Troubleshoot Common AnyConnect Communication Issues on ASA

Contents

Introduction

This document describes how to troubleshoot some of the most common communication issues of the Cisco AnyConnect Secure Mobility Client on ASA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AnyConnect Secure Mobility Client
- Adaptive Security Appliance (ASA)

Components Used

- ASA 9.12 managed by ASDM 7.13
- 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 applies to common communication issues that you have when connected to a Remote Access Client VPN gateway (ASA). These sections address and provide solutions to the problems:

- AnyConnect Clients Cannot Access Internal Resources

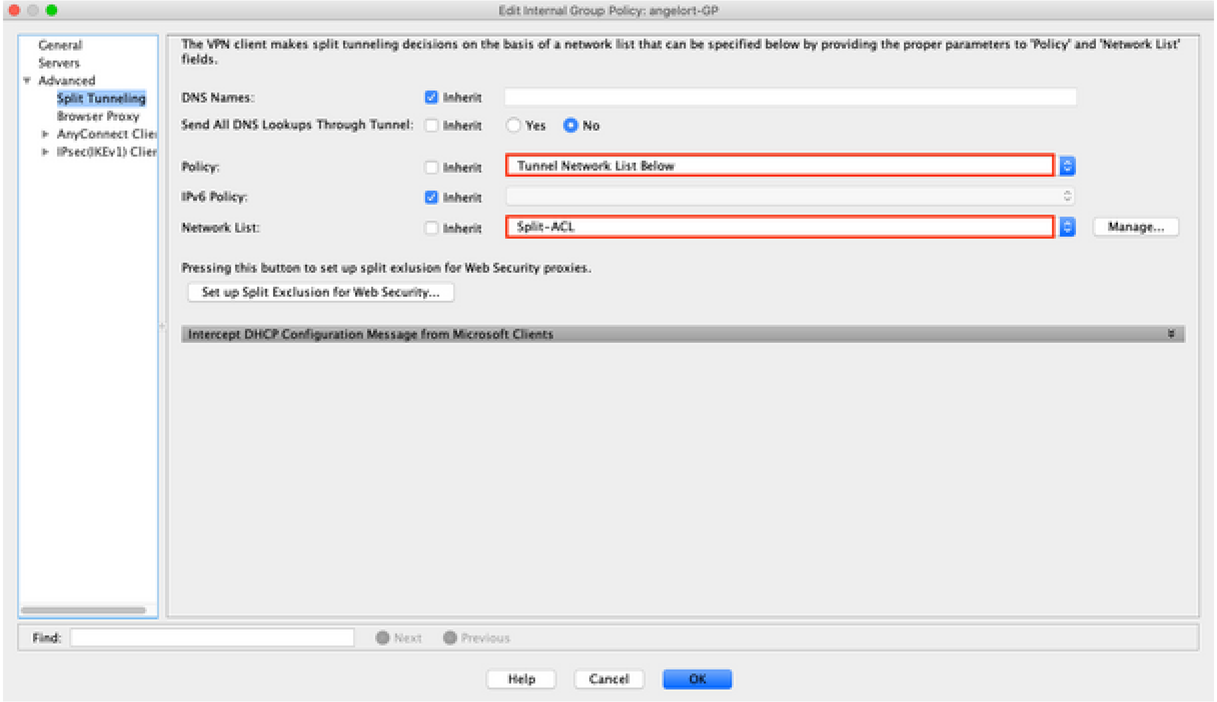
- AnyConnect Clients Do Not Have Internet Access
- AnyConnect Clients Cannot Communicate Between Each Other
- AnyConnect Clients Cannot Establish Phone Calls
- AnyConnect Clients Can Establish Phone Calls But There Is No Audio On The Calls

AnyConnect Clients Cannot Access Internal Resources

Complete these steps:

Step 1. Verify Split tunnel configuration.

- Navigate to the Connection Profile that users are connected to: **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profile** > **Select the Profile**
- Navigate to the Group-Policy assigned to that Profile: **Group Policy** > **Manage** > **Edit** > **Advanced** > **Split Tunneling**
- Check the Split Tunnel configuration.


Edit Internal Group Policy: angelort-GP
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Clie
IPsec(IKEv1) Clier
Manage...
Set up Split Exclusion for Web Security...
Intercept DHCP Configuration Message from Microsoft Clients
Find:
Next
Previous
Help
Cancel
OK

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: □ Inherit ○ Yes ● No

Policy: □ Inherit Tunnel Network List Below

IPv6 Policy: ☑ Inherit

Network List: □ Inherit Split-ACL

Pressing this button to set up split exlusion for Web Security proxies.

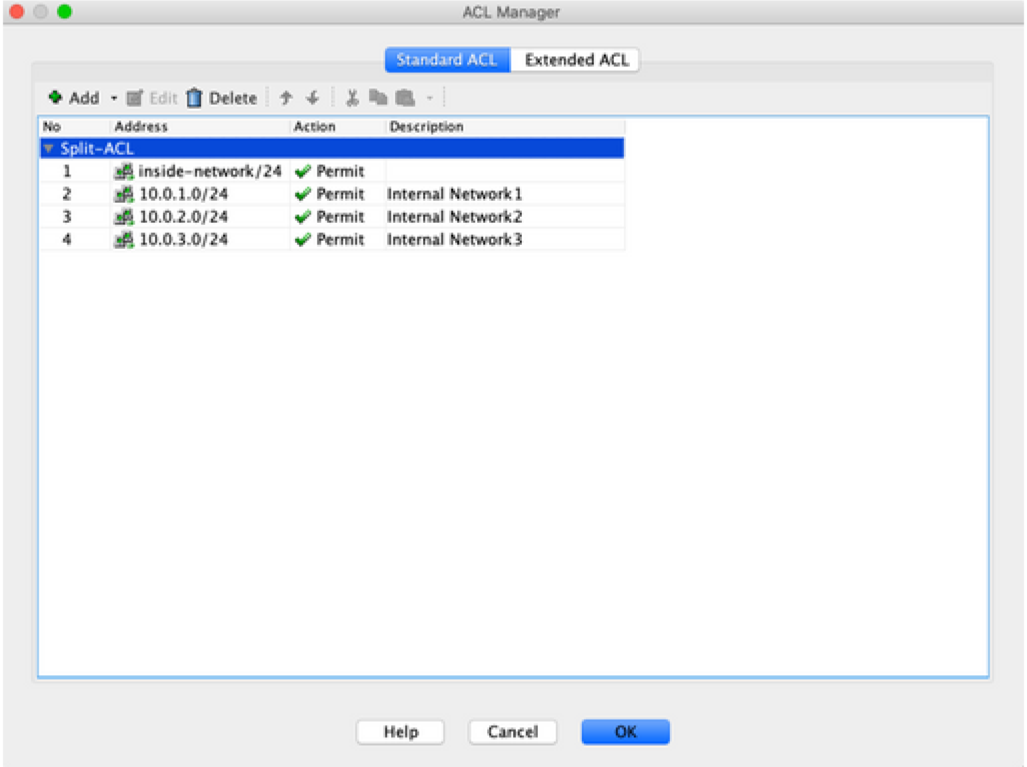
Equivalent CLI Configuration:

```
ASA# show running-config tunnel-group

tunnel-group AnyConnectTG type remote-access

tunnel-group AnyConnectTG general-attributes

default-group-policy AnyConnectGP-Split

tunnel-group AnyConnectTG webvpn-attributes

 group-alias AnyConnectTG enable

ASA# show running-config group-policy AnyConnectGP-Split

group-policy AnyConnectGP-Split internal
```

```
group-policy AnyConnectGP-Split attributes
 dns-server value 10.0.1.1
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split-ACL
 split-dns none
 split-tunnel-all-dns disable
```

- If configured as Tunnel networks Listed Below, verify the Access Control List (ACL) configuration.

In the same window navigate to **Manage > Select the Access List > Edit the Access List for Split tunnel**



No	Address	Action	Description
Split-ACL			
1	inside-network/24	✓ Permit	
2	10.0.1.0/24	✓ Permit	Internal Network1
3	10.0.2.0/24	✓ Permit	Internal Network2
4	10.0.3.0/24	✓ Permit	Internal Network3

- Ensure that the networks that you try to reach from the AnyConnect VPN client are listed in that Access Control List (ACL).

Equivalent CLI Configuration:

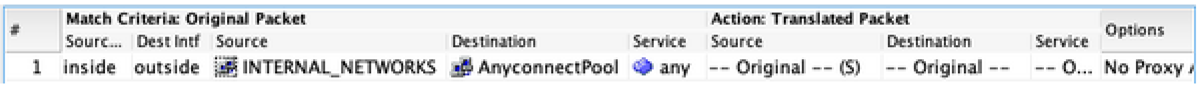
```
ASA# show running-config access-list Split-ACL
access-list Split-ACL standard permit 10.28.28.0 255.255.255.0
access-list Split-ACL remark Internal Network1
access-list Split-ACL standard permit 10.0.1.0 255.255.255.0
access-list Split-ACL remark Internal Network2
```

```
access-list Split-ACL standard permit 10.0.2.0 255.255.255.0

access-list Split-ACL remark Internal Network3

access-list Split-ACL standard permit 10.0.3.0 255.255.255.0
```

Step 2. Verify NAT exemption configuration.

Remember that you 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: **Configuration > Firewall > NAT Rules**
- Make sure 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.



#	Match Criteria: Original Packet					Action: Translated Packet			Options
	Sourc...	Dest Intf	Source	Destination	Service	Source	Destination	Service	
1	inside	outside	INTERNAL_NETWORKS	AnyconnectPool	any	-- Original -- (S)	-- Original --	-- O...	No Proxy

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

Equivalent CLI Configuration:

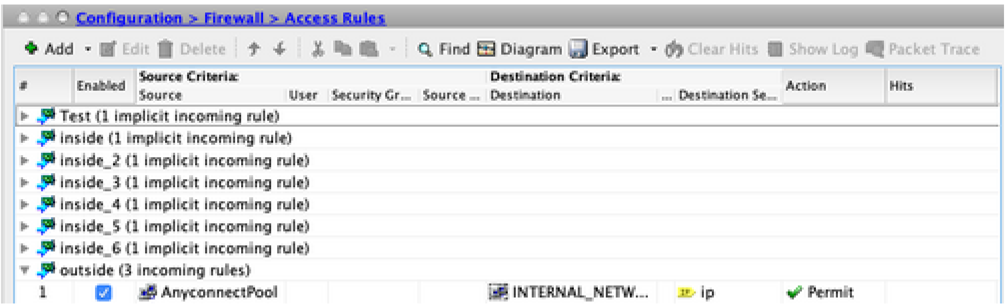
```
ASA# show running-config nat

nat (inside,outside) source static INTERNAL_NETWORKS INTERNAL_NETWORKS destination static AnyConnectPool AnyConnectPool no-proxy-arp route-lookup

ASA# show running-config object-group id INTERNAL_NETWORKS

object-group network INTERNAL_NETWORKS

 network-object object InternalNetwork1

 network-object object InternalNetwork2

 network-object object InternalNetwork3

ASA# show running-config object id InternalNetwork1

object network InternalNetwork1

 subnet 10.0.1.0 255.255.255.0

ASA# show running-config object id InternalNetwork2

object network InternalNetwork2

 subnet 10.0.2.0 255.255.255.0

ASA# show running-config object id InternalNetwork3

object network InternalNetwork3
```

```
 subnet 10.0.3.0 255.255.255.0
```

```
ASA# show running-config object id AnyConnectPool

object network AnyConnectPool

 subnet 192.168.1.0 255.255.255.0
```

Step 3. Verify Access Rules.

Per your access rules configuration, make sure that traffic from the AnyConnect Clients is allowed to reach the selected internal networks.



Configuration > Firewall > Access Rules

#	Enabled	Source Criteria:				Destination Criteria:			Action	Hits
		Source	User	Security Gr...	Source ...	Destination	...	Destination Se...		
Test (1 implicit incoming rule)										
inside (1 implicit incoming rule)										
inside_2 (1 implicit incoming rule)										
inside_3 (1 implicit incoming rule)										
inside_4 (1 implicit incoming rule)										
inside_5 (1 implicit incoming rule)										
inside_6 (1 implicit incoming rule)										
outside (3 incoming rules)										
1	☑	AnyconnectPool				INTERNAL_NETW...		ip	✓ Permit	

Equivalent CLI Configuration:

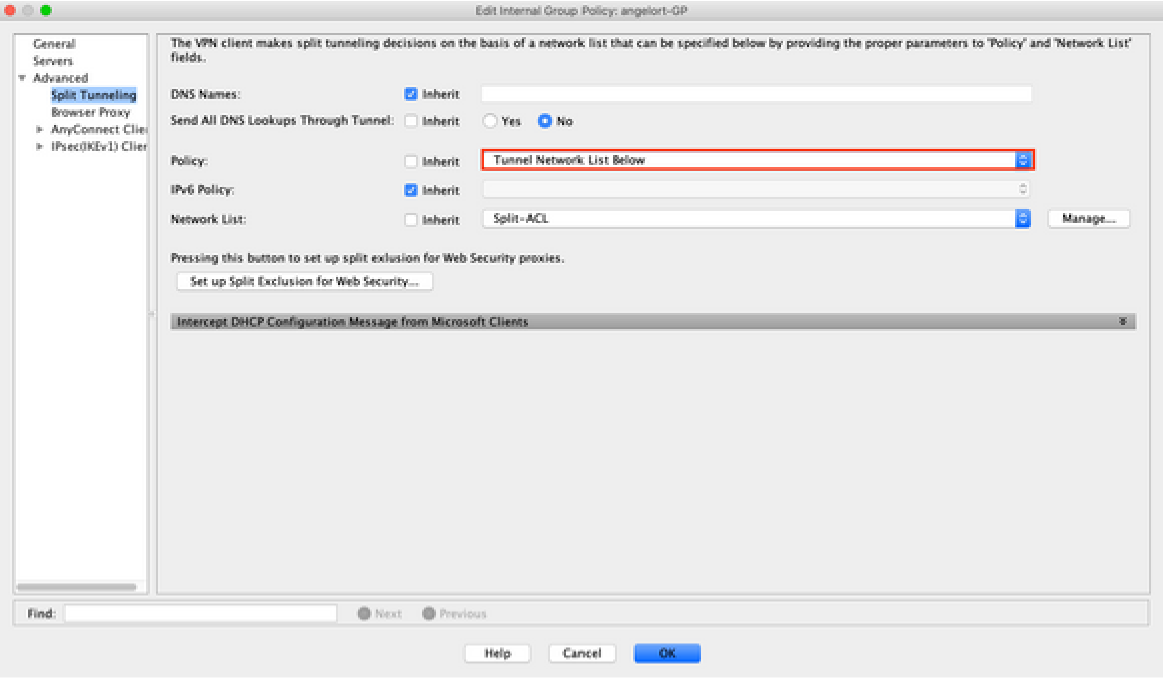
```
ASA# show run access-group

access-group outside_access_in in interface outside

ASA# show run access-list outside_access_in

access-list outside_access_in extended permit ip object AnyConnectPool object-group
INTERNAL_NETWORKS log disable
```

AnyConnect Clients Do Not Have Internet Access

There are two possible scenarios for this issue:

Traffic Destined For The Internet Must Not Go Through The VPN Tunnel

Make sure that the Group-Policy is configured for Split tunnel as Tunnel networks Listed Below and NOT as Tunnel All Networks.



Edit Internal Group Policy: angelort-GP
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Clie
IPsec(IKEv1) Clier
Manage...
Set up Split Exclusion for Web Security...
Intercept DHCP Configuration Message from Microsoft Clients
Find:
Next
Previous
Help
Cancel
OK

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: □ Inherit ○ Yes ● No

Policy: □ Inherit Tunnel Network List Below

IPv6 Policy: ☑ Inherit

Network List: □ Inherit Split-ACL

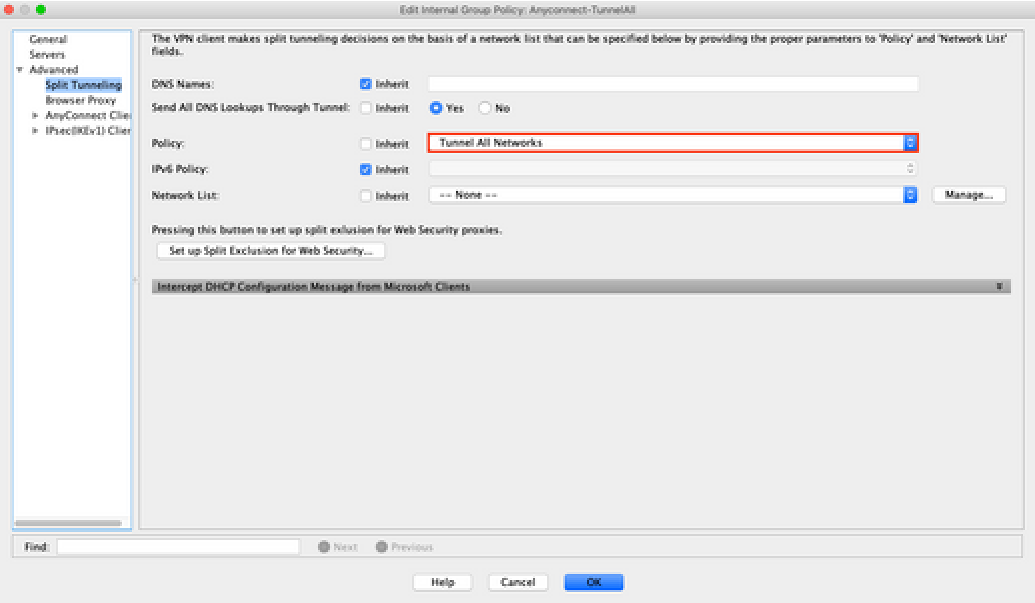
Pressing this button to set up split exlusion for Web Security proxies.

Equivalent CLI Configuration:

```
ASA# show running-config tunnel-group

tunnel-group AnyConnectTG type remote-access

tunnel-group AnyConnectTG general-attributes

 default-group-policy AnyConnectGP-Split

tunnel-group AnyConnectTG webvpn-attributes

 group-alias AnyConnectTG enable

ASA# show run group-policy AnyConnectGP-Split

group-policy AnyConnectGP-Split internal

group-policy AnyConnectGP-Split attributes

 dns-server value 10.0.1.1

 vpn-tunnel-protocol ikev2 ssl-client

 split-tunnel-policy tunnelspecified

 split-tunnel-network-list value Split-ACL

 split-dns none

 split-tunnel-all-dns disable
```

Traffic Destined For The Internet Must Go Through The VPN Tunnel

In this case, the most common Group-Policy configuration for Split tunnel would be to select Tunnel All Networks.



Edit Internal Group Policy: Anyconnect-TunnelAll
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Clie
IPsec(IKEv1) Clier
Manage...
Set up Split Exclusion for Web Security...
Intercept DHCP Configuration Message from Microsoft Clients
Find:
Next
Previous
Help
Cancel
OK

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: □ Inherit ● Yes ○ No

Policy: □ Inherit Tunnel All Networks

IPv6 Policy: ☑ Inherit

Network List: □ Inherit -- None --

Pressing this button to set up split exlusion for Web Security proxies.

Equivalent CLI Configuration:

```
ASA# show run tunnel-group
tunnel-group AnyConnectTG type remote-access
tunnel-group AnyConnectTG general-attributes
default-group-policy AnyConnectGP-Split
tunnel-group AnyConnectTG webvpn-attributes
 group-alias AnyConnectTG enable
ASA# show run group-policy AnyConnectGP-Split
group-policy AnyConnectGP-Split internal
group-policy AnyConnectGP-Split attributes
 dns-server value 10.0.1.1
 vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
 split-dns none
 split-tunnel-all-dns disable
```

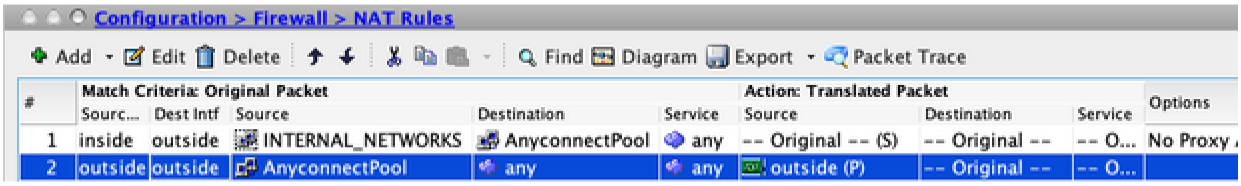
Step 1. Verify NAT exemption configuration for internal network reachability.

Remember that we must still configure a NAT exemption rule to have access to the internal network. Please review Step 2 of the previous section.

Step 2. Verify hairpin configuration for dynamic translations.

In order for AnyConnect clients to have internet access through the VPN tunnel, you need to make sure that the Hairpin NAT configuration is correct for traffic to be translated to the interface´s IP address.

- Navigate to the NAT configuration: **Configuration** > **Firewall** > **NAT Rules**
- Make sure that the Dynamic PAT (Hide) rule is configured for the correct interface (ISP link) as source and destination (hairpin). Also, check that the network used for the AnyConnect VPN address pool is selected in Original source address and the outside interface (or the interface for Internet access) is selected for Translated source:



#	Match Criteria: Original Packet					Action: Translated Packet			Options
	Sourc...	Dest Intf	Source	Destination	Service	Source	Destination	Service	
1	inside	outside	INTERNAL_NETWORKS	AnyconnectPool	any	-- Original -- (S)	-- Original --	-- O...	No Proxy
2	outside	outside	AnyconnectPool	any	any	outside (P)	-- Original --	-- O...	

Equivalent CLI Configuration:

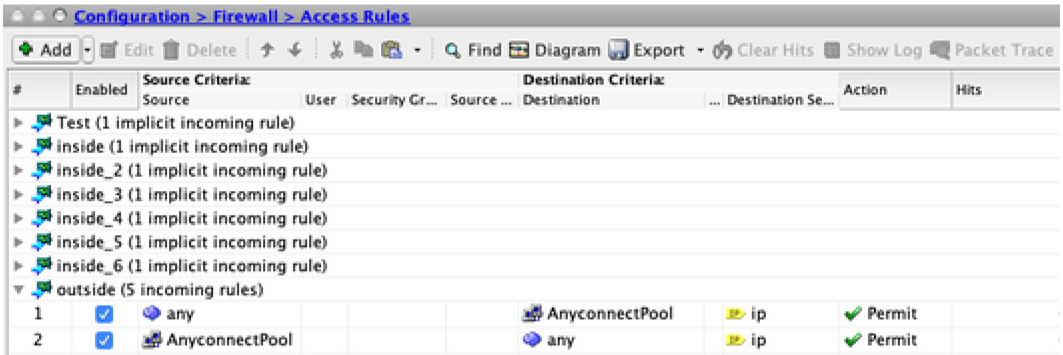
```
ASA# show run object id AnyConnectPool

object network AnyConnectPool

 nat (outside,outside) dynamic interface
```

OR

```
ASA# show run nat

nat (outside,outside) source dynamic AnyConnectPool interface
```

Step 3. Verify Access Rules.

Per your access rules configuration, make sure that traffic from the AnyConnect Clients is allowed to reach the external resources.



#	Enabled	Source Criteria:				Destination Criteria:			Action	Hits
		Source	User	Security Gr...	Source ...	Destination	...	Destination Se...		
Test (1 implicit incoming rule)										
inside (1 implicit incoming rule)										
inside_2 (1 implicit incoming rule)										
inside_3 (1 implicit incoming rule)										
inside_4 (1 implicit incoming rule)										
inside_5 (1 implicit incoming rule)										
inside_6 (1 implicit incoming rule)										
outside (5 incoming rules)										
1	☑	any				AnyconnectPool		ip	✓ Permit	
2	☑	AnyconnectPool				any		ip	✓ Permit	

Equivalent CLI Configuration:

```
access-list outside_access_in extended permit ip object AnyConnectPool any

access-list outside_access_in extended permit ip any object AnyConnectPool

access-group outside_access_in in interface outside
```

AnyConnect Clients Cannot Communicate Between Each Other

There are two possible scenarios for this issue:

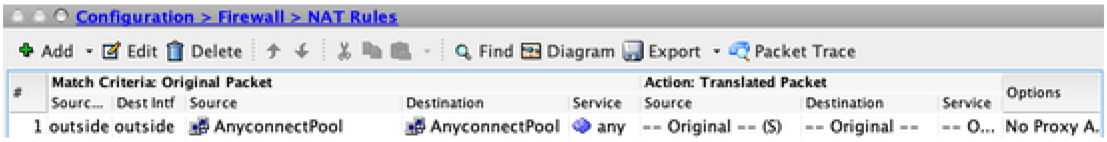
AnyConnect Clients With Tunnel All Networks Configuration In Place

When Tunnel All Networks is configured for AnyConnect means that all traffic, internal and external, must be forwarded to the AnyConnect headend, this becomes a problem when you have Network Address Translation (NAT) for Public Internet access, since traffic that 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.

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: **Configuration** > **Firewall** > **NAT Rules.**
- Make sure 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.



#	Match Criteria: Original Packet					Action: Translated Packet			Options
	Sourc...	Dest Intf	Source	Destination	Service	Source	Destination	Service	
1	outside	outside	AnyconnectPool	AnyconnectPool	any	-- Original -- (S)	-- Original --	-- O...	No Proxy A.

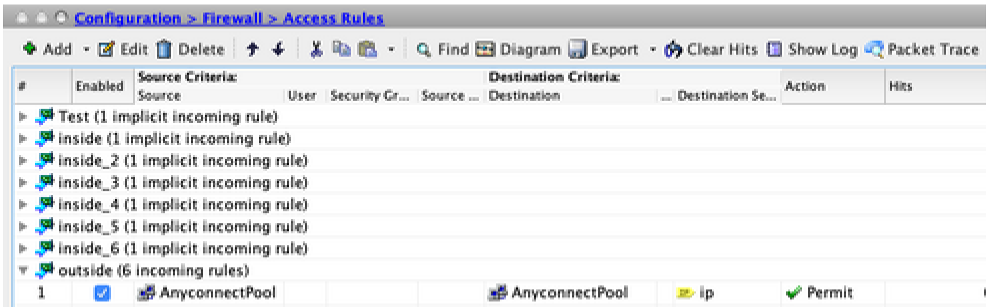
Equivalent CLI Configuration:

ASA# show run nat

nat (outside,outside) source static AnyConnectPool AnyConnectPool destination static AnyConnectPool AnyConnectPool no-proxy-arp route-lookup

Step 2. Verify Access Rules.

Per your access rules configuration, make sure that traffic from the AnyConnect Clients is allowed.



#	Enabled	Source Criteria:				Destination Criteria:			Action	Hits
		Source	User	Security Gr...	Source ...	Destination	...	Destination Se...		
Test (1 implicit incoming rule)										
inside (1 implicit incoming rule)										
inside_2 (1 implicit incoming rule)										
inside_3 (1 implicit incoming rule)										
inside_4 (1 implicit incoming rule)										
inside_5 (1 implicit incoming rule)										
inside_6 (1 implicit incoming rule)										
outside (6 incoming rules)										
1	☑	AnyconnectPool				AnyconnectPool		ip	✓ Permit	

Equivalent CLI Configuration:

access-list outside_access_in extended permit ip object AnyConnectPool object AnyConnectPool

access-group outside_access_in in interface outside

AnyConnect Clients With Tunnel Networks Listed Below Configuration In Place

With Tunnel Networks Listed Below configured for the AnyConnect clients only specific traffic must be forwarded to through the VPN tunnel. However, we need to make sure that the headend has the proper configuration to allow communication within the AnyConnect clients.

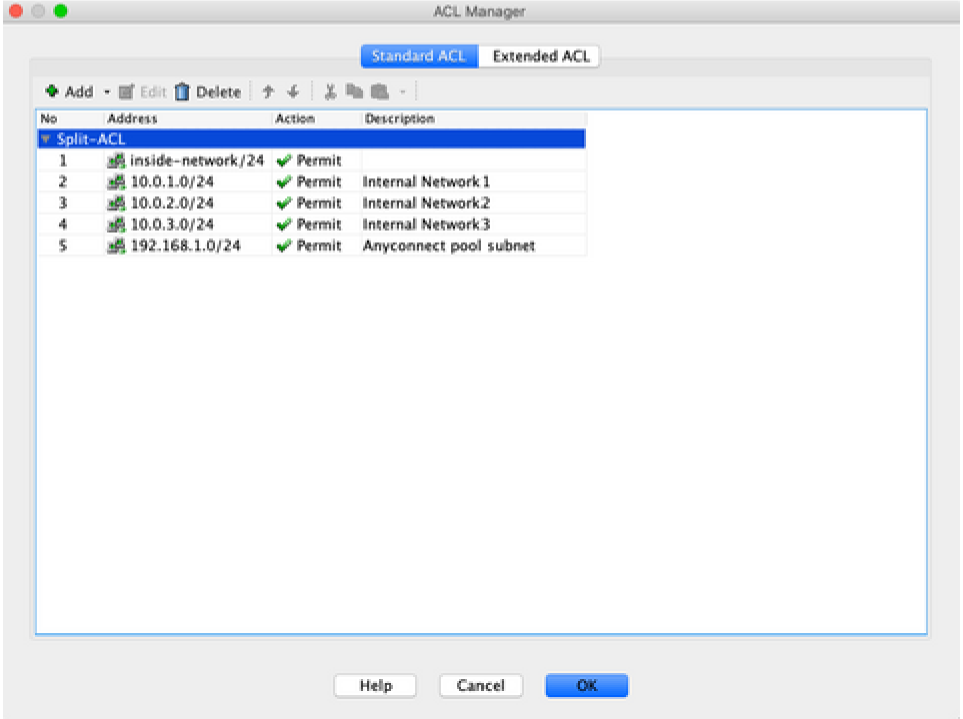
Step 1. Verify NAT exemption configuration.

Please check Step 1 of point 1 in this same section.

Step 2. Verify Split tunnel configuration.

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

- Please read Step 1 of the AnyConnect clients cannot access internal resources section.
- Make sure that the AnyConnect VPN Pool network is listed in the Split tunnel AccessControl List (ACL).



No	Address	Action	Description
Split-ACL			
1	inside-network/24	✓ Permit	
2	10.0.1.0/24	✓ Permit	Internal Network1
3	10.0.2.0/24	✓ Permit	Internal Network2
4	10.0.3.0/24	✓ Permit	Internal Network3
5	192.168.1.0/24	✓ Permit	Anyconnect pool subnet

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

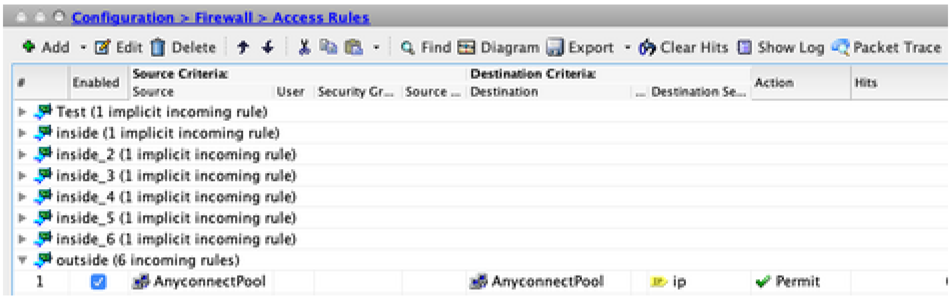
Equivalent CLI Configuration:

```
ip local pool RAVPN-Pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

tunnel-group AnyConnectTG type remote-access

tunnel-group AnyConnectTG general-attributes

 default-group-policy AnyConnectGP-Split

tunnel-group AnyConnectTG webvpn-attributes

 group-alias AnyConnectTG enable

group-policy AnyConnectGP-Split internal
```

```
group-policy AnyConnectGP-Split attributes
 dns-server value 10.0.1.1
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
 split-dns none
 split-tunnel-all-dns disable
ASA# show run access-list Split-ACL
access-list Split-ACL standard permit 10.28.28.0 255.255.255.0
access-list Split-ACL remark Internal Network1
access-list Split-ACL standard permit 10.0.1.0 255.255.255.0
access-list Split-ACL remark Internal Network2
access-list Split-ACL standard permit 10.0.2.0 255.255.255.0
access-list Split-ACL remark Internal Network3
access-list Split-ACL standard permit 10.0.3.0 255.255.255.0
access-list Split-ACL remark AnyConnect pool subnet
access-list Split-ACL standard permit 192.168.1.0 255.255.255.0
```

Step 3. Verify Access Rules.

Per your access rules configuration, make sure that traffic from the AnyConnect Clients is allowed.



#	Enabled	Source Criteria:				Destination Criteria:			Action	Hits
		Source	User	Security Gr...	Source ...	Destination	...	Destination Se...		
Test (1 implicit incoming rule)										
inside (1 implicit incoming rule)										
inside_2 (1 implicit incoming rule)										
inside_3 (1 implicit incoming rule)										
inside_4 (1 implicit incoming rule)										
inside_5 (1 implicit incoming rule)										
inside_6 (1 implicit incoming rule)										
outside (6 incoming rules)										
1	☑	AnyconnectPool				AnyconnectPool		ip	✓ Permit	

Equivalent CLI Configuration:

```
access-list outside_access_in extended permit ip object AnyConnectPool object AnyConnectPool
access-group outside_access_in in interface outside
```

AnyConnect Clients Cannot Establish Phone Calls

There are times where we 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 these points:

- Network topology for voice.
- Protocols involved. For example, Session Initiation Protocol (SIP), Rapid Spanning Tree Protocol (RSTP), and so on.
- How the VPN phones connect to the Cisco Unified Communications Manager (CUCM).

By default, 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 next 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, you can use the **show service-policy** command as shown:

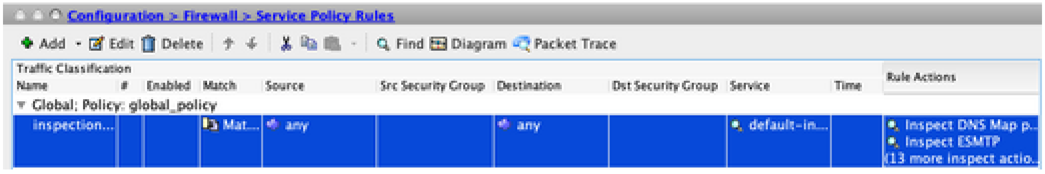
```
ASA#show service-policy

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 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 you want to use voice services over AnyConnect VPN.

To disable SIP inspection complete the next steps:

Step 1. Navigate to **Configuration > Firewall > Service Policy Rules.**

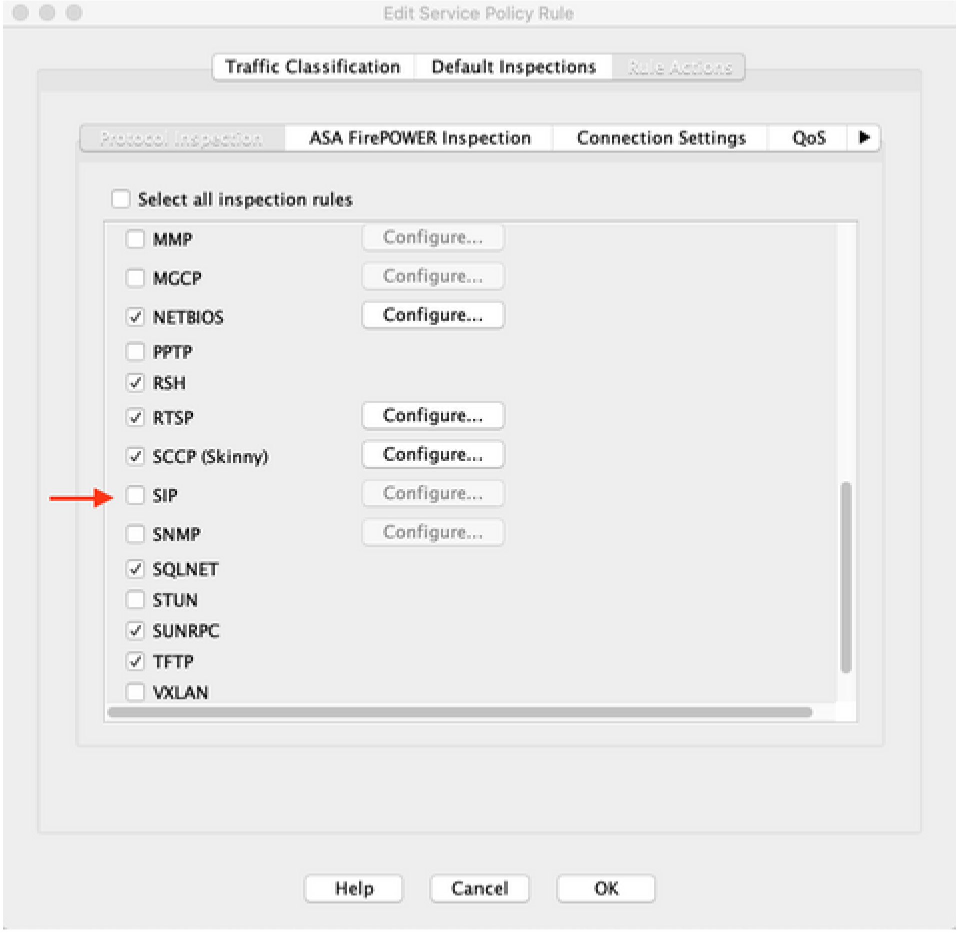


Configuration > Firewall > Service Policy Rules

Traffic Classification										Rule Actions
Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	
Global; Policy: global_policy										
inspection...			Mat...	any		any		default-in...		Inspect DNS Map p... Inspect ESMTP (13 more inspect actio...

Step 2. Edit the **Global Policy Rule > Rule Actions.**

Uncheck the SIP protocol box.



Edit Service Policy Rule

□ Select all inspection rules

□ MMP
□ MGCP
☑ NETBIOS
□ PPTP
☑ RSH
☑ RTSP
☑ SCCP (Skinny)
□ SIP
□ SNMP
☑ SQLNET
□ STUN
☑ SUNRPC
☑ TFTP
□ VXLAN

Equivalent CLI Configuration:

```
ASA# show run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
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 esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
```

Next step is to disable SIP inspection:

```
ASA# configure terminal
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect sip
```

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

```
ASA# show run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
```

```
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 esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
```

AnyConnect Clients Can Establish Phone Calls But There Is No Audio On The Calls

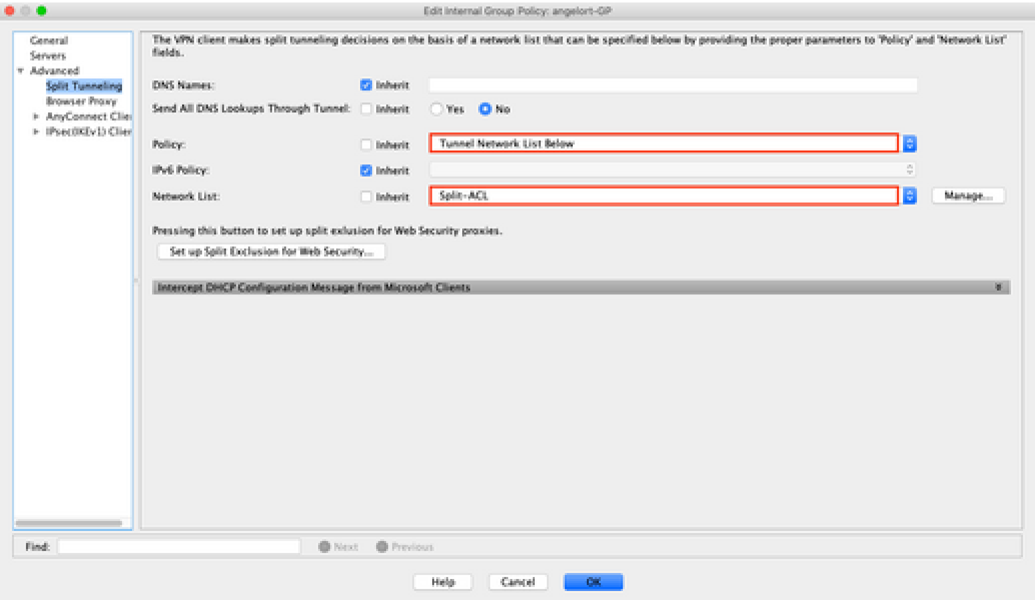
As mentioned in the previous section, a very common need for AnyConnect clients is to establish phone calls when connected to the VPN. In some cases, the call can be established, however, clients can experience lack of audio on it. This applies to the next scenarios:

- 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, you can check these steps:

Step 1. Verify Split tunnel configuration.

- Navigate to the Connection Profile that users are connected to: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile > Select the Profile.**
- Navigate to the Group-Policy assigned to that Profile; **Group Policy > Manage > Edit > Advanced > Split Tunneling.**
- Check the Split Tunnel configuration.


Edit Internal Group Policy: angelort-GP
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Clie
IPsec(IKEv1) Clier
Set up Split Exclusion for Web Security...
Intercept DHCP Configuration Message from Microsoft Clients
Manage...
Find:
Next
Previous
Help
Cancel
OK

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: □ Inherit ○ Yes ● No

Policy: □ Inherit Tunnel Network List Below

IPv6 Policy: ☑ Inherit

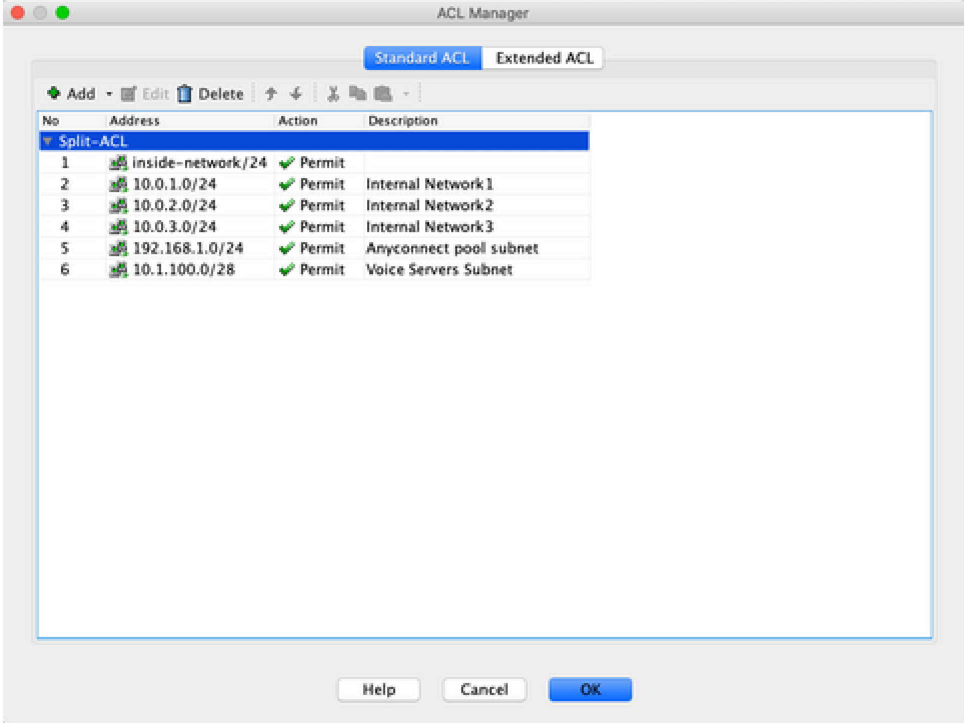
Network List: □ Inherit Split-ACL

Pressing this button to set up split exlusion for Web Security proxies.

- If configured as Tunnel Networks Listed Below, verify the Access Control List (ACL) configuration.

In the same window navigate to **Manage > Select the Access List > Edit the Access List for Split tunnel.**

Make sure that the Voice Servers and the AnyConnect IP Pool networks are listed in the Split tunnel Access Control List (ACL).



No	Address	Action	Description
Split-ACL			
1	inside-network/24	✓ Permit	
2	10.0.1.0/24	✓ Permit	Internal Network1
3	10.0.2.0/24	✓ Permit	Internal Network2
4	10.0.3.0/24	✓ Permit	Internal Network3
5	192.168.1.0/24	✓ Permit	Anyconnect pool subnet
6	10.1.100.0/28	✓ Permit	Voice Servers Subnet

Equivalent CLI Configuration:

```
tunnel-group AnyConnectTG type remote-access

tunnel-group AnyConnectTG general-attributes

 default-group-policy AnyConnectGP-Split

tunnel-group AnyConnectTG webvpn-attributes
```

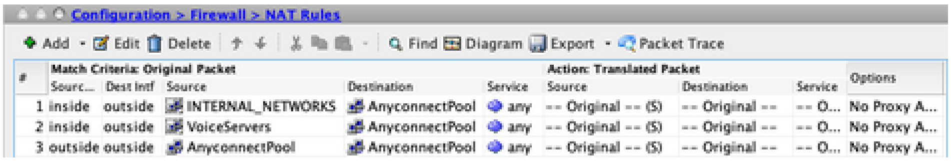
```
 group-alias AnyConnectTG enable
group-policy AnyConnectGP-Split internal
group-policy AnyConnectGP-Split attributes
 dns-server value 10.0.1.1
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split-ACL
 split-dns none
 split-tunnel-all-dns disable
access-list Split-ACL standard permit 10.28.28.0 255.255.255.0
access-list Split-ACL remark Internal Network1
access-list Split-ACL standard permit 10.0.1.0 255.255.255.0
access-list Split-ACL remark Internal Network2
access-list Split-ACL standard permit 10.0.2.0 255.255.255.0
access-list Split-ACL remark Internal Network3
access-list Split-ACL standard permit 10.0.3.0 255.255.255.0
access-list Split-ACL remark AnyConnect pool subnet
access-list Split-ACL standard permit 192.168.1.0 255.255.255.0
access-list Split-ACL remark Voice Servers Subnet
access-list Split-ACL standard permit 10.1.100.0 255.255.255.240
```

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: **Configuration > Firewall > NAT Rules.**

Make sure 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.



Configuration > Firewall > NAT Rules

#	Match Criteria: Original Packet					Action: Translated Packet			Options
	Sourc...	Dest Intf	Source	Destination	Service	Source	Destination	Service	
1	inside	outside	INTERNAL_NETWORKS	AnyconnectPool	any	-- Original -- (S)	-- Original --	-- O...	No Proxy A...
2	inside	outside	VoiceServers	AnyconnectPool	any	-- Original -- (S)	-- Original --	-- O...	No Proxy A...
3	outside	outside	AnyconnectPool	AnyconnectPool	any	-- Original -- (S)	-- Original --	-- O...	No Proxy A...

Equivalent CLI Configuration:

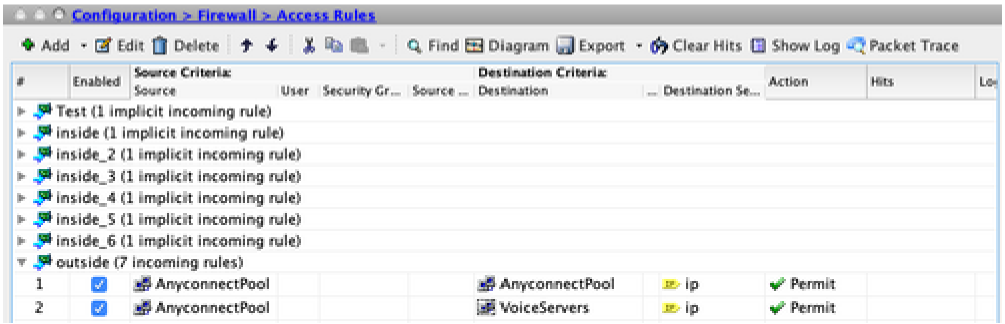
```
nat (inside,outside) source static INTERNAL_NETWORKS INTERNAL_NETWORKS destination static AnyConnectPool AnyConnectPool no-proxy-arp route-lookup

nat (inside,outside) source static VoiceServers VoiceServers destination static AnyConnectPool AnyConnectPool no-proxy-arp route-lookup

nat (outside,outside) source static AnyConnectPool AnyConnectPool destination static AnyConnectPool AnyConnectPool no-proxy-arp route-lookup
```

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 Rules.

Per your access rules configuration, make sure that traffic from the AnyConnect Clients is allowed to reach the Voice servers and involved networks.



#	Enabled	Source Criteria:				Destination Criteria:			Action	Hits	Lo
		Source	User	Security Gr...	Source ...	Destination	...	Destination Se...			
Test (1 implicit incoming rule)											
inside (1 implicit incoming rule)											
inside_2 (1 implicit incoming rule)											
inside_3 (1 implicit incoming rule)											
inside_4 (1 implicit incoming rule)											
inside_5 (1 implicit incoming rule)											
inside_6 (1 implicit incoming rule)											
outside (7 incoming rules)											
1	☑	AnyconnectPool				AnyconnectPool		ip	✓ Permit		
2	☑	AnyconnectPool				VoiceServers		ip	✓ Permit		

Equivalent CLI Configuration:

```
access-list outside_access_in extended permit ip object AnyConnectPool object AnyConnectPool

access-list outside_access_in extended permit ip object AnyConnectPool object-group VoiceServers

access-group outside_access_in in interface outside
```

Related Information

- For additional assistance, please contact TAC. A valid support contract is required: Cisco Worldwide Support Contacts
- You can also visit the Cisco VPN Community here.