

ASA での AnyConnect 管理 VPN トンネルの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[管理トンネルの動作](#)

[制限事項](#)

[設定](#)

[ASDM/CLIを使用したASAでの設定](#)

[AnyConnect管理VPNプロファイルの作成](#)

[AnyConnect管理VPNプロファイルの展開方法](#)

[\(オプション\) Tunnel-All設定をサポートするカスタム属性を設定します](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、VPNゲートウェイが管理VPNトンネルを介してAnyConnectセキュアモバイルクライアントからの接続を受け入れるようにASAを設定する方法について説明します。

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。

- Adaptive Security Device Manager(ASDM)によるVPN設定
- 基本的な適応型セキュリティアプライアンス(ASA)のCLI設定
- X509証明書

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。

- Cisco ASAソフトウェアバージョン9.12(3)9
- Cisco ASDMソフトウェアバージョン7.12.2

- Cisco AnyConnectセキュアモビリティクライアントバージョン4.8.03036がインストールされたWindows 10

 注：AnyConnect VPN Web deployパッケージ([anyconnect-win*.pkg](#) or [anyconnect-macos*.pkg](#))は、Cisco [Software Download](#) (登録ユーザ専用) からダウンロードします。リモートユーザコンピュータにダウンロードされるASAのフラッシュメモリにAnyConnect VPNクライアントをコピーし、ASAとのSSL VPN接続を確立します。詳細については、ASAコンフィギュレーションガイドの「[AnyConnectクライアントのインストール](#)」セクションを参照してください。

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、クリアな(デフォルト)設定で作業を開始しています。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。

背景説明

管理VPNトンネルは、エンドユーザによってVPN接続が確立される場合だけでなく、クライアントシステムの電源が投入されるたびに企業ネットワークへの接続を保証します。オフィス外のエンドポイント、特にユーザがVPN経由でオフィスのネットワークにほとんど接続していないデバイスに対して、パッチ管理を実行できます。企業ネットワーク接続を必要とするエンドポイントOSログインスクリプトでも、この機能を利用できます。

AnyConnect管理トンネルを使用すると、管理者はユーザがログインする前に、ユーザの介入なしでAnyConnectを接続できます。AnyConnect管理トンネルはTrusted Network Detection(TND)と組み合わせて動作できるため、エンドポイントがオフプレミスで、ユーザが開始したVPNから切断された場合にのみトリガーされます。AnyConnect管理トンネルはエンドユーザに対して透過的で、ユーザがVPNを開始すると自動的に切断されます。

| OS/アプリケーション | 最小バージョン要件 |
|--------------------------|------------|
| ASA | 9.0.1 |
| ASDM | 7.10.1 |
| Windows AnyConnect/バージョン | 4.7.00136 |
| macOS AnyConnect/バージョン | 4.7.01076 |
| Linux | サポートされていない |

管理トンネルの動作

AnyConnect VPNエージェントサービスは、システムの起動時に自動的に開始されます。管理トンネル機能が(管理VPNプロファイルを介して)有効になっていることが検出されるため、管理クライアントアプリケーションが起動されて管理トンネル接続が開始されます。管理クライアントアプリケーションは、管理VPNプロファイルからのホストエントリを使用して接続を開始します。次に、VPNトンネルは通常どおり確立されますが、例外が1つあります。管理トンネルはユーザに対して透過的に動作するように意図されているため、管理トンネルの接続中にソフトウェ

アの更新は行われません。

ユーザはAnyConnect UIを使用してVPNトンネルを開始し、これにより管理トンネルの終端がトリガーされます。管理トンネルが終端すると、ユーザトンネルの確立は通常どおり継続されます。

ユーザがVPNトンネルの接続を解除すると、管理トンネルの自動再確立がトリガーされます。

制限事項

- ユーザーの操作はサポートされていません
- マシン証明書ストア(Windows)による証明書ベースの認証のみがサポートされます
- 厳密なサーバ証明書チェックが適用される
- プライベートプロキシはサポートされていません
- パブリックプロキシはサポートされていません (ネイティブプロキシ設定がブラウザから取得されないプラットフォームでは、ProxyNative値がサポートされています)
- AnyConnectカスタマイズスクリプトはサポートされていません

 注：詳細については、「[管理VPNトンネルについて](#)」を参照してください。

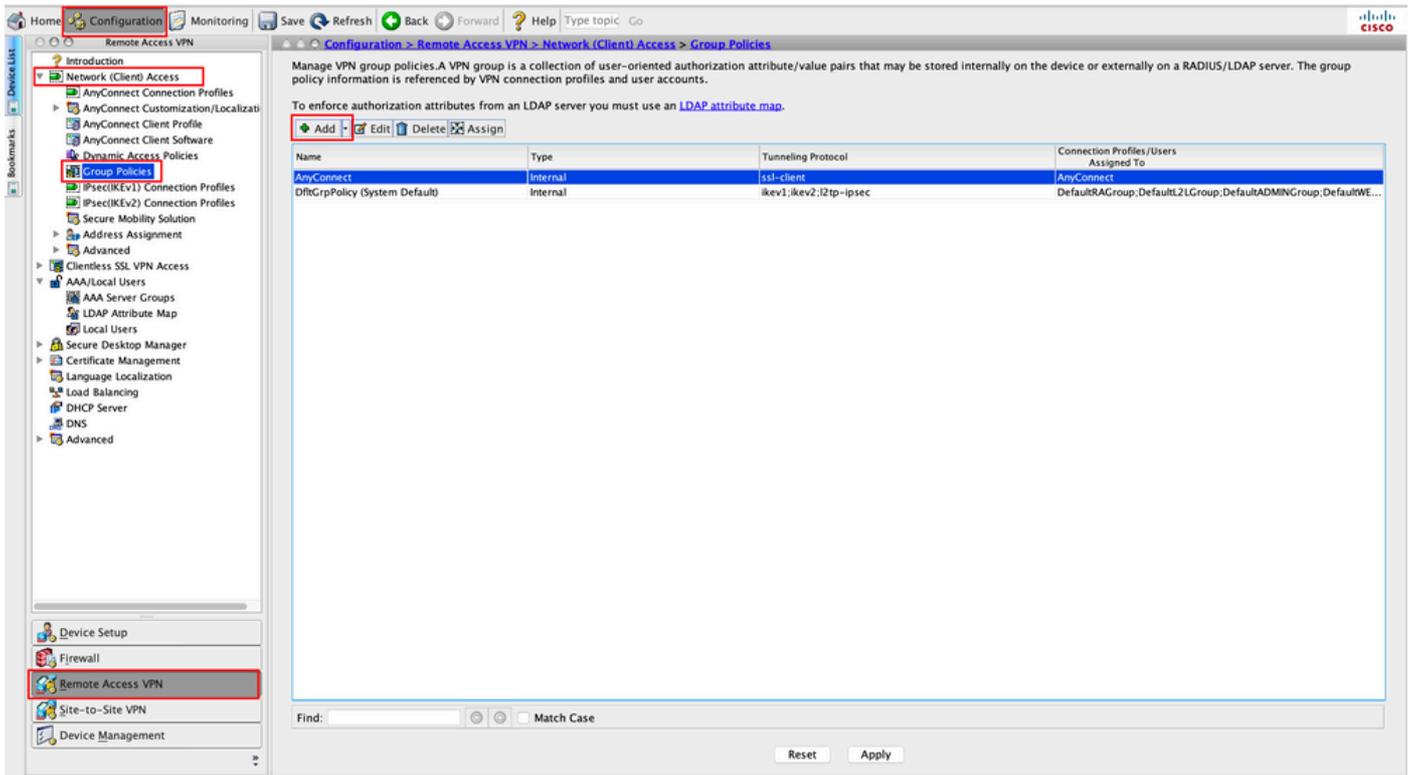
設定

このセクションでは、Cisco ASAをVPNゲートウェイとして設定し、管理VPNトンネル経由でAnyConnectクライアントからの接続を受け入れる方法について説明します。

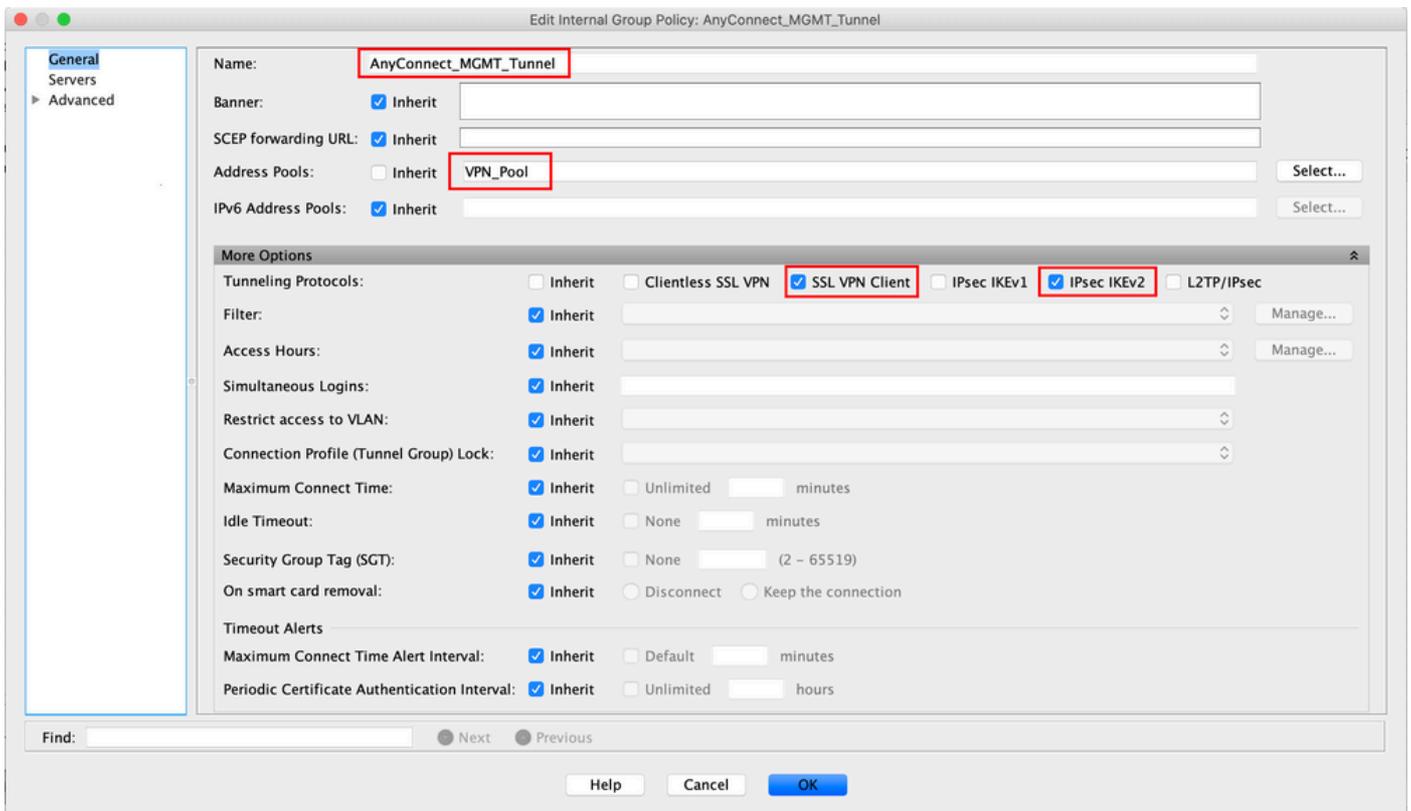
ASDM/CLIを使用したASAでの設定

ステップ 1：AnyConnectグループポリシーを作成します。に移動し Configuration > Remote Access VPN > Network (Client) Access > Group Policies ます。をクリックします。 Add

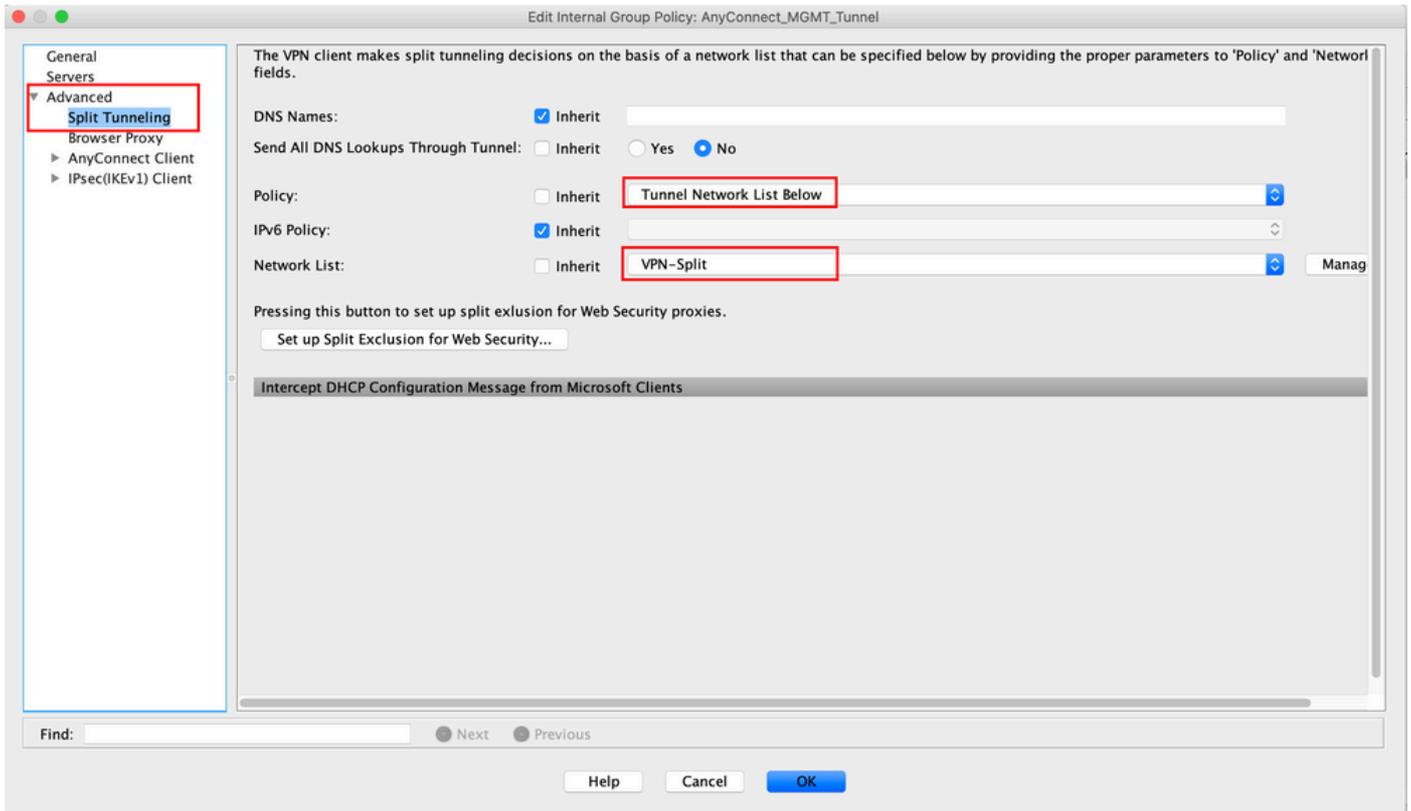
 注：新しいAnyConnectグループポリシーを作成することをお勧めします。このポリシーは、AnyConnect管理トンネルのみに使用されます。



ステップ 2 : グループポリシーのName 「」を指定します。を割り当て/作成し Address Pool ます。次の図に示すように、 Tunneling Protocols aSSL VPN Client and/orIPsec IKEv2 を選択します。

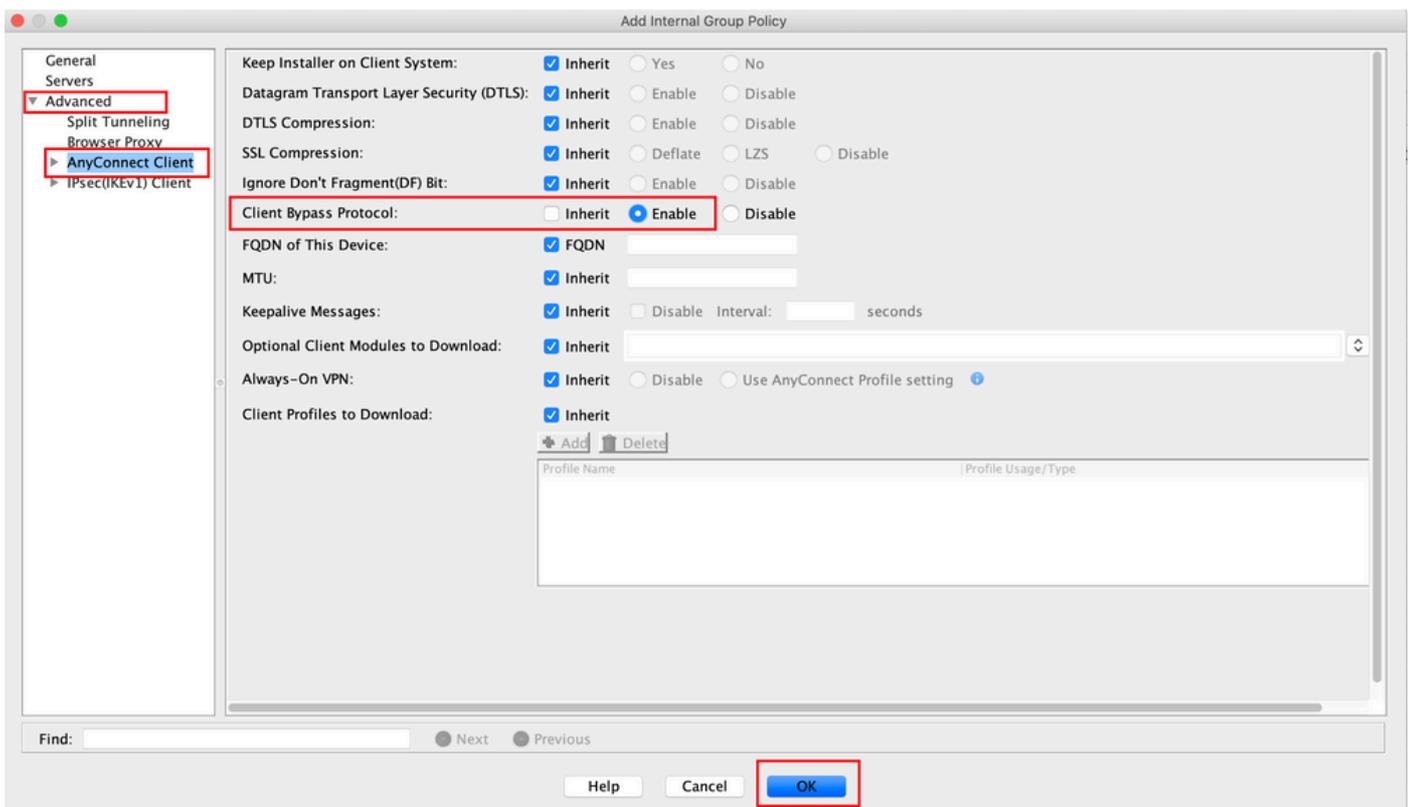


ステップ 3 : に移動し Advanced > Split Tunneling ます。図に示すように Policy、 を設定し Tunnel Network List Below、 Network List を選択します。

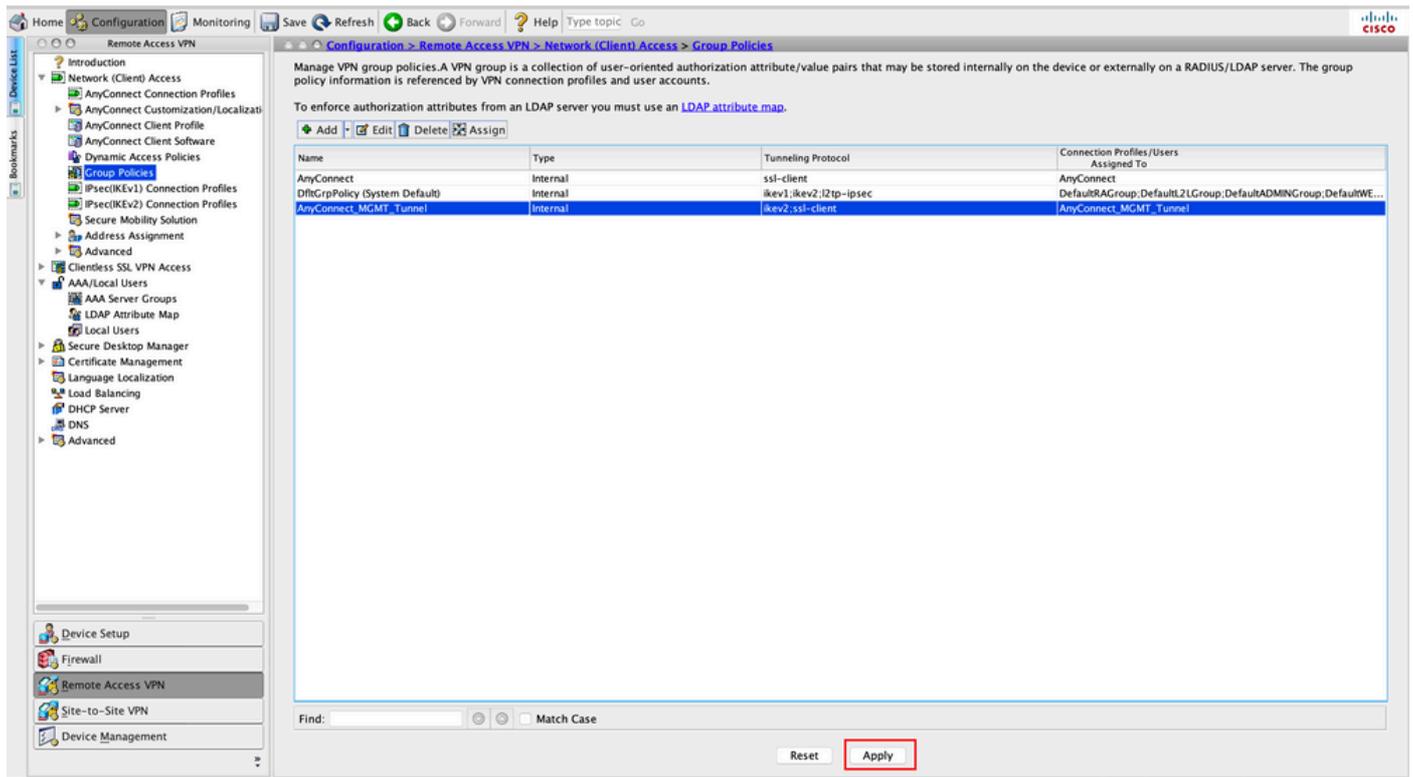


注：クライアントアドレスが両方のIPプロトコル（IPv4とIPv6）に対してプッシュされていない場合、対応するトラフィックが管理トンネルによって中断されないようにClient Bypass Protocol設定する必要があります。設定するには、「[ステップ4](#)」を参照してください。

ステップ4： に移動しAdvanced > AnyConnect Client ます。 に設定Client Bypass Protocol しEnable ます。 図に示すように、OK[Save]をクリックします。



ステップ 5 : 次の図に示すように、をクリックしてApply、設定をASAにプッシュします。



グループポリシーのCLI設定 :

```
<#root>
```

```
ip local pool
```

```
VPN_Pool
```

```
192.168.10.1-192.168.10.100 mask 255.255.255.0  
!
```

```
access-list
```

```
VPN-split
```

```
standard permit 172.16.0.0 255.255.0.0  
!
```

```
group-policy
```

```
AnyConnect_MGMT_Tunnel
```

```
internal  
group-policy
```

```
AnyConnect_MGMT_Tunnel
```

```
attributes  
vpn-tunnel-protocol
```

```
ikev2 ssl-client
```

```
split-tunnel-network-list value
```

```
VPN-split
```

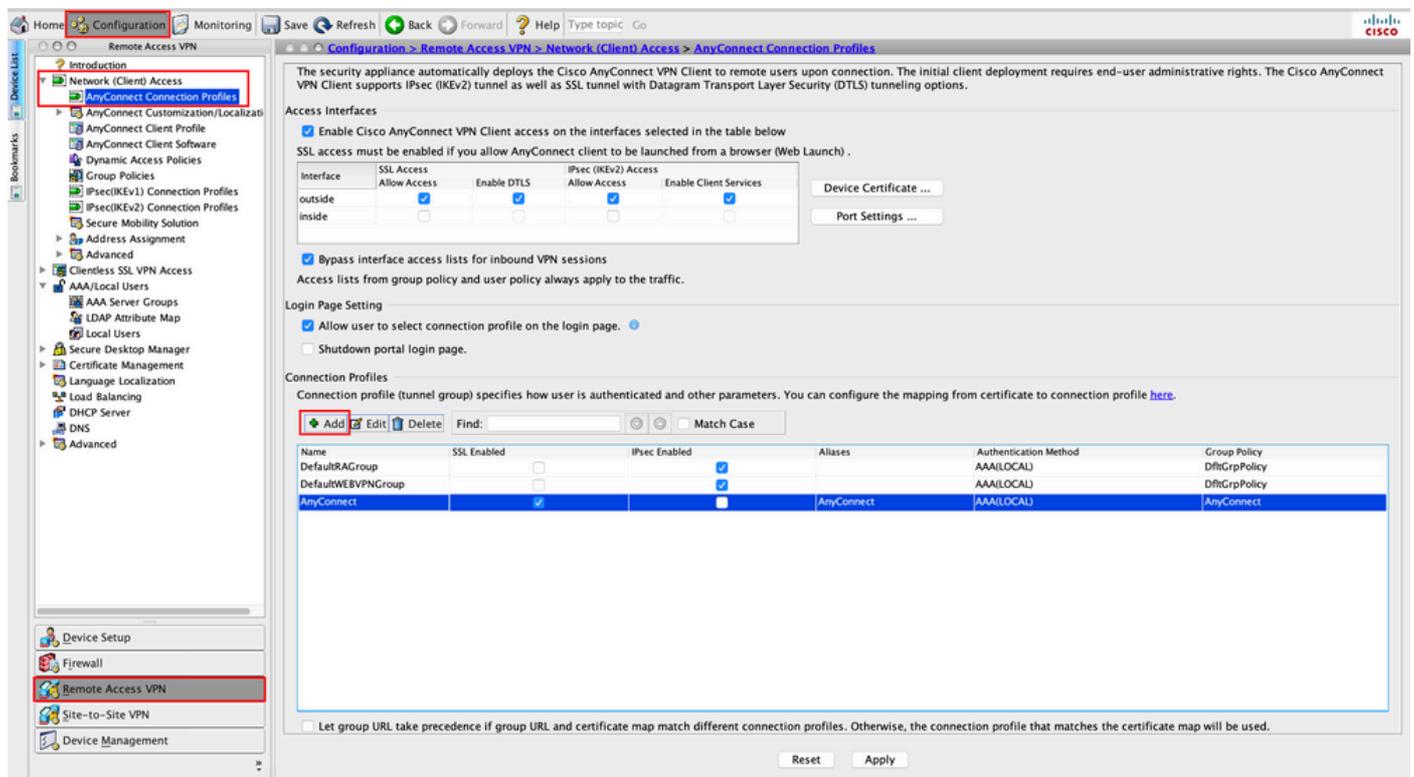
client-bypass-protocol enable

address-pools value

VPN_Pool

手順 6 : AnyConnect接続プロファイルを作成します。に移動し Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile ます。 をクリックします。 Add

 注 : 新しいAnyConnect接続プロファイルを作成することをお勧めします。このプロファイルは、AnyConnect管理トンネルのみで使用されます。



The screenshot shows the Cisco AnyConnect Configuration page. The left sidebar shows the navigation tree with 'AnyConnect Connection Profiles' highlighted. The main content area shows the 'Access Interfaces' section with a table for configuring access on 'outside' and 'inside' interfaces. Below that is the 'Connection Profiles' section with a table listing existing profiles and an 'Add' button highlighted in red.

| Interface | SSL Access | Enable DTLS | IPsec (IKEv2) Access | Enable Client Services |
|-----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| outside | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| inside | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Name | SSL Enabled | IPsec Enabled | Aliases | Authentication Method | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|------------|-----------------------|---------------|
| DefaultRAGroup | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | AAA(LLOCAL) | DfltGrpPolicy |
| DefaultWEBVPNGroup | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | AAA(LLOCAL) | DfltGrpPolicy |
| AnyConnect | <input checked="" type="checkbox"/> | <input type="checkbox"/> | AnyConnect | AAA(LLOCAL) | AnyConnect |

手順 7 : Connection ProfileにName を指定し、として設定Authentication MethodCertificate only します。ステツプ1で作成したとしてGroup Policy、 を選択します。

Add AnyConnect Connection Profile

Basic
 ▶ Advanced

Name: AnyConnect_MGMT_Tunnel

Aliases:

Authentication
 Method: Certificate only

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

SAML Identity Provider
 SAML Server : --- None --- Manage...

Client Address Assignment
 DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: Select...

Client IPv6 Address Pools: Select...

Default Group Policy
 Group Policy: AnyConnect_MGMT_Tunnel Manage...

(Following fields are linked to attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

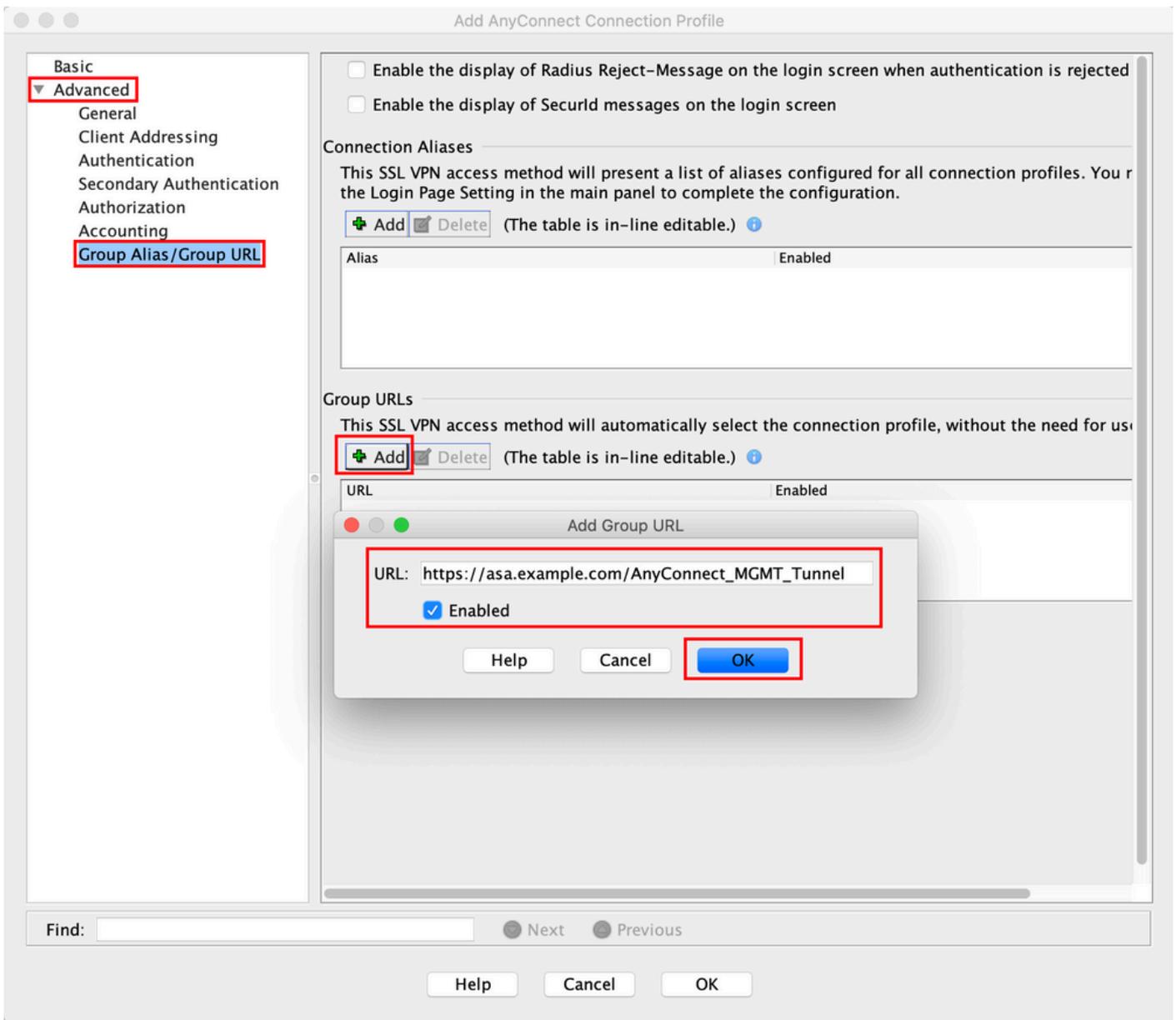
Find: Next Previous

Help Cancel OK

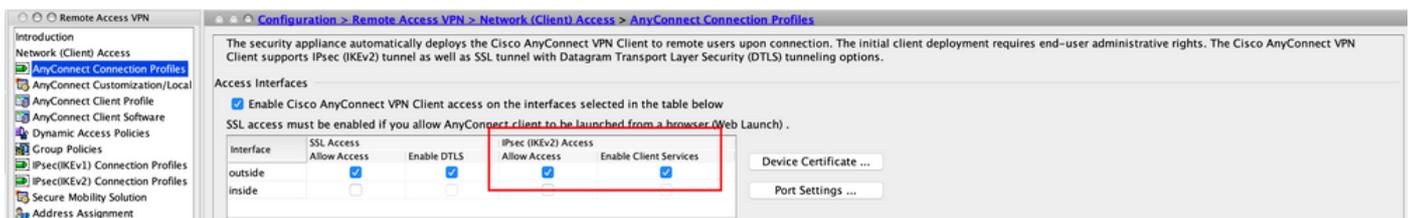
注：ローカルCAからのルート証明書がASAに存在することを確認します。証明書を追加または表示するには、Configuration > Remote Access VPN > Certificate Management > CA Certificates に移動します。

注：同じローカルCAによって発行されたID証明書が、マシン証明書ストア (Windowsの場合) またはシステムキーチェーン (macOSの場合) に存在することを確認してください。

ステップ 8： に移動し Advanced > Group Alias/Group URL ます。の Add 下をクリックし Group URLs、 を追加し URL ます。がオンになっていることを確認します Enabled。図に示すように、OK[Save]をクリックします。



IKEv2を使用する場合は、AnyConnectに使用するインターフェイスでIPsec (IKEv2) Access、が有効になっていることを確認します。



ステップ 9 : をクリックApplyして、設定をASAにプッシュします。

接続プロファイル (トンネルグループ) のCLI設定 :

```
<#root>
tunnel-group
AnyConnect_MGMT_Tunnel
  type remote-access
  tunnel-group
AnyConnect_MGMT_Tunnel
  general-attributes
  default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes
  authentication certificate
  group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

ステップ 10 : 信頼できる証明書がASAにインストールされ、AnyConnect接続に使用されるインターフェイスにバインドされていることを確認します。に移動してConfiguration > Remote Access VPN > Advanced > SSL Settings、この設定を追加または表示します。

 注 : 「[ASAへのID証明書のインストール](#)」を参照してください。

Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

The minimum SSL version for the security appliance to negotiate as a "server": DTLSV1 DTLSV1.2

The minimum SSL version for the security appliance to negotiate as a "client":

Diffie-Hellman group to be used with SSL:

ECDH group to be used with SSL:

Encryption

| Cipher Version | Cipher Security Level | Cipher Algorithms/ Custom String |
|----------------|-----------------------|--|
| Default | Medium | DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA DHE-RSA... |
| TLSV1 | Medium | DHE-RSA-AES256-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA... |
| TLSV1.1 | Medium | DHE-RSA-AES256-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA... |
| TLSV1.2 | Medium | ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D... |
| DTLSV1 | Medium | DHE-RSA-AES256-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA... |
| DTLSV1.2 | Medium | ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D... |

Server Name Indication (SNI)

| Domain | Certificate |
|--------|-------------|
| | |

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

| Interface | Primary Certificate | Load Balancing Certificate | Key-Type |
|------------|------------------------------------|----------------------------|--|
| inside | | | |
| management | | | |
| outside | ROOT-CA.hostname=ASA.example.co... | | Primary: RSA (2048 bits), Load Balancing: none |

Configuration changes saved successfully. admin 15 13/4/20 3:00:45 PM UTC

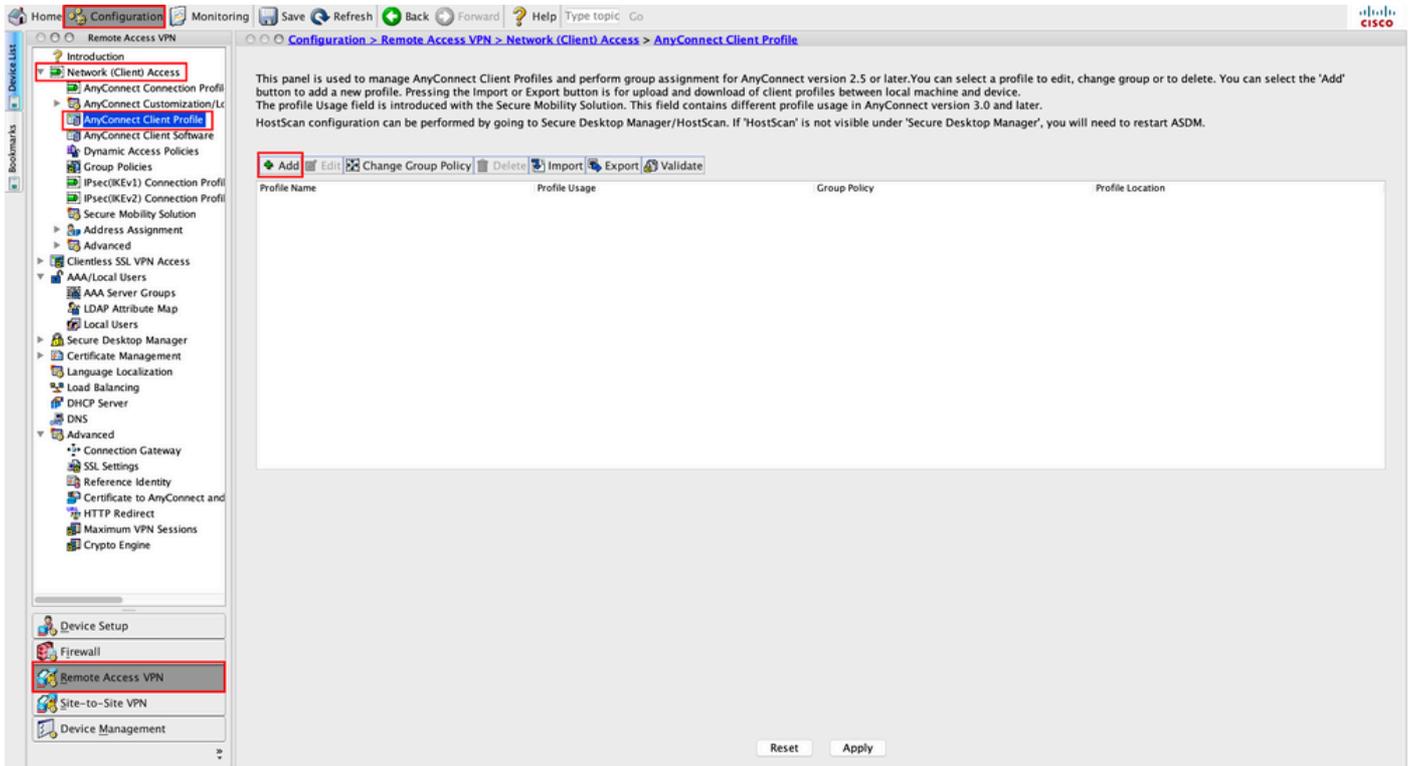
SSLトラストポイントのCLI設定：

```
<#root>
```

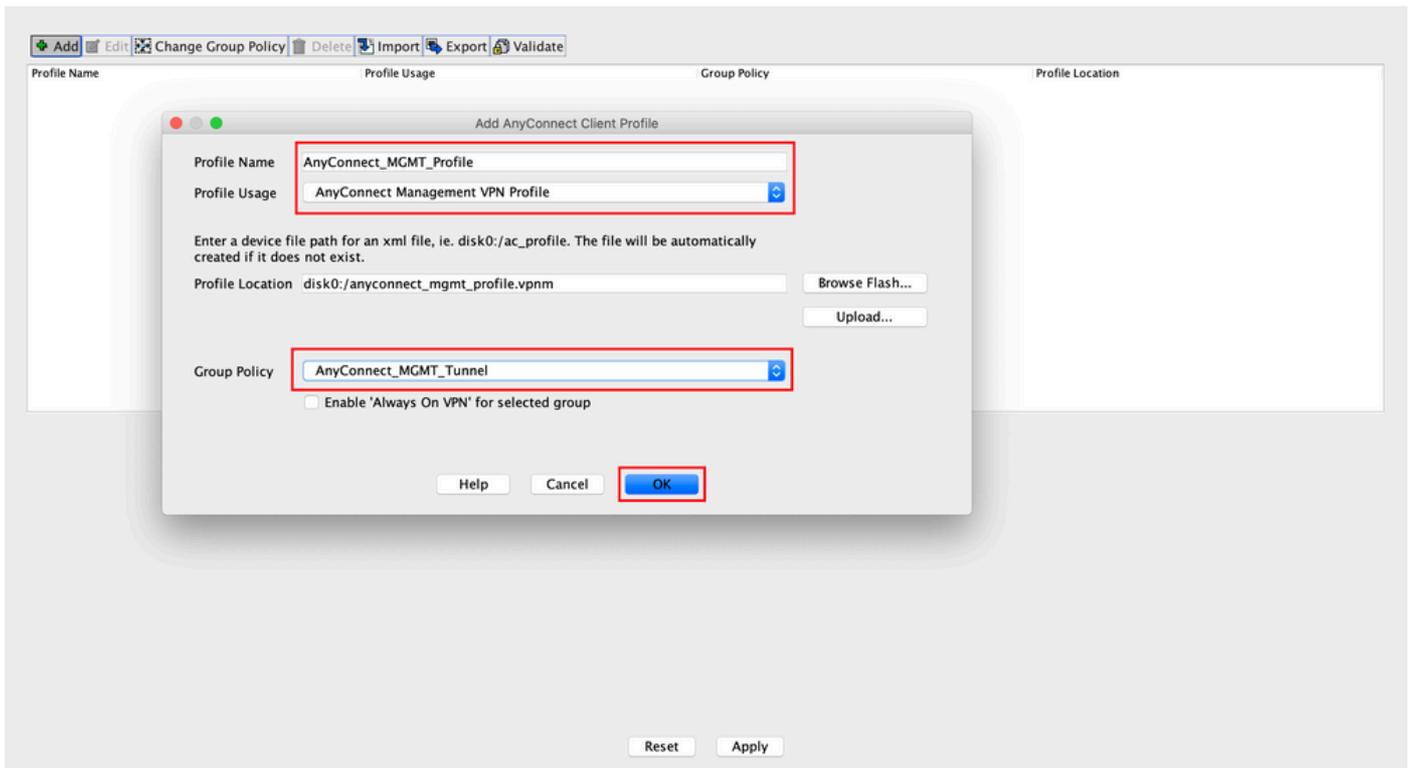
```
ssl trust-point ROOT-CA outside
```

AnyConnect管理VPNプロファイルの作成

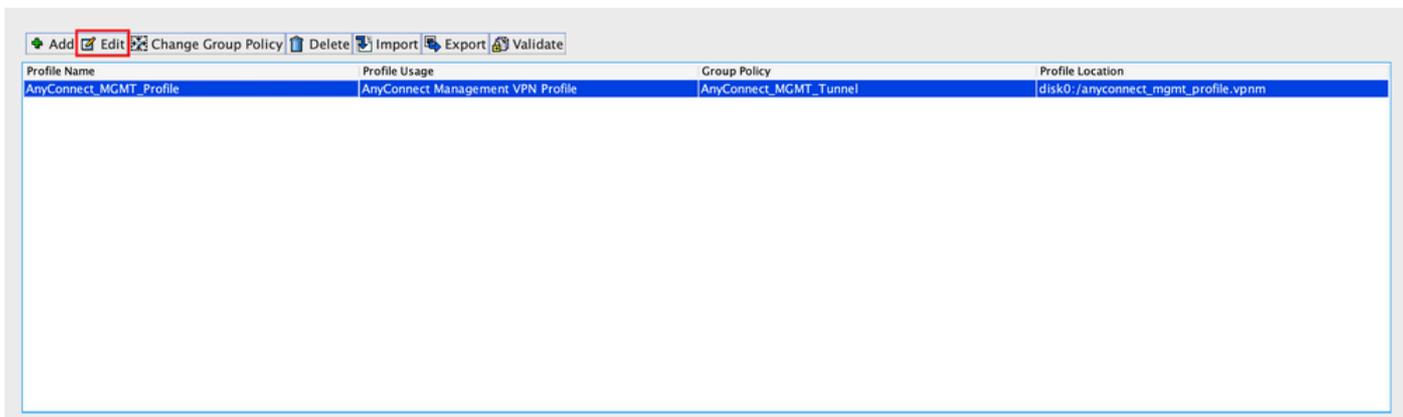
ステップ 1： AnyConnectクライアントプロファイルを作成します。に移動しConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profileます。図に示すように、をクリックしますAdd。



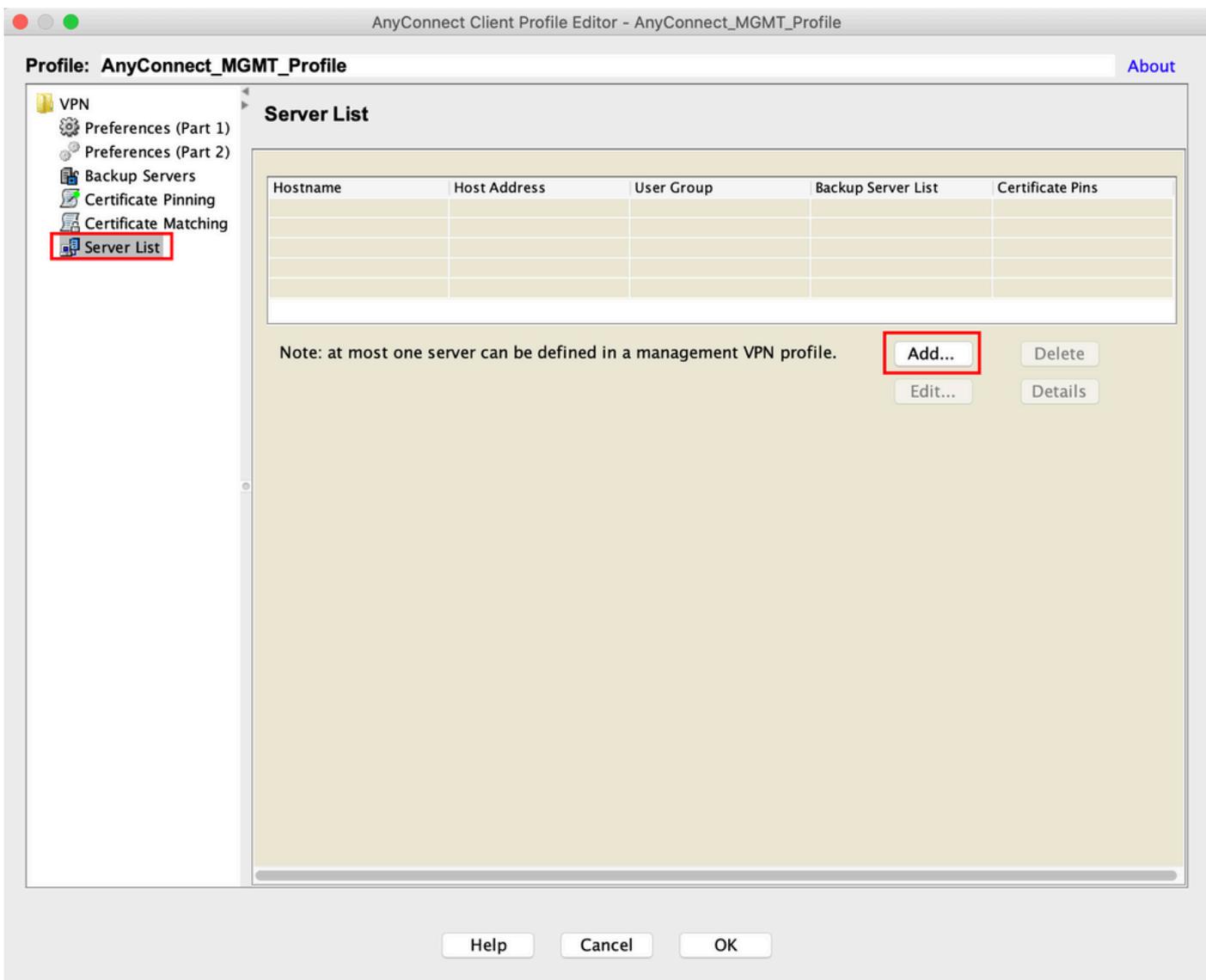
ステップ 2 : Profile Name を指定します。as を選択し Profile Usage AnyConnect Management VPN profile ます。 [ステップ 1](#) で作成した Group Policy を選択します。図に示すように、をクリックします OK。



ステップ 3 : 作成したプロファイルを選択し、図に示すように Edit をクリックします。



ステップ 4 : に移動しServer Listます。クリックAdd して、図に示すように、新しいサーバリストエントリを追加します。



ステップ 5 : Display Name を指定します。ASAのFQDN/IP address を追加します。をトンネルグループ名として指定しますUser Group。 はGroup URL、 FQDN andで自動的に設定されますUser Group。 をクリックします。OK

Server Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Addr... / User Group (required)

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

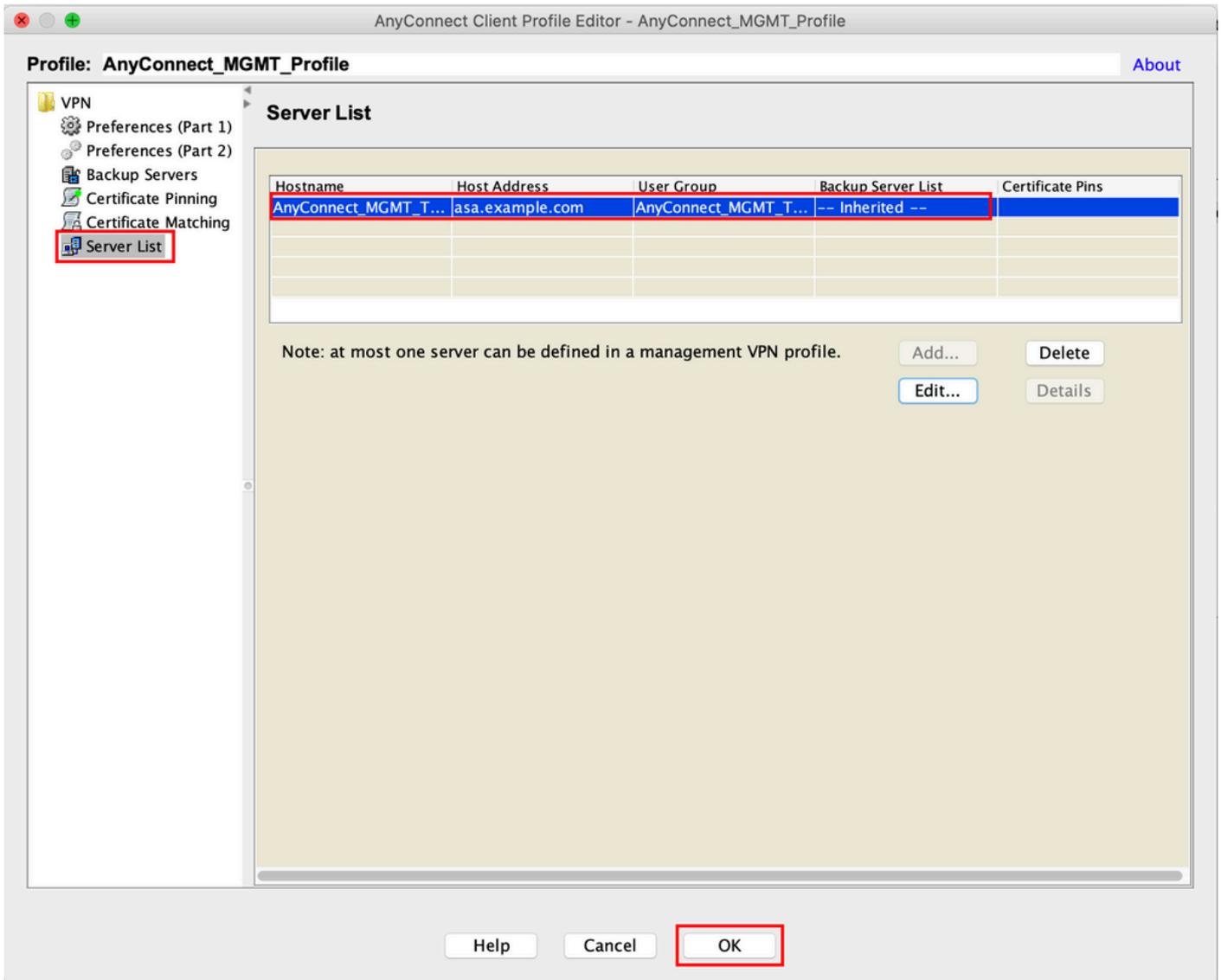
Backup Servers

| Host Address | |
|--|------------------------------------|
| <input type="text"/> | <input type="button" value="Add"/> |
| <input type="button" value="Move Up"/> | |
| <input type="button" value="Move Down"/> | |
| <input type="button" value="Delete"/> | |

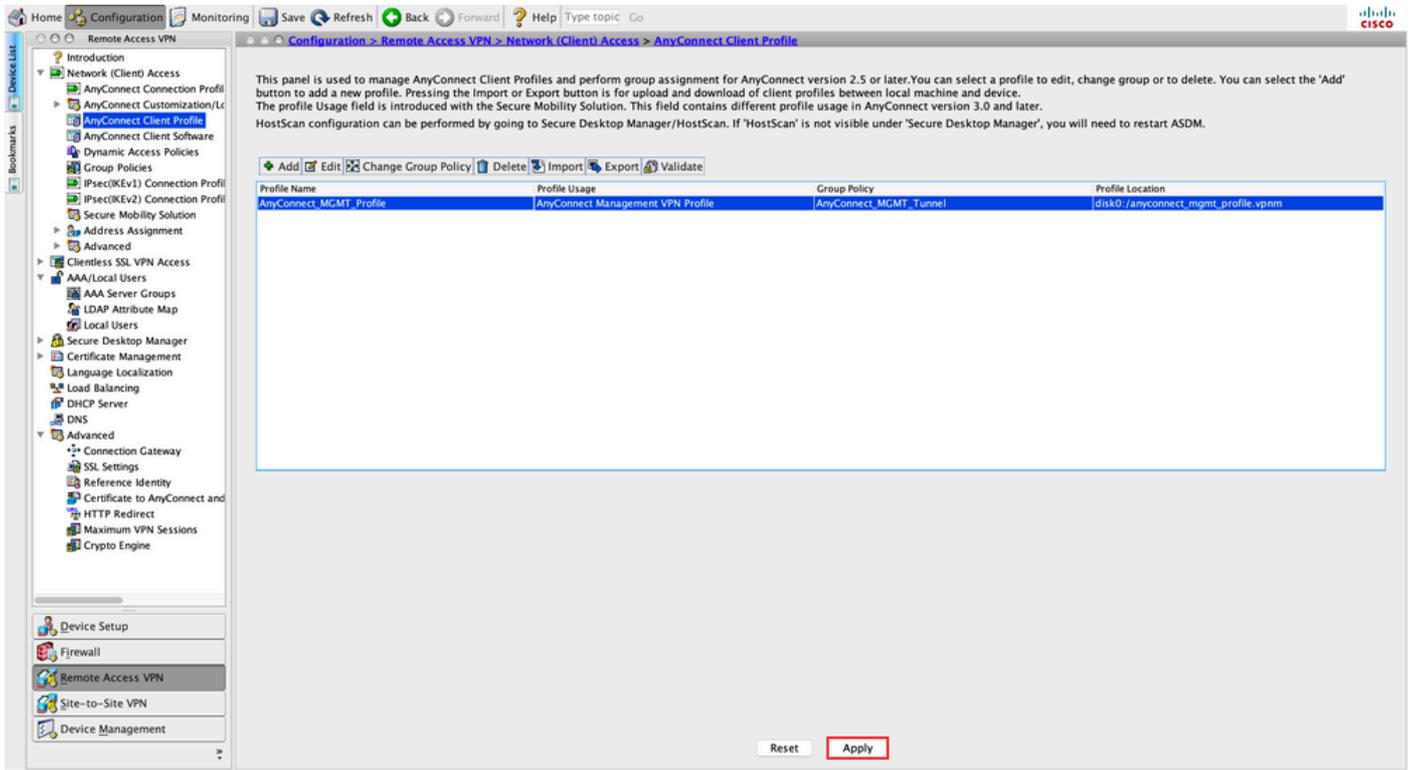
 注：FQDN/IPアドレス+ユーザグループは、[ステップ8](#)でAnyConnect接続プロファイルを設定するときに指定したグループURLと同じである必要があります。

 注：プロトコルとしてIKEv2を使用するAnyConnectは、ASAへの管理VPNを確立するためにも使用できます。[ステップ5](#)でPrimary Protocol、[が](#)に設定されていることを確認しますIPsec。

手順 6：図に示すように、クリックしてOK[保存]をクリックします。



手順 7 : 図Applyに示すように、をクリックして設定をASAにプッシュします。



AnyConnect管理VPNプロファイル追加後のCLI設定

```
<#root>
```

```
webvpn
```

```
enable outside
hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1

anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm

anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable
!
```

```
group-policy AnyConnect_MGMT_Tunnel internal
```

```
group-policy AnyConnect_MGMT_Tunnel attributes
```

```
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-network-list value VPN-Split
client-bypass-protocol enable
address-pools value VPN_Pool
```

```
webvpn
```

```
anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

AnyConnectクライアントマシンのAnyConnect管理VPNプロファイル :

<#root>

<?xml version="1.0" encoding="UTF-8"?>

<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"

<ClientInitialization>

<UseStartBeforeLogon UserControllable="false">>false</UseStartBeforeLogon>

true

<ShowPreConnectMessage>>false</ShowPreConnectMessage>

Machine

System

true

```
<ProxySettings>IgnoreProxy</ProxySettings>  
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>  
<AuthenticationTimeout>30</AuthenticationTimeout>
```

--- Output Omitted ---

```
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>  
<AllowManualHostInput>false</AllowManualHostInput>  
</ClientInitialization>
```

AnyConnect_MGMT_Tunnel

asa.example.com

</AnyConnectProfile>

 注：Trusted Network Detection(TND)がユーザのAnyConnect VPNプロファイルで使用されている場合は、一貫したユーザエクスペリエンスを得るために管理VPNプロファイルで同じ設定を照合することをお勧めします。管理VPNトンネルは、ユーザVPNトンネルプロファイルに適用されたTND設定に基づいてトリガーされます。また、管理VPNプロファイルのTND Connectアクション（管理VPNトンネルがアクティブの場合にのみ適用）は、常にユーザVPNトンネルに適用され、管理VPNトンネルがエンドユーザに対して透過的であることが保証されます。

 注：エンドユーザPCでは、管理VPNプロファイルでTND設定が有効になっており、ユーザVPNプロファイルがない場合、ユーザVPNプロファイルがない代わりに、TNDのデフォルト設定（ACクライアントアプリケーションのデフォルト設定で無効）が考慮されます。この不一致により、予期しない動作や未定義の動作が発生する可能性があります。デフォルトでは、TND設定はデフォルト設定で無効になっています。AnyConnect Clientアプリケーションのデフォルト設定ハードコード設定を克服するには、エンドユーザPCに2つのVPNプロファイル（ユーザVPNプロファイルとAC管理VPNプロファイル）が必要で、両方に同じTND設定が必要です。管理VPNトンネルの接続および切断のロジックは、管理VPNトンネルを確立するために、ACエージェントはユーザVPNプロファイルTND設定を使用し、管理VPNトンネルの切断には、管理VPNプロファイルTND設定を確認することです。

AnyConnect管理VPNプロファイルの展開方法

- VPNゲートウェイからAnyConnect管理VPNプロファイルをダウンロードするには、ASA接続プロファイルを使用してユーザVPN接続が正常に完了します。
-

 注：管理VPNトンネルに使用されるプロトコルがIKEv2の場合、最初の接続は（ASAからAnyConnect管理VPNプロファイルをダウンロードするために）SSLを介して確立する必要があります。

- AnyConnect管理VPNプロファイルは、GPOプッシュまたは手動インストール(プロファイル

の名前が VpnMgmtTunProfile.xml であることを確認)によってクライアントマシンに手動でアップロードできます。

プロファイルを追加する必要があるフォルダの場所：

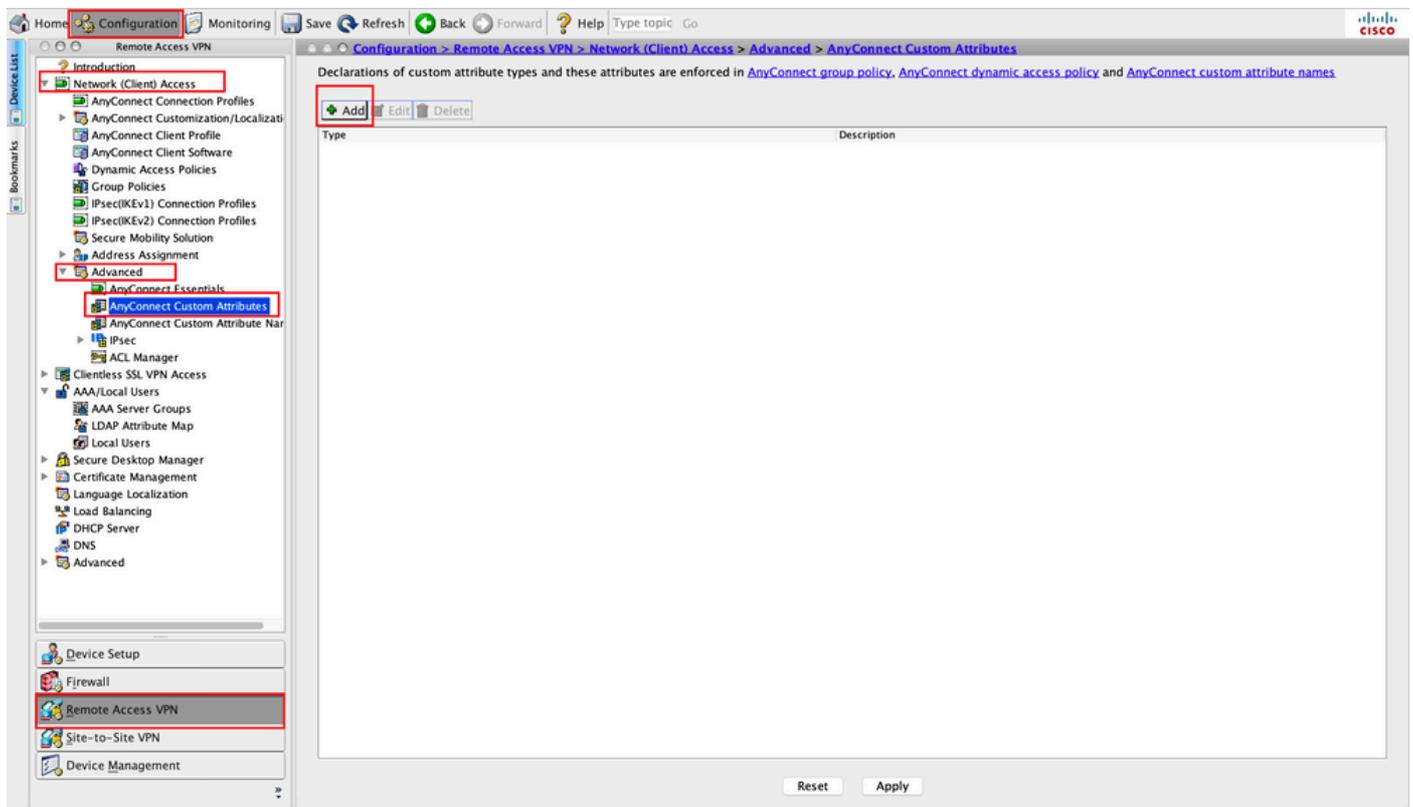
Windows： C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun

macOS： /opt/cisco/anyconnect/profile/mgmttun/

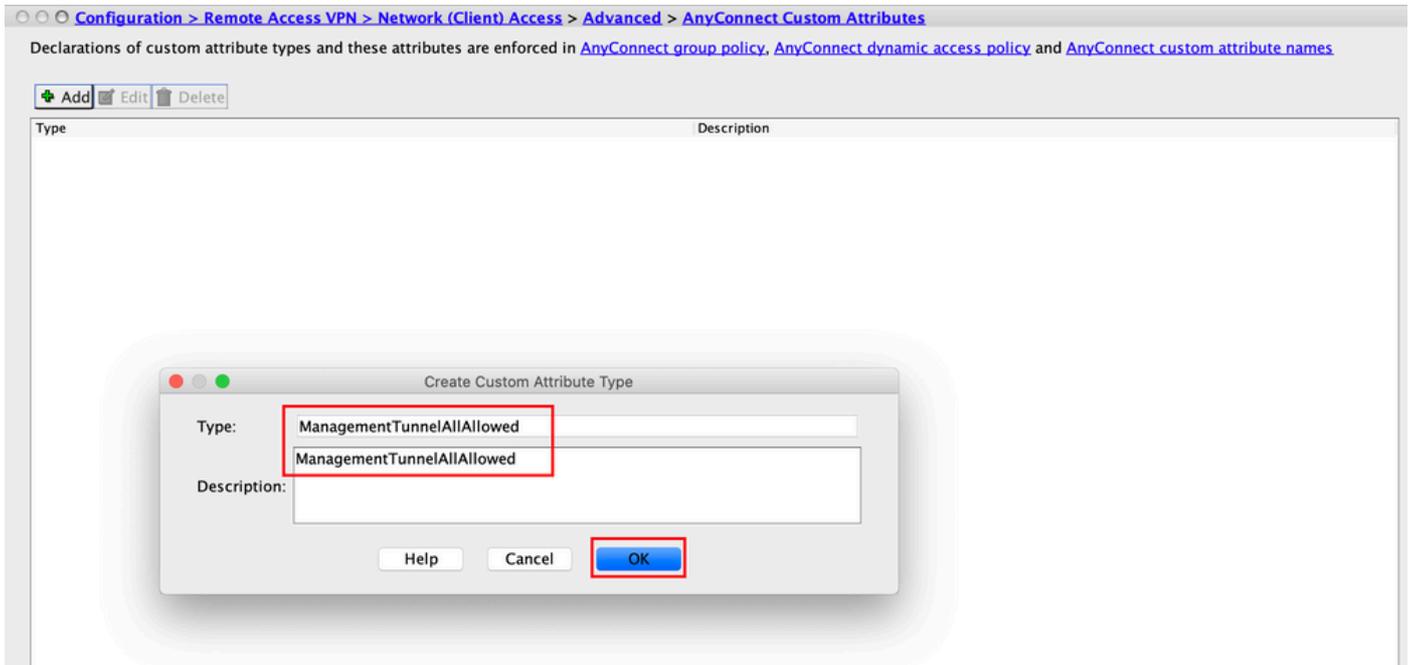
(オプション) Tunnel-All設定をサポートするカスタム属性を設定します

管理VPNトンネルでは、ユーザが開始するネットワーク通信に影響を与えないように、デフォルトでトンネリング設定を含むスプリットが必要です。これは、管理トンネル接続で使用されるグループポリシーでカスタム属性を設定する場合に上書きできます。

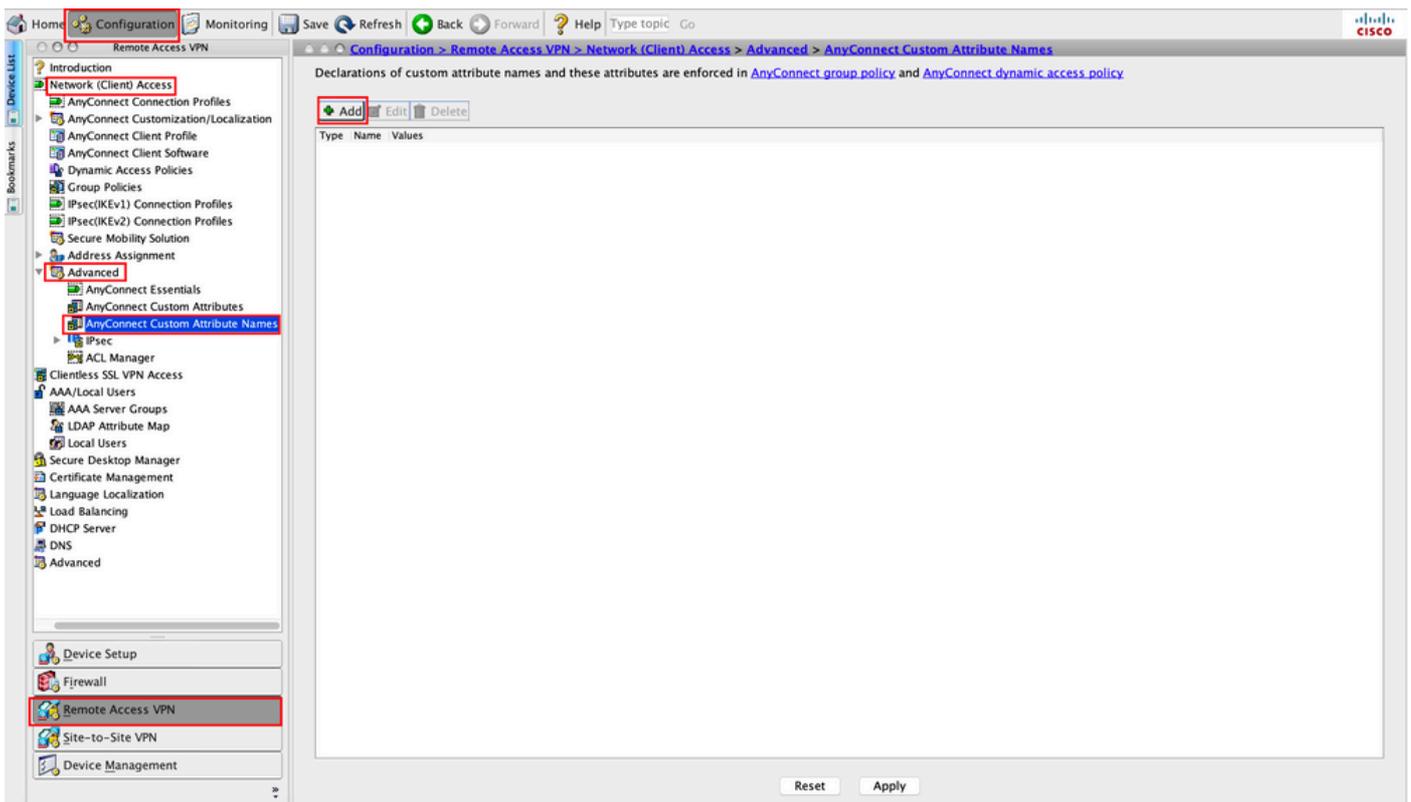
ステップ 1： に移動し Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes ます。 図に示すように、 をクリックします。



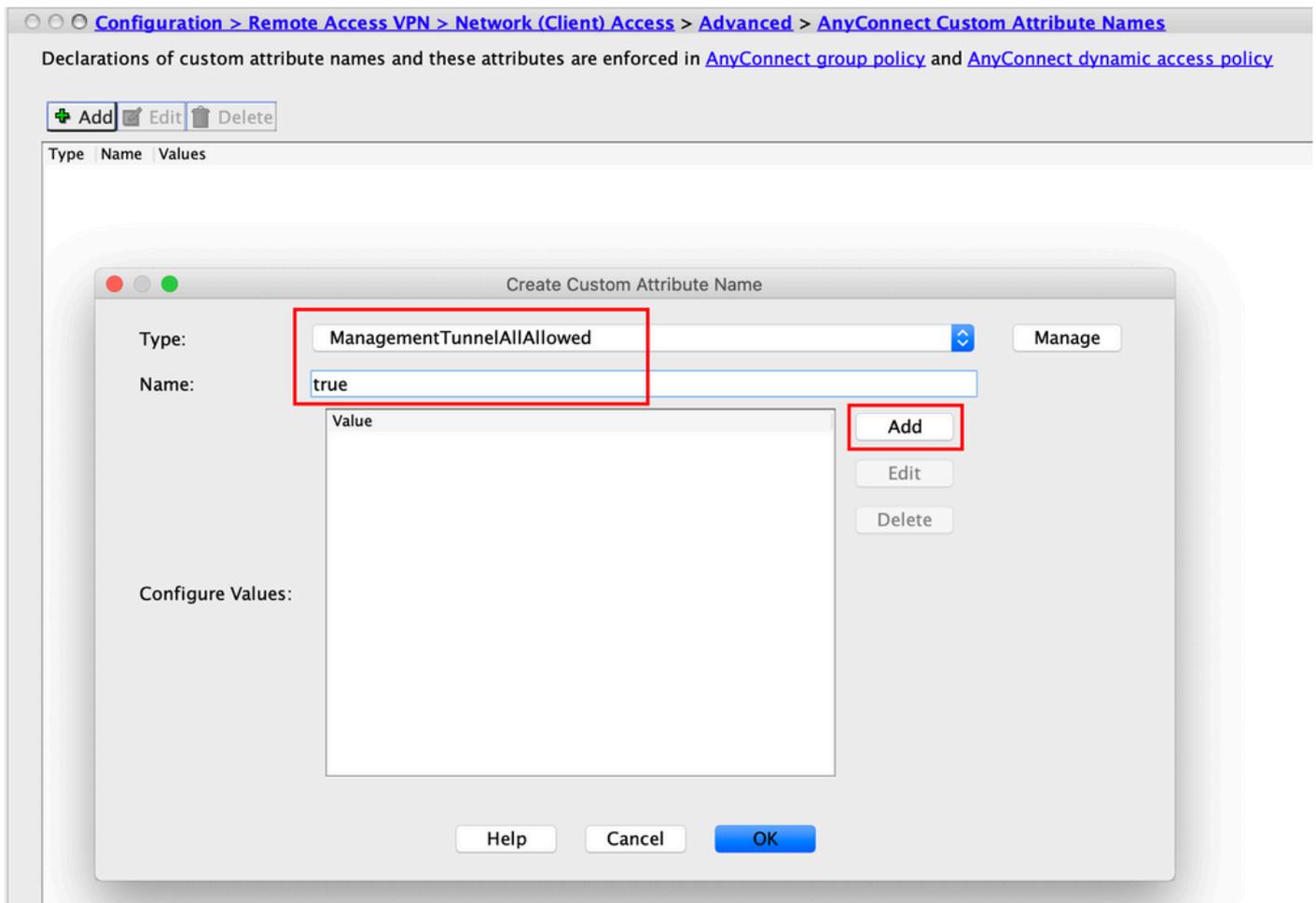
ステップ2.カスタム属性タイプを ManagementTunnelAllAllowed に設定 し、 を指定 Description します。 図に示すように、 をクリックします OK。



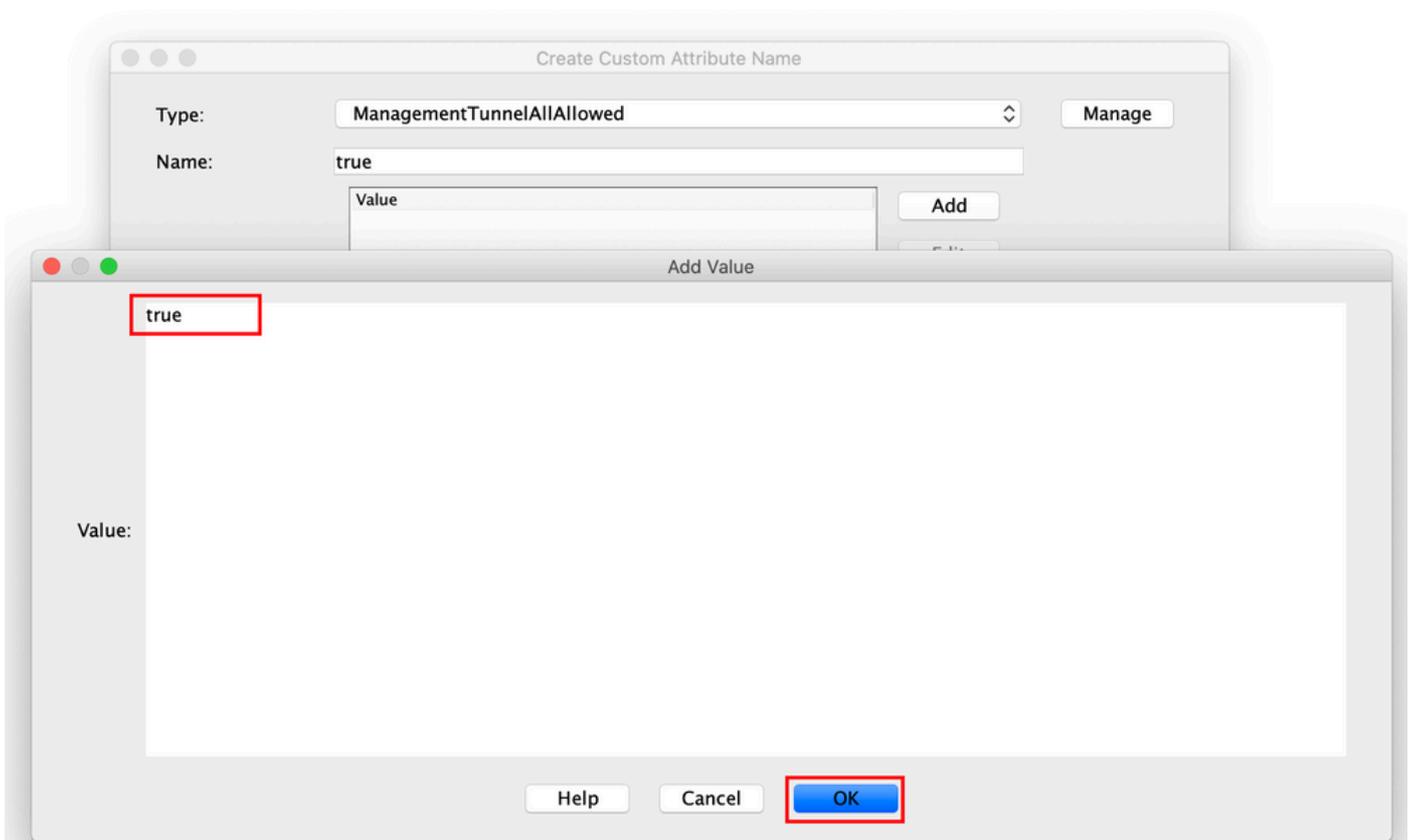
ステップ 3 : に移動し Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names ます。図に示すように、 をクリックします。



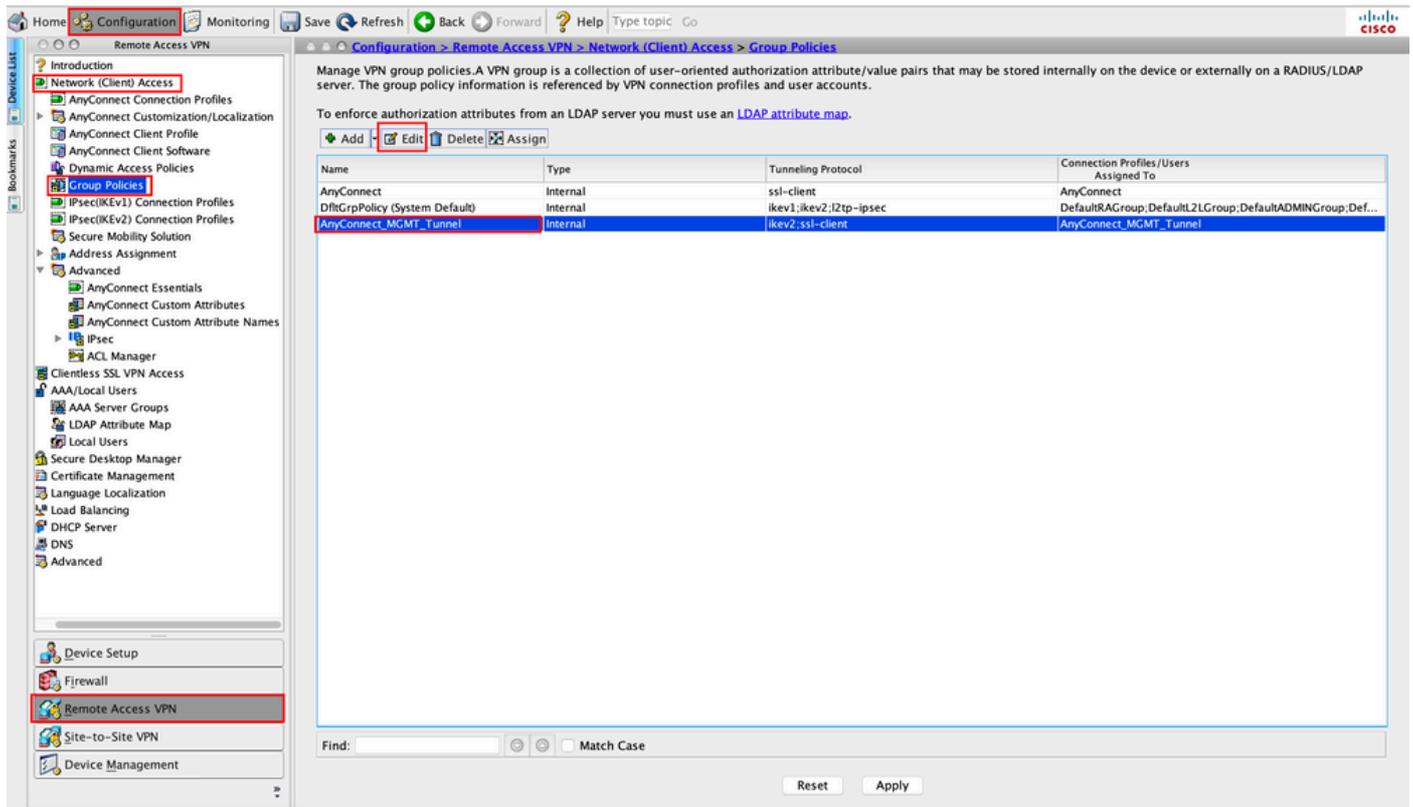
ステップ 4 : タイプとして ManagementTunnelAllAllowed を選択します。名前を に設定し true ます。クリック Add して、図に示すようにカスタム属性値を指定します。



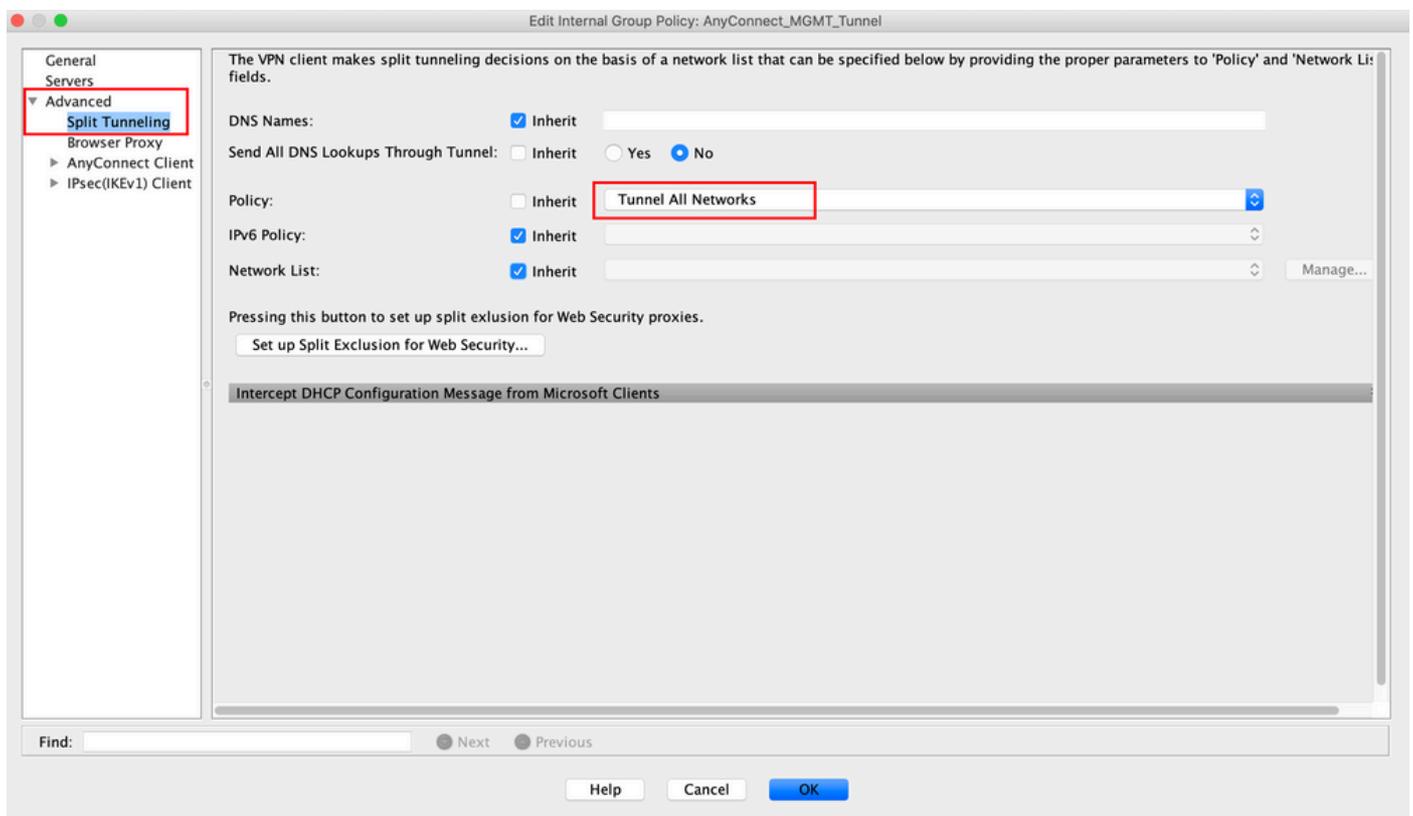
ステップ 5 : 値をに設定しtrueます。図に示すように、をクリックしますOK。



手順 6 : に移動し Configuration > Remote Access VPN > Network (Client) Access > Group Policies ます。グループポリシーを選択します。図に示すように、を Edit クリックします。

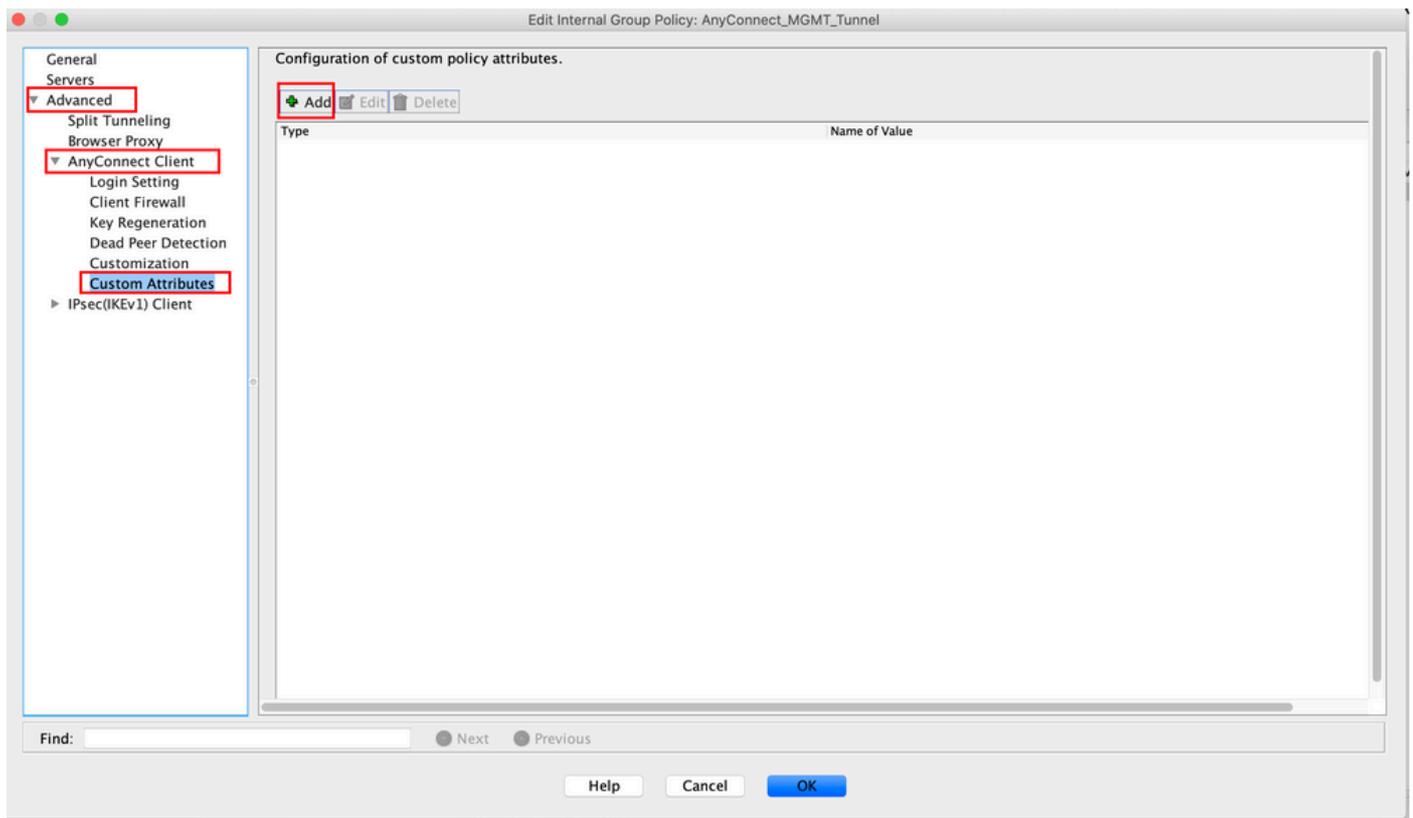


手順 7 : 次の図に示すように、に移動し Advanced > Split Tunneling ます。ポリシーを に設定し Tunnel All Networks ます。

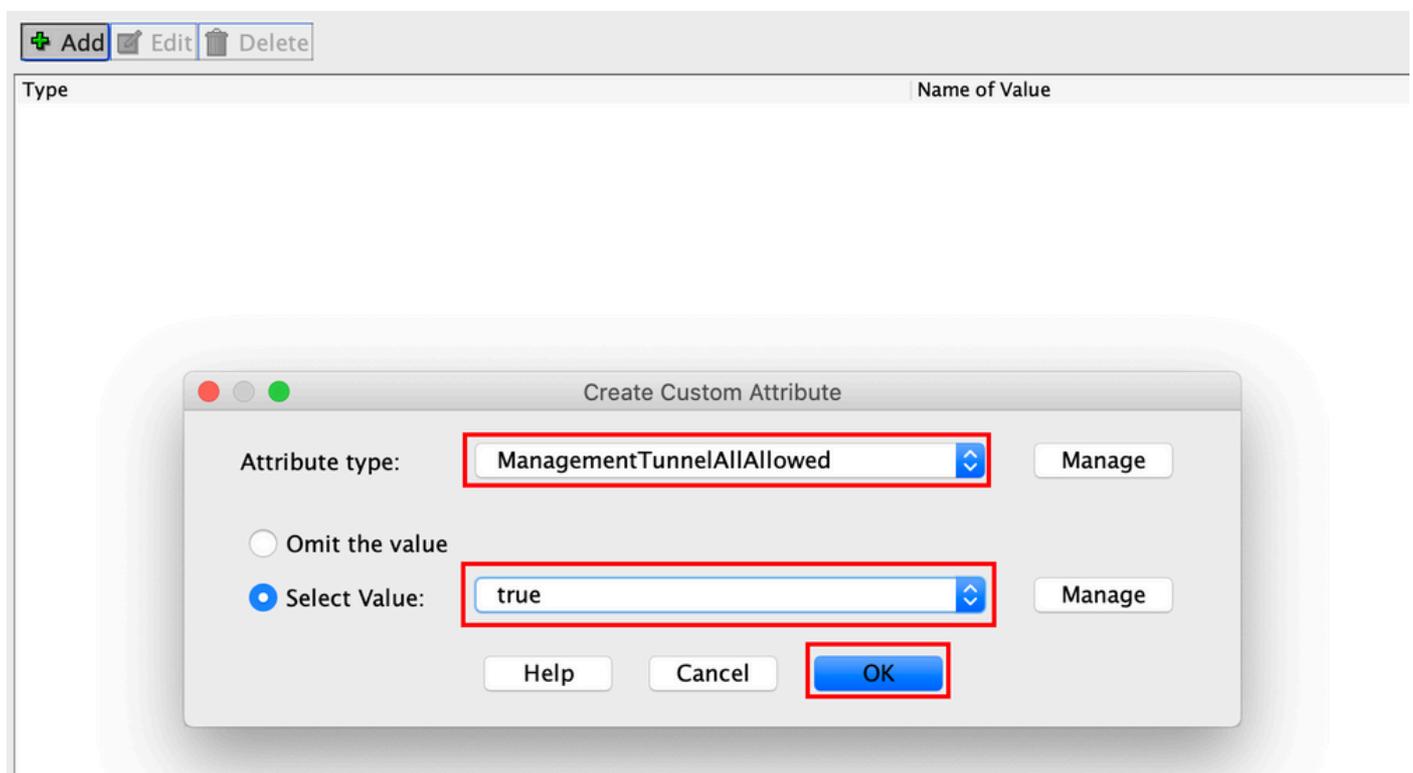


ステップ 8 : に移動し Advanced > Anyconnect Client > Custom Attributes ます。図に示すように、をクリックし

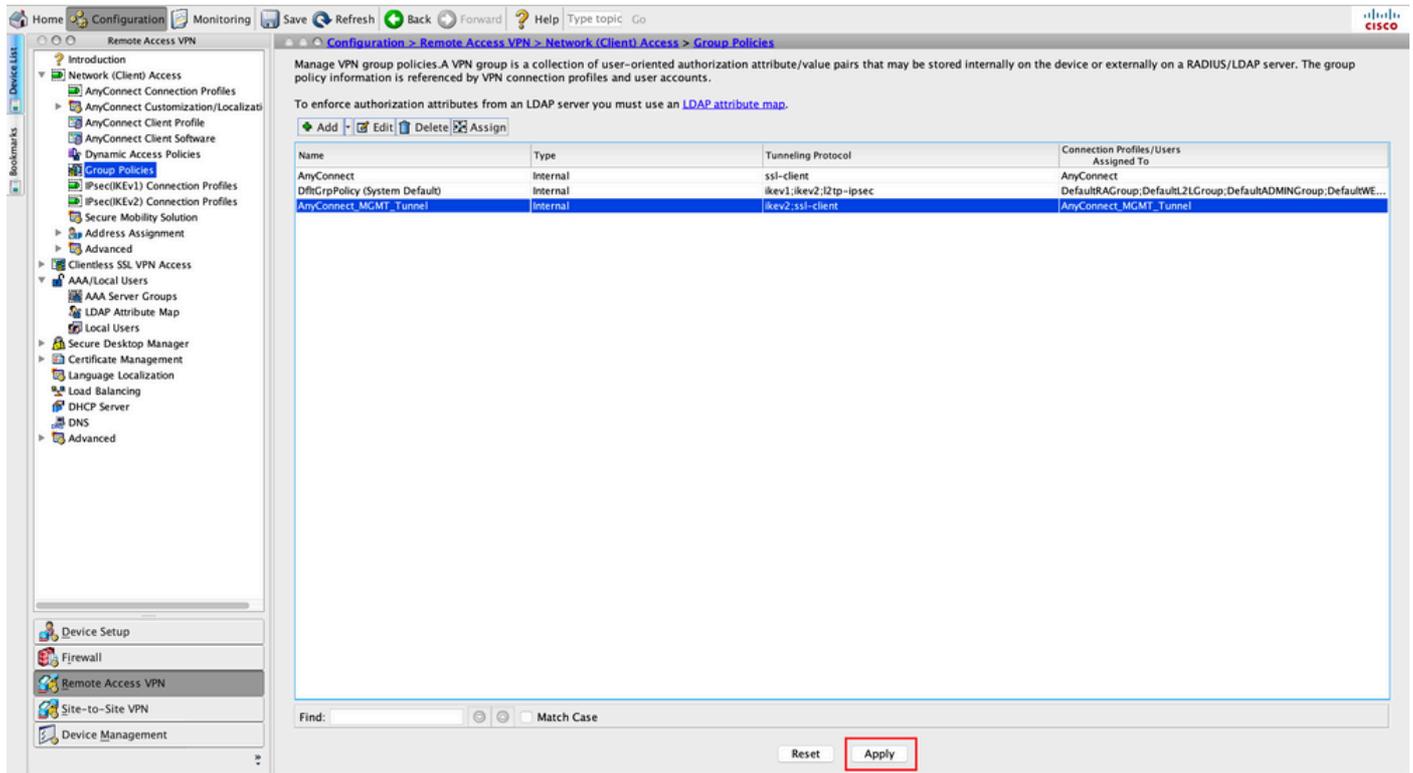
まず Add。



ステップ 9： 属性タイプとして ManagementTunnelAllAllowed を選択し、値として true を選択します。図に示すように OK、をクリックします。



ステップ 10： クリックすると Apply、図に示すように、設定が ASA にプッシュされます。



カスタム属性を追加した後のCLI設定ManagementTunnelAllAllowed:

```
<#root>
```

```
webvpn
```

```
enable outside
```

```
anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
```

```
hsts
```

```
enable
```

```
max-age 31536000
```

```
include-sub-domains
```

```
no preload
```

```
no anyconnect-essentials
```

```
anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
```

```
anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
```

```
anyconnect enable
```

```
tunnel-group-list enable
```

```
cache
```

```
disable
```

```
error-recovery disable
```

```
!
```

```
anyconnect-custom-data ManagementTunnelAllAllowed true true
```

```
!
```

```
group-policy AnyConnect_MGMT_Tunnel internal
```

```
group-policy AnyConnect_MGMT_Tunnel attributes
```

```
vpn-tunnel-protocol ikev2 ssl-client
```

```
split-tunnel-policy tunnelall

client-bypass-protocol enable
address-pools value VPN_Pool

anyconnect-custom ManagementTunnelAllAllowed value true

webvpn

anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

確認

コマンド `show vpn-sessiondb detail anyconnect` を使用して、ASA CLIの管理VPNトンネル接続を確認します。

。

<#root>

ASA#

```
show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username :

vpnuser

Index : 10

Assigned IP :

192.168.10.1

Public IP : 10.65.84.175

Protocol :

AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384

Bytes Tx : 17238 Bytes Rx : 1988

Pkts Tx : 12 Pkts Rx : 13

Pkts Tx Drop : 0 Pkts Rx Drop : 0

Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel

Login Time : 01:23:55 UTC Tue Apr 14 2020

Duration : 0h:11m:36s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : c0a801010000a0005e9510ab

Security Grp : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

--- Output Omitted ---

DTLS-Tunnel:

Tunnel ID : 10.3
Assigned IP : 192.168.10.1 Public IP : 10.65.84.175
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 57053
UDP Dst Port : 443

Auth Mode : Certificate

Idle Time Out: 30 Minutes Idle TO Left : 18 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03036
Bytes Tx : 17238 Bytes Rx : 1988
Pkts Tx : 12 Pkts Rx : 13
Pkts Tx Drop : 0 Pkts Rx Drop : 0

ASDMで管理VPNトンネル接続を確認します。

[モニタリング (Monitoring)] > [VPN] > [VPN 統計情報 (VPN Statistics)] > [セッション (Sessions)] の順に移動します。クライアントセッションを表示するには、AnyConnect Clientでフィルタリングします。

The screenshot shows the ASDM interface for monitoring VPN sessions. The breadcrumb path is Monitoring > VPN > VPN Statistics > Sessions. The left sidebar shows the navigation tree with 'VPN Statistics' and 'Sessions' highlighted. The main content area displays a summary table and a detailed table of sessions. The detailed table has a red box around the first row, which represents an active session for 'vpnuser'.

| Type | Active | Cumulative | Peak Concurrent | Inactive | |
|-------------------|--------|------------|-----------------|----------|---|
| AnyConnect Client | 1 | 1 | 19 | 1 | 0 |
| SSL/TLS/DTLS | 1 | 1 | 19 | 1 | 0 |

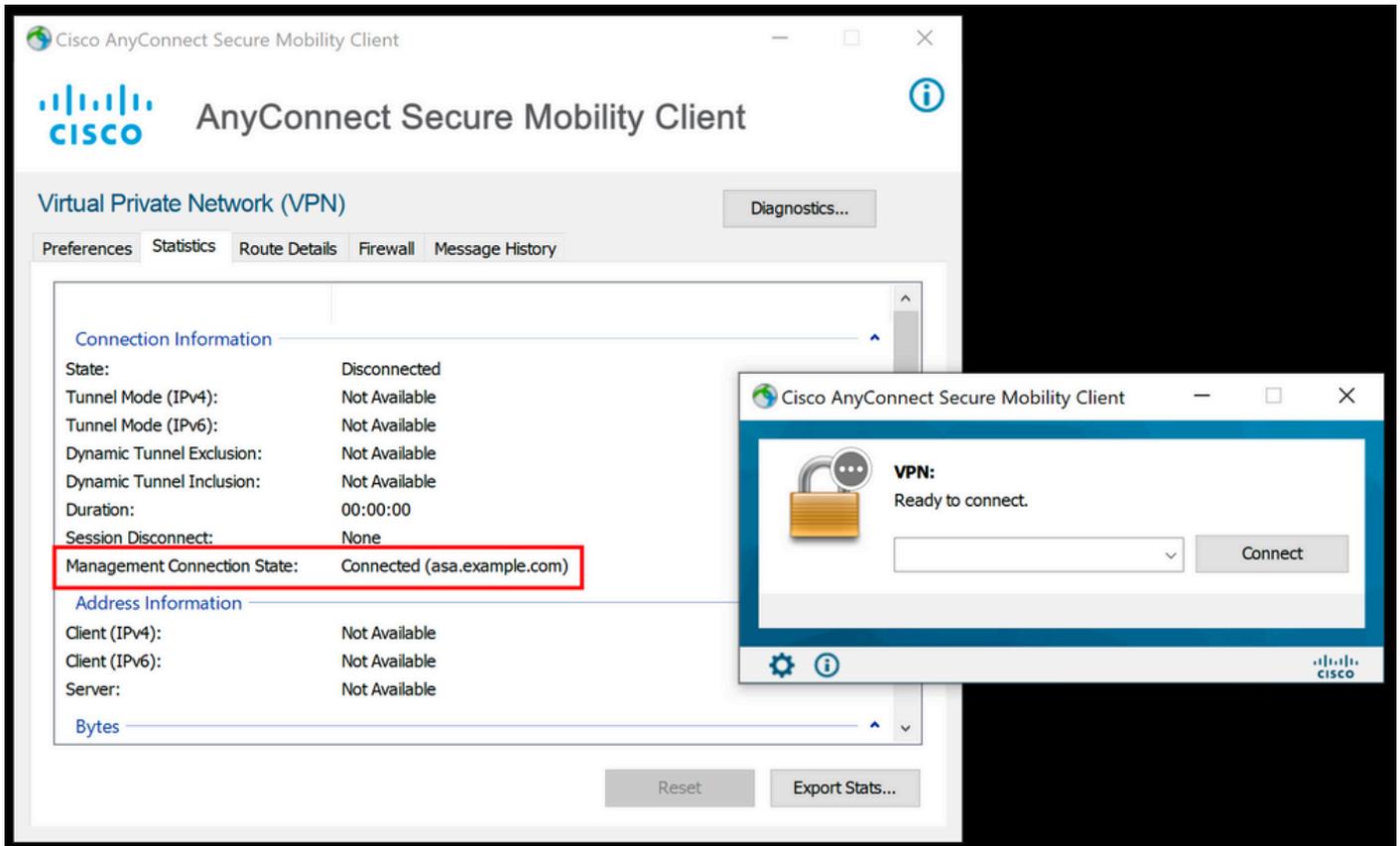
Filter By: AnyConnect Client -- All Sessions -- Filter

| Username | Group Policy | Assigned IP Address | Protocol | Login Time | Bytes Tx | Inactivity | Audit | Details |
|----------|--------------------|---------------------|----------------------------|-----------------|----------|------------|----------|---------|
| | Connection Profile | Public IP Address | Encryption | Duration | Bytes Rx | | | |
| vpnuser | AnyConnect_MGMT... | 192.168.10.1 | AnyConnect-Parent | 10:52:25 UTC .. | 34688 | 0h:00m:00s | c0a80... | Logout |
| | AnyConnect_MGMT... | 10.65.84.175 | AnyConnect-Parent: (1)none | 0h:01m:31s | 33954 | | | Ping |

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessio... Logout Sessions

クライアントマシンでの管理VPNトンネル接続の確認:



トラブルシューティング

新しいUI統計行（管理接続状態）は、管理トンネルの接続問題のトラブルシューティングに使用できません。一般的に見られるエラー状態を次に示します。

切断（無効）:

- この機能は無効になっています。
- 管理VPNプロファイルが、ユーザトンネル接続（ユーザトンネルグループポリシーに管理VPNプロファイルを追加する必要がある）を介して、またはプロファイルの手動アップロードによってアウトオブバンドで、クライアントに展開されていることを確認します。
- 管理VPNプロファイルが、トンネルグループを含む単一のホストエントリで設定されていることを確認します。

切断（信頼できるネットワーク）:

- TNDが信頼できるネットワークを検出したため、管理トンネルが確立されません。

切断（ユーザトンネルがアクティブ）:

- ユーザVPNトンネルが現在アクティブである。

切断（プロセスの起動に失敗）:

- 管理トンネル接続の試行中にプロセスの起動エラーが発生しました。

切断 (接続に失敗しました):

- 管理トンネルの確立時に接続エラーが発生しました。
- 証明書認証がトンネルグループに設定されていること、グループポリシーにバナーが存在しないこと、およびサーバ証明書が信頼されていることを確認します。

切断 (無効なVPN構成):

- 無効なスプリットトンネリング構成またはクライアントバイパスプロトコル構成をVPNサーバーから受信しました。
- 管理トンネルグループポリシーの設定をドキュメントと照合します。

切断 (ソフトウェアの更新が保留中):

- AnyConnectソフトウェアのアップデートは現在保留中です。

切断されました:

- 管理トンネルを確立しようとしているか、または他の理由で確立できません。

さらにトラブルシューティングを行うために[DART](#)を[収集](#)します。

関連情報

- [管理VPNトンネルの設定](#)
- [管理VPNトンネルのトラブルシューティング](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。