Internet Service Provider (ISP) link) as source and destination (hairpinning). Also check that the network used for the AnyConnect VPN address pool is selected in Original source and the Destination **Interface IP** option is selected for Translated source, as shown in the image.

#	Dire...	Type	Original Packet			Translated Packet			Options
			Source Interface ...	Destination Interface ...	Original Sources	Original Destinations	Original Services	Translated Sources	
NAT Rules Before									
Auto NAT Rules									
#	➔	Dynamic	outside_int	outside_int	Anyconnect_Pool		Interface		Dns:fail

### Step 3. Verify Access Control Policy.

Per your Access Control Policy configuration, ensure that traffic from the AnyConnect clients is allowed to reach the external resources, as shown in the image.

#	Name	Source ...	Dest ...	Source Networks	Dest Networks	VL...	Users	Ap...	Sou...	Des...	URLs	ISE...	Ac...	Options	
														Allow	Count
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	Allow	0
4	Internet-to-Anyconnect	Outside	Outside	Any	Anyconnect_Pool	Any	Any	Any	Any	Any	Any	Any	Any	Allow	0

### AnyConnect clients cannot communicate between each other

There are two possible scenarios for this issue:

1. AnyConnect clients with **Allow all traffic over tunnel** configuration in place.
2. AnyConnect clients with **Tunnel networks specified below** configuration in place.

1. AnyConnect clients with **Allow all traffic over tunnel** configuration in place.

When **Allow all traffic over tunnel** is configured for AnyConnect means that all traffic, internal and external, should be forwarded to the AnyConnect headend, this becomes a problem when you have NAT for Public Internet access, since traffic comes from an AnyConnect client destined to another AnyConnect client is translated to the interface IP address and therefore communication fails.

### Step 1. Verify NAT exemption configuration.

In order to overcome this problem a manual NAT exemption rule must be configured to allow bidirectional communication within the AnyConnect clients.

- Navigate to the NAT configuration: **Devices > NAT**.
- Ensure that the NAT exemption rule is configured for the correct source (AnyConnect VPN Pool) and destination. (AnyConnect VPN Pool) networks. Also check that the correct hairpin configuration is in place, as shown in the image.

#	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-ic, no-prox

## Step 2. Verify Access Control Policy.

Per your Access Control Policy configuration, ensure that traffic from the AnyConnect Clients is allowed, as shown in the image.



2. Anyconnect clients with **Tunnel networks specified below** configuration in place.

With **Tunnel networks specified below** configured for the AnyConnect clients only specific traffic is forwarded to through the VPN tunnel. However, we need to ensure that the headend has the proper configuration to allow communication within the AnyConnect clients.

## Step 1. Verify NAT exemption configuration.

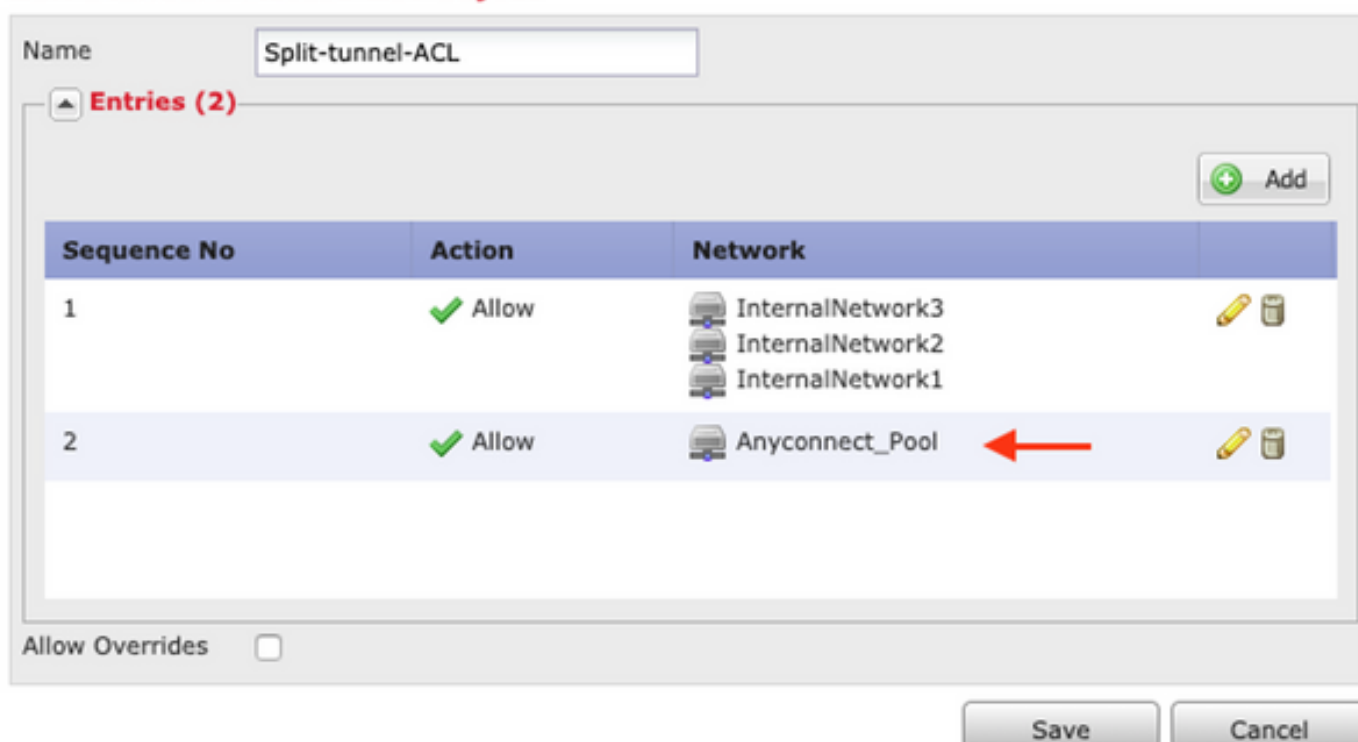
Please check **Step 1**, in the **Allow all traffic over tunnel** section.

## Step 2. Verify Split tunneling configuration.

For AnyConnect clients to communicate between them we need to add the VPN pool addresses into the Split-Tunnel ACL.

- Please follow **Step 1** of the **AnyConnect clients cannot access internal resources** section.
- Ensure that the AnyConnect VPN Pool network is listed in the Split tunneling Access List, as shown in the image.

### Edit Standard Access List Object





**Note:** If there is more than one IP Pool for AnyConnect clients and communication between the different pools is needed, ensure to add all of the pools in the split tunneling ACL, also add a NAT exemption rule for the needed IP Pools.

### Step 3. Verify Access Control Policy.

Ensure that traffic from the AnyConnect clients is allowed as shown in the image.



### AnyConnect clients cannot establish phone calls

There are some scenarios where AnyConnect clients need to establish phone calls and video conferences over VPN.

AnyConnect clients can connect to the AnyConnect headend without any problem. They can reach internal and external resources, however phone calls cannot be established.

For this cases we need to consider the follow points:

- Network topology for voice.
- Protocols involved. I.e. Session Initiation Protocol (SIP), Rapid Spanning Tree Protocol (RSTP), etc.
- How the VPN phones connect to the Cisco Unified Communications Manager (CUCM).

By default, FTD and ASA have applications inspection enabled by default in their global policy-map.

In most cases scenarios the VPN phones are not able to establish a reliable communication with the CUCM because the AnyConnect headend has an application inspection enabled that modifies the signal and voice traffic.

For more information about the voice and video application where you can apply application inspection see the follow document:

[Chapter: Inspection for Voice and Video Protocols](#)

In order to confirm if an application traffic is dropped or modified by the global policy-map we can use the **show service-policy** command as shown below.

```
firepower#show service-policy
```

```
Global policy:  
Service-policy: global_policy  
Class-map: inspection_default  
.
```



<Output omitted>

```
.  
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  
.
```

<Output omitted>

In this case we can see how SIP inspection drops the traffic.

Moreover, SIP inspection can also translate IP addresses inside the payload, not in the IP header, causes different issues, hence it is recommended to disable it when we want to use voice services over AnyConnect VPN.

In order to disable it we need to complete the next steps:

### **Step 1. Enter the privileged EXEC mode.**

For more information on how to access this mode see the next document:

[Chapter: Use the Command Line Interface \(CLI\)](#)

### **Step 2. Verify the global policy-map.**

Run the next command and verify if SIP inspection is enabled.

```
firepower#show running-config policy-map
```

```
.
```

<Output omitted>

```
.
```

```
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

### **Step 3. Disable SIP inspection.**

If SIP inspection is enabled, turn it off running command below from clish prompt:

```
> configure inspection sip disable
```

### **Step 4. Verify the Global Policy-map again.**

Ensure that SIP inspection is disabled from the global policy-map:

```
firepower#show running-config policy-map
```

.

<Output omitted>

.

```
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 can establish phone calls, however there is no audio on the calls**

As mentioned in the previous section, a very common need for AnyConnect clients is to establish phone calls when connected to the VPN. In some cases the call can be established, however clients may experience lack of audio on it. This applies to the next scenarios:

- No audio on the call between an AnyConnect client and an external number.
- No audio on the call between an AnyConnect client and another AnyConnect client.

In order to get this fixed, we can follow these steps:

### **Step 1. Verify Split tunneling configuration.**

- Navigate to the Connection Profile use to connect to: **Devices > VPN > Remote Access > Connection Profile > Select the Profile.**
- Navigate to the Group-Policy assigned to that Profile: **Edit Group Policy > General.**
- Check the Split Tunneling configuration, as shown in the 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

- If configured as **Tunnel networks specified below**, verify the Access List configuration: **Objects > Object Management > Access List > Edit the Access List for Split tunneling.**
- Ensure that the Voice Servers and the AnyConnect IP Pool networks are listed in the Split tunneling Access List, as shown in the image.

## 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

### Step 2. Verify NAT exemption configuration.

NAT exemption rules must be configured to exempt traffic from the AnyConnect VPN network to the Voice Servers network and also to allow bidirectional communication within the AnyConnect clients.

- Navigate to the NAT configuration: **Devices > NAT**.
- ensure that the NAT exemption rule is configured for the correct source (Voice Servers) and destination (AnyConnect VPN Pool) networks, and the hairpin NAT rule to allow AnyConnect client to AnyConnect client communication is in place. Moreover, check that the correct inbound and outbound interfaces configuration is in place for each rule, per your network design, as shown in the image.

Rules

Filter by Device

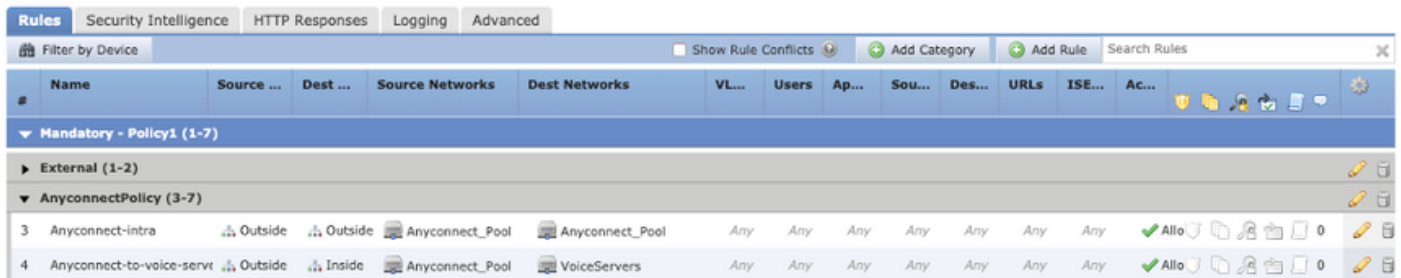
#..	Dir...	T...	Original Packet				Translated Packet				Options	
			Source Interface Ob...	Destination Interface Obje...	Original Sources	Original Destinations	O... S...	Translated Sources	Translated Destinations	T... S...		
▼ NAT Rules Before												
1	↔	S...	Inside_interfac	outside_interface	InternalNetworksGroup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

### Step 3. Verify that SIP inspection is disabled.

Please review the previous section **AnyConnect clients cannot establish phone calls** to know how to disable SIP inspection.

### Step 4. Verify Access Control Policy.

Per your Access Control Policy configuration, ensure that traffic from the AnyConnect clients is allowed to reach the Voice servers and involved networks, as shown in the image.



The screenshot shows the Cisco ISE Policy Rules configuration interface. The 'Rules' tab is active, and the 'Mandatory - Policy1 (1-7)' policy is expanded. Two rules are visible under the 'AnyconnectPolicy (3-7)' group:

#	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-servt	Outside	Inside	Anyconnect_Pool	VoiceServers	Any	Any	Any	Any	Any	Any	Any	Any	✓ Allo				0

## Related Information

- This video provides the configuration example for the different issues discussed in this document.
- For additional assistance, please contact Technical Assistance center (TAC). A valid support contract is required: [Cisco Worldwide Support Contacts](#).
- You can also visit the Cisco VPN Community [here](#).