

FTDでの一般的なAnyConnect通信の問題のトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[推奨されるトラブルシューティングプロセス](#)

[AnyConnectクライアントが内部リソースにアクセスできない](#)

[AnyConnectクライアントがインターネットにアクセスできない](#)

[AnyConnectクライアントは相互に通信できない](#)

[AnyConnectクライアントが電話を確立できない](#)

[AnyConnectクライアントは通話を確立できますが、通話に音声は流れません](#)

[関連情報](#)

概要

このドキュメントでは、Secure Socket Layer(SSL)またはInternet Key Exchange(IKEv2)を使用する場合に、Firepower Threat Defense(FTD)上のCisco AnyConnectセキュアモビリティクライアントの最も一般的な通信問題のトラブルシューティング方法について説明します。

著者 : Cisco TACエンジニア、Angel OrtizおよびFernando Jimenez

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTDはFMC 6.4.0によって管理されます。
- AnyConnect 4.8

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

推奨されるトラブルシューティングプロセス

このガイドでは、FTDをリモートアクセス仮想プライベートネットワーク(VPN)ゲートウェイとして使用する場合にAnyConnectクライアントが抱える一般的な通信の問題のトラブルシューティング方法について説明します。これらのセクションでは、次の問題に対処し、解決策を提供します。

- AnyConnectクライアントは内部リソースにアクセスできません。
- AnyConnectクライアントはインターネットにアクセスできません。
- AnyConnectクライアントは相互に通信できません。
- AnyConnectクライアントは電話を確立できません。
- AnyConnectクライアントは電話を確立できます。ただし、コールに音声はありません。

AnyConnectクライアントが内部リソースにアクセスできない

次のステップを実行します。

ステップ1：スプリットトンネルの設定を確認します。

- AnyConnectクライアントが接続されている接続プロファイルに移動します。 [Devices] > [VPN] > [Remote Access] > [Connection Profile] > [Select the Profile]
- そのプロファイルに割り当てられたグループポリシーに移動します：[グループポリシーの編集] > [一般]。
- 図に示すように、スプリットトンネリングの設定を確認します。

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

- 次に示すトンネルネットワークとして設定されている場合、アクセスコントロールリスト (ACL) の設定を確認します。

[Objects] > [Object Management] > [Access List] > [Edit the Access List for Split tunneling]に移動します。

- 図に示すように、AnyConnect VPNクライアントから到達しようとするネットワークが、そのアクセスリストにリストされていることを確認します。

Edit Standard Access List Object

? X

Name: Split-tunnel-ACL

Entries (1)

Sequence No	Action	Network
1	Allow	InternalNetwork1 InternalNetwork2 InternalNetwork3

Allow Overrides

Save Cancel

ステップ 2： ネットワークアドレス変換(NAT)免除の設定を確認します。

トラフィックがインターフェイスのIPアドレスに変換されないように、NAT免除ルールを設定する必要があります。通常はインターネットアクセス用に設定されます(Port Address Translation(PAT)を使用)。

- NAT設定に移動します。 [Devices] > [NAT]。
- 正しい送信元 (内部) および宛先 (AnyConnect VPNプール) ネットワークに対してNAT除外ルールが設定されていることを確認します。また、図に示すように、正しい送信元インターフェイスと宛先インターフェイスが選択されていることを確認します。

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

注： NAT免除ルールが設定されている場合は、no-proxy-arpをチェックし、ベストプラクティスとしてルートルックアップオプションを実行します。

ステップ3： アクセス制御ポリシーを確認します。

アクセスコントロールポリシーの設定に従って、図に示すように、AnyConnectクライアントからのトラフィックが選択した内部ネットワークに到達することを確認します。



AnyConnectクライアントがインターネットにアクセスできない

この問題には2つのシナリオがあります。

1. インターネット宛てのトラフィックは、VPNトンネルを通過できません。

図に示すように、グループポリシーがスプリットトンネリングに対してTunnel networksとして設定され、Allow all traffic over tunnelとして設定されていないことを確認します。

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. インターネット宛てのトラフィックは、VPNトンネルを通過する必要があります。

この場合、スプリットトンネリングの最も一般的なグループポリシー設定では、図に示すように[Allow all traffic over tunnel]を選択します。

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

ステップ1：内部ネットワークの到達可能性に関するNAT免除の設定を確認します。

内部ネットワークにアクセスするには、NAT除外ルールを設定する必要があることに注意してください。のステップ2を確認してください。 AnyConnectクライアントが内部リソースにアクセスできない。

ステップ2：ダイナミック変換のヘアピンング設定を確認します。

AnyConnectクライアントがVPNトンネル経由でインターネットにアクセスできるようにするには、トラフィックをインターフェイスのIPアドレスに変換するためのヘアピンングNAT設定が正しいことを確認する必要があります。

- NAT設定に移動します。 [Devices] > [NAT]。
- ダイナミックNATルールが、送信元および宛先（ヘアピンング）として正しいインターフェイス(インターネットサービスプロバイダー(ISP)リンク)に設定されていることを確認します。また、[Original source]および[Destination Interface IP]でAnyConnect VPNアドレスプールに使用するネットワークが選択されていることを確認します 図に示すように、[Translated source]オプションが選択されます。

#	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:fa...

ステップ3：アクセス制御ポリシーを確認します。

アクセスコントロールポリシーの設定に従って、図に示すように、AnyConnectクライアントからのトラフィックが外部リソースに到達できることを確認します。

#	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

AnyConnectクライアントは相互に通信できない

この問題には2つのシナリオがあります。

1. AnyConnectクライアント トンネル上のすべてのトラフィックを許可する 設定を行います。
2. AnyConnectクライアント 下で指定したトンネルネットワーク 設定を行います。

1. AnyConnectクライアント トンネル上のすべてのトラフィックを許可する 設定を行います。

時期 トンネル上のすべてのトラフィックを許可する はAnyConnect用に設定されているため、内部および外部のすべてのトラフィックをAnyConnectヘッドエンドに転送する必要があります。これは、パブリックインターネットアクセス用のNATがある場合に問題になります。これは、別のAnyConnectクライアント宛てのトラフィックがインターフェイスIPアドレスにに変換されます。

ステップ1:NAT免除設定を確認します。

この問題を解決するには、AnyConnectクライアント内で双方向通信を可能にするために、手動NAT除外ルールを設定する必要があります。

- NAT設定に移動します。 [Devices] > [NAT]。
- NAT除外ルールが正しい送信元 (AnyConnect VPNプール) と宛先に設定されていることを確認します。 (AnyConnect VPNプール) ネットワーク。また、図に示すように、正しいヘアピン設定が設定されていることを確認します。

#	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-proxy

ステップ2 : アクセスコントロールポリシーを確認します。

アクセスコントロールポリシーの設定に従って、図に示すように、AnyConnectクライアントからのトラフィックが許可されていることを確認します。

#	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. Anyconnectクライアントと 下で指定したトンネルネットワーク 設定を行います。

さらにトラブルシューティングを行うために、 下で指定したトンネルネットワーク AnyConnectクライアントに設定された特定のトラフィックだけが、VPNトンネルを介して転送されます。ただし、ヘッドエンドがAnyConnectクライアント内で通信できるように適切に設定されていることを確認する必要があります。

ステップ1:NAT免除設定を確認します。

「Allow all traffic over tunnel」セクションのステップ1をチェックして下さい。

ステップ2 : スプリットトンネリングの構成を確認します。

AnyConnectクライアントがクライアント間で通信するには、スプリットトンネルACLにVPNプールアドレスを追加する必要があります。

- のステップ1に従ってください。 AnyConnectクライアントが内部リソースにアクセスできない。
- 図に示すように、AnyConnect VPNプールネットワークがスプリットトンネリングアクセスリストにリストされていることを確認します。

Edit Standard Access List Object

? X

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

注：AnyConnectクライアントに複数のIPプールがあり、異なるプール間の通信が必要な場合は、スプリットトンネリングACLですべてのプールを追加し、必要なIPプールにNAT免除ルールを追加します。

ステップ3：アクセス制御ポリシーを確認します。

図に示すように、AnyConnectクライアントからのトラフィックが許可されていることを確認します。

#	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	✓ Allow

AnyConnectクライアントが電話を確立できない

AnyConnectクライアントがVPN経由で電話コールとビデオ会議を確立する必要があるシナリオがいくつかあります。

AnyConnectクライアントは、問題なくAnyConnectヘッドエンドに接続できます。内部および外部のリソースに到達できますが、電話を確立できません。

この場合、次の点を考慮する必要があります。

- 音声のネットワークトポロジ。
- 関連するプロトコル。セッション開始プロトコル(SIP)、ラピッドスパンニングツリープロトコル(RSTP)など

- VPN電話がCisco Unified Communications Manager(CUCM)に接続する方法

デフォルトでは、FTDとASAのグローバルポリシーマップでは、デフォルトでアプリケーションインスペクションが有効になっています。

ほとんどの場合、AnyConnectヘッドエンドで信号および音声トラフィックを変更するアプリケーションインスペクションが有効になっているため、VPN電話はCUCMとの信頼性の高い通信を確立できません。

アプリケーションインスペクションを適用できる音声およびビデオアプリケーションの詳細については、次のドキュメントを参照してください。

[章：音声およびビデオプロトコルの検査](#)

アプリケーショントラフィックがグローバルポリシーマップによってドロップまたは変更されているかどうかを確認するには、次に示すようにshow service-policyコマンドを使用します。

```
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
```

```
.
```

この例では、SIPインスペクションによってトラフィックがどのようにドロップされるかを確認できます。

さらに、SIPインスペクションでは、IPヘッダーではなくペイロード内のIPアドレスを変換する場合にも異なる問題が発生するため、AnyConnect VPNで音声サービスを使用する場合は無効にすることを推奨します。

これを無効にするには、次の手順を実行する必要があります。

ステップ1：特権EXECモードに入ります。

このモードにアクセスする方法の詳細については、次のドキュメントを参照してください。

[章：コマンドラインインターフェイス\(CLI\)の使用](#)

ステップ2：グローバル・ポリシー・マップを確認します。

次のコマンドを実行し、SIPインスペクションが有効になっているかどうかを確認します。

```
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
```

ステップ3:SIPインスペクションを無効にします。

SIPインスペクションが有効になっている場合は、次のclishプロンプトからrunningコマンドをオフにします。

```
> configure inspection sip disable
```

ステップ4：グローバルポリシーマップを再度確認します。

グローバルポリシーマップからSIPインスペクションが無効になっていることを確認します。

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

```
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect netbios
inspect tftp
inspect ip-options
inspect icmp
inspect icmp error
inspect esmtp
```

AnyConnectクライアントは通話を確立できますが、通話に音声は流れません

前のセクションで説明したように、AnyConnectクライアントの非常に一般的なニーズは、VPNに接続するときに電話コールを確立することです。コールを確立できる場合もありますが、クライアントで音声がかえれない場合があります。これは、次のシナリオに適用されます。

- AnyConnectクライアントと外部番号の間のコールに音声がかえない。
- AnyConnectクライアントと別のAnyConnectクライアントの間のコールで音声がかえない。

これを修正するには、次の手順を実行します。

ステップ1：スプリットトンネリングの構成を確認します。

- 接続に使用する接続プロファイルに移動します。 [Devices] > [VPN] > [Remote Access] > [Connection Profile] > [Select the Profile]
- そのプロファイルに割り当てられたグループポリシーに移動します：[グループポリシーの編集] > [一般]。
- 図に示すように、スプリットトンネリングの設定を確認します。

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

- 次のように設定されている場合 下で指定したトンネルネットワークアクセスリストの設定を確認します。 **Objects > Object Management > Access List > Edit the Access List for Split tunneling。**
- 図に示すように、音声サーバとAnyConnect IPプールネットワークがスプリットトンネリングアクセスリストにリストされていることを確認します。

Edit Standard Access List Object

? X

Name: Split-tunnel-ACL

Entries (2)

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

Allow Overrides

Save Cancel

ステップ2:NAT免除設定を確認します。

NAT免除ルールは、AnyConnect VPNネットワークから音声サーバネットワークへのトラフィックを除外し、AnyConnectクライアント内で双方向通信を許可するように設定する必要があります。

- NAT設定に移動します。 [Devices] > [NAT]。
- 正しい送信元（音声サーバ）および宛先（AnyConnect VPNプール）ネットワークにNAT免除ルールが設定されていること、およびAnyConnectクライアントとAnyConnectクライアントの通信を許可するヘアピンNATルールが設定されていることを確認します。さらに、図に示すように、ネットワーク設計に従って、ルールごとに正しい着信インターフェイスと発信インターフェイスの設定が行われていることを確認します。

Rules

Filter by Device Add Rule

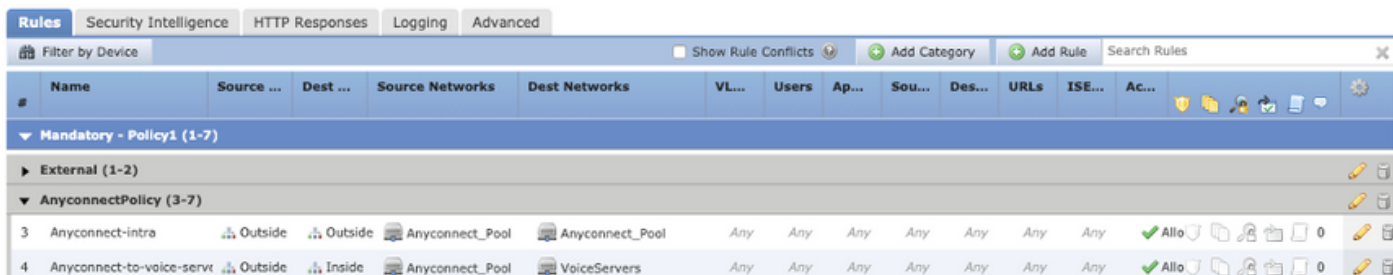
#..	Dir...	T...	Original Packet				Translated Packet				Options
			Source Interface Ob...	Destination Interface Obje...	Original Sources	Original Destinations	O... S...	Translated Sources	Translated Destinations	T...	
▼ NAT Rules Before											
1	↔	S...	Inside_interfac	outside_interface	InternalNetworksGroup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

ステップ3:SIPインスペクションが無効になっていることを確認します。

前のセクションを確認してください AnyConnectクライアントが電話を確立できない を参照してください。

ステップ4 : アクセスコントロールポリシーを確認します。

アクセスコントロールポリシーの設定に従って、図に示すように、AnyConnectクライアントからのトラフィックが音声サーバおよび関連するネットワークに到達できることを確認します。



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

関連情報

- このビデオでは、このドキュメントで説明するさまざまな問題の設定例を示します。
- その他のサポートについては、Technical Assistance Center(TAC)にお問い合わせください。有効なサポート契約が必要です。 [各国のシスコ サポートの連絡先](#).
- Cisco VPN Community [here](#).