在 ASA 上配置 AnyConnect 管理 VPN 隧道

目录

简介

本文档介绍如何将ASA配置为VPN网关通过管理VPN隧道接受来自Cisco AnyConnect安全移动客户端的连接。

先决条件

要求

Cisco 建议您了解以下主题：

- 通过自适应安全设备管理器(ASDM)配置VPN
- 基本自适应安全设备(ASA)CLI配置
- X509证书

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ASA软件版本9.12(3)9
- 思科ASDM软件版本7.12.2
- Windows 10与Cisco AnyConnect安全移动客户端4.8.03036版

注意：下载AnyConnect VPN Web部署软件包(anyconnect-win*.pkg or anyconnect-macos*.pkg)下载思科软件(仅限注册客户)。将AnyConnect VPN客户端复制到要下载到远程用户计算机的ASA的闪存中，以与ASA建立SSL VPN连接。有关详细信息，请参阅ASA配置指南的安装

AnyConnect客户端部分。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

管理VPN隧道可确保在客户端系统启动时连接到企业网络，而不仅仅是在最终用户建立VPN连接时。您可以在办公室外终端（尤其是用户通过VPN不经常连接到办公室网络的设备）上执行补丁管理。需要企业网络连接的终端OS登录脚本也受益于此功能。

AnyConnect Management Tunnel允许管理员在用户登录之前将AnyConnect连接起来，而无需用户干预。AnyConnect管理隧道可与受信任网络检测结合使用，因此仅当终端位于外部并与用户发起的VPN断开连接时才会触发。AnyConnect管理隧道对最终用户是透明的，并在用户启动VPN时自动断开。

操作系统/应用	**最低版本要求**
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect版本	4.7.00136
macOS AnyConnect版本	4.7.01076
Linux	不支持

管理隧道的运行

AnyConnect VPN代理服务在系统启动时自动启动。它检测到管理隧道功能已启用（通过管理VPN配置文件），因此它会启动管理客户端应用以启动管理隧道连接。管理客户端应用使用管理VPN配置文件中的主机条目发起连接。然后VPN隧道会照常建立，但有一个例外：管理隧道连接期间不会执行软件更新，因为管理隧道对用户是透明的。

用户通过AnyConnect UI启动VPN隧道，这将触发管理隧道终端。管理隧道终止后，用户隧道的建立会照常继续。

用户断开VPN隧道，从而触发管理隧道的自动重建。

限制

- 不支持用户交互
- 仅支持通过计算机证书存储区(Windows)进行的基于证书的身份验证
- 实施严格的服务器证书检查
- 不支持专用代理
- 不支持公共代理（在未从浏览器检索本地代理设置的平台上支持ProxyNative值）
- 不支持AnyConnect自定义脚本

注意：有关详细信息，请参阅关于管理VPN隧道。

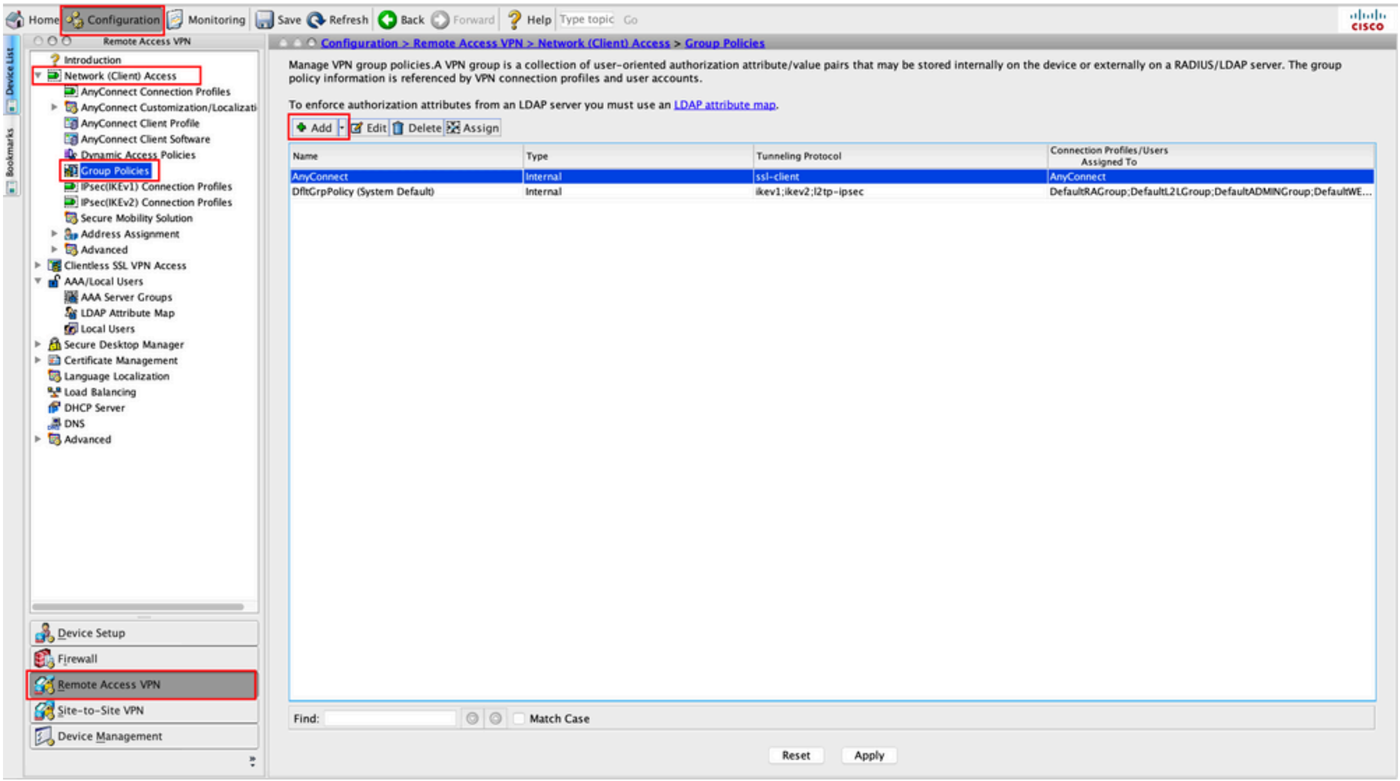
配置

本节介绍如何将Cisco ASA配置为VPN网关，以通过管理VPN隧道接受来自AnyConnect客户端的连接。

通过ASDM/CLI在ASA上进行配置

步骤1:创建AnyConnect组策略。导航至 Configuration > Remote Access VPN > Network (Client) Access > Group Policies.点击 Add.

注意：建议创建仅用于AnyConnect管理隧道的新AnyConnect组策略。



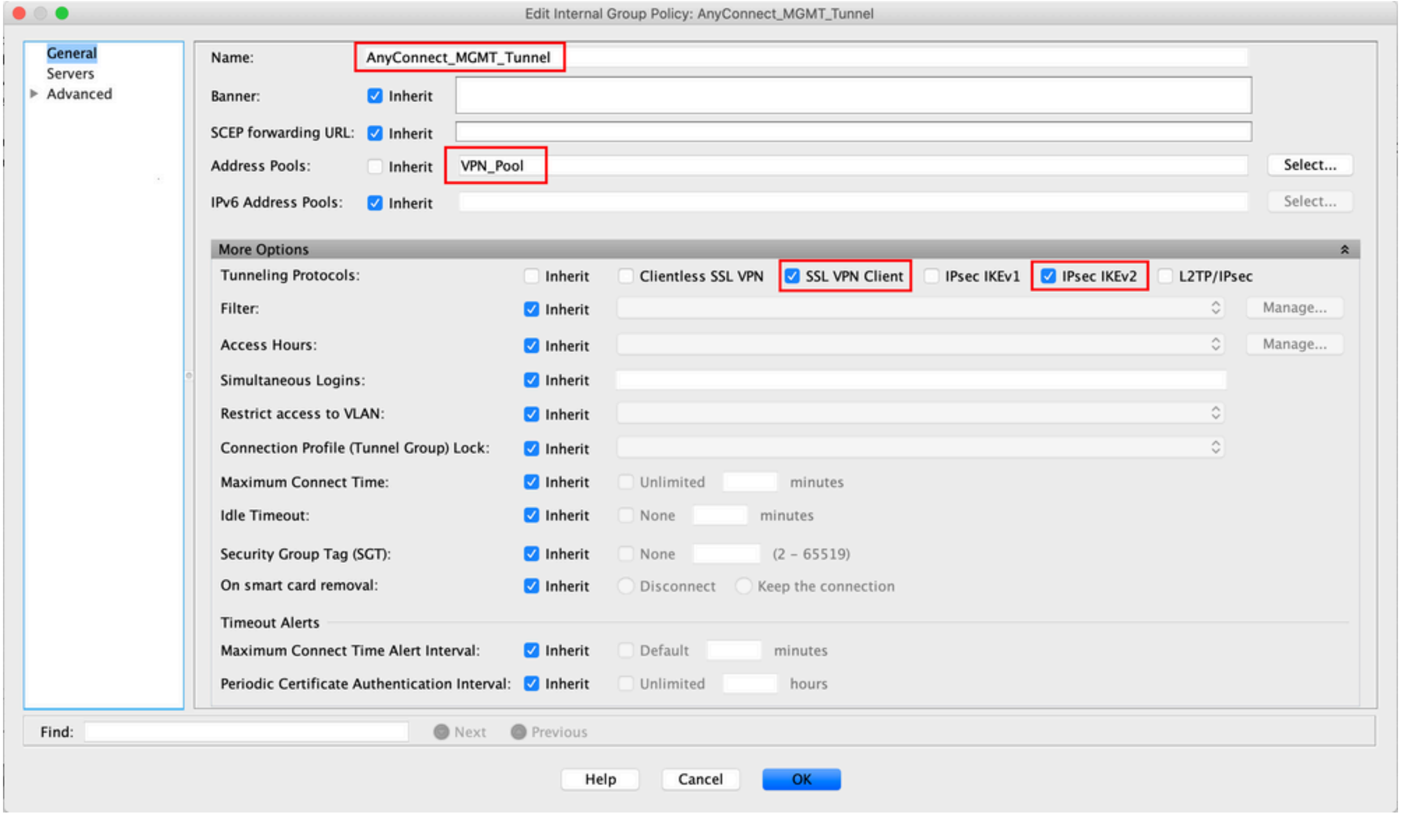
Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
AnyConnect	Internal	ssl-client	AnyConnect
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE...

第二步：提供 Name 组策略。分配/创建 Address Pool.选择 Tunneling Protocols 作为 SSL VPN Client 和/或 IPsec IKEv2,如图所示.



Edit Internal Group Policy: AnyConnect_MGMT_Tunnel

Name: AnyConnect_MGMT_Tunnel

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

Address Pools: □ Inherit VPN_Pool

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec IKEv1 ☑ IPsec IKEv2 □ L2TP/IPsec

Filter: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ None minutes

Security Group Tag (SGT): ☑ Inherit □ None (2 – 65519)

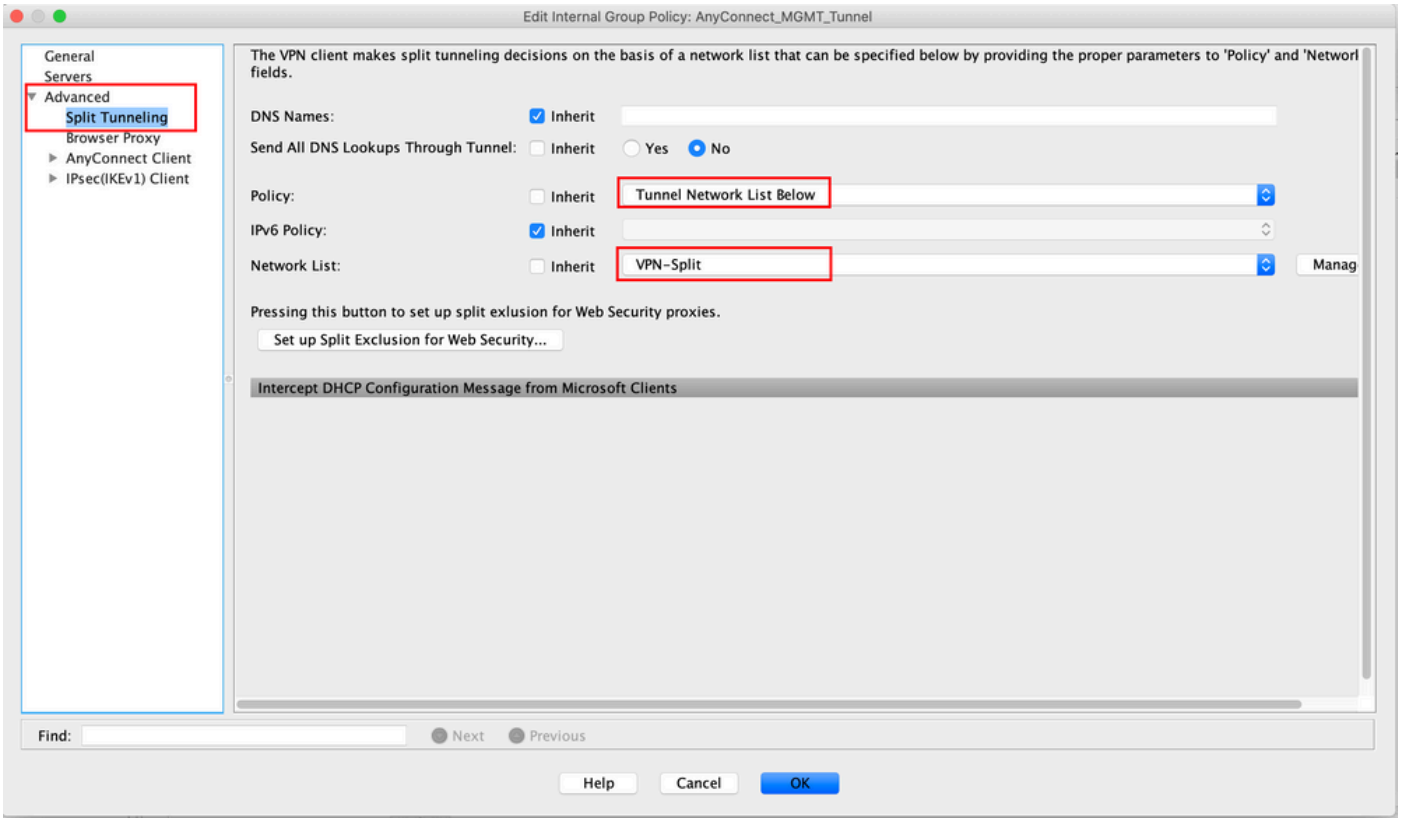
On smart card removal: ☑ Inherit ○ Disconnect ○ Keep the connection

Timeout Alerts

Maximum Connect Time Alert Interval: ☑ Inherit □ Default minutes

Periodic Certificate Authentication Interval: ☑ Inherit □ Unlimited hours

第三步： 导航至 Advanced > Split Tunneling.配置 Policy 作为 Tunnel Network List Below 并选择 Network List,如图所示.



Edit Internal Group Policy: AnyConnect_MGMT_Tunnel

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 'Networl 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 VPN-Split

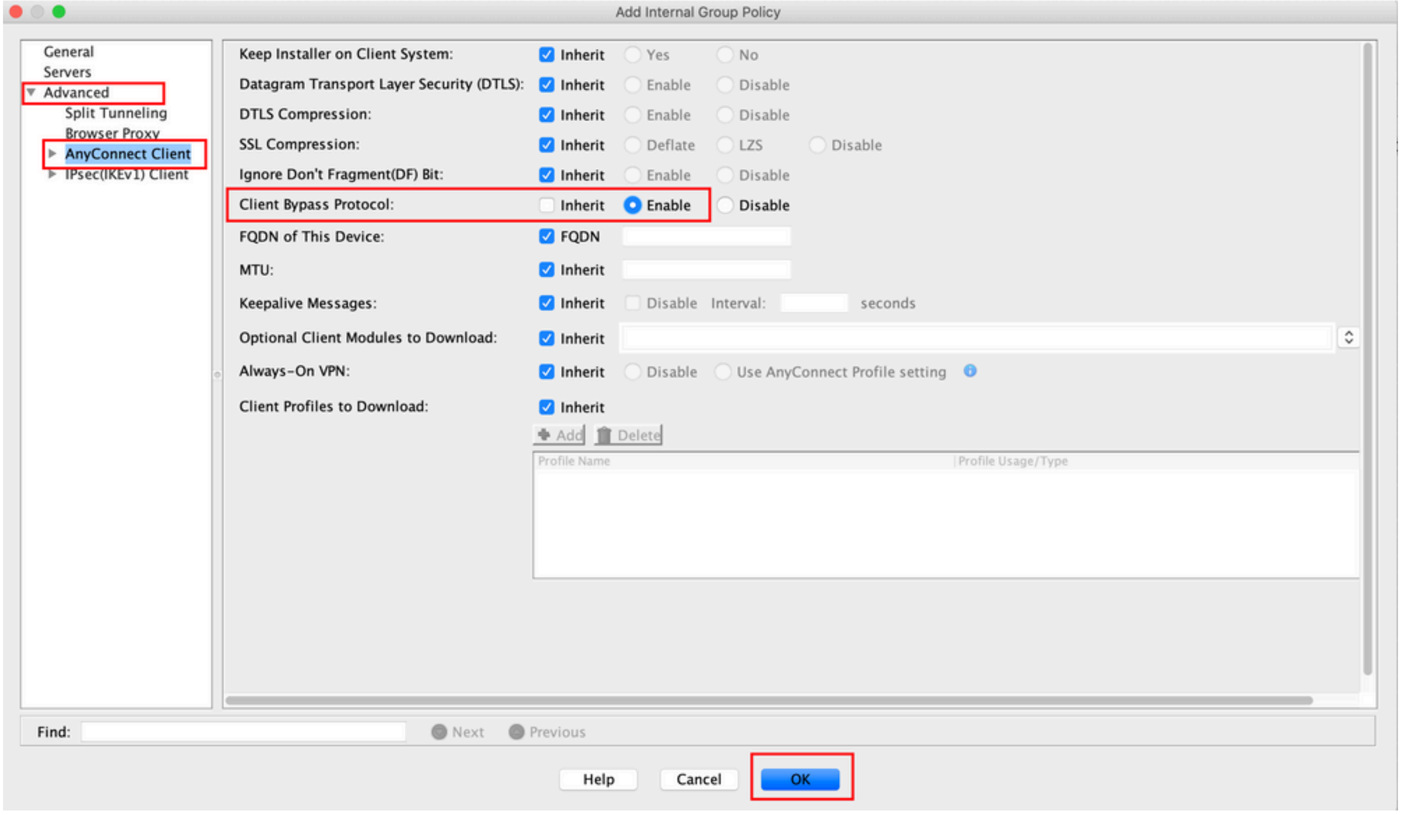
Pressing this button to set up split exlusion for Web Security proxies.

Set up Split Exclusion for Web Security...

Intercept DHCP Configuration Message from Microsoft Clients

注意：如果未同时为IP协议（IPv4和IPv6）推送客户端地址， **Client Bypass Protocol** 设置必须为 enabled 以便对应的流量不会受到管理隧道的干扰。要配置，请参阅步骤4。

第四步： 导航至 Advanced > AnyConnect Client. 设置 Client Bypass Protocol 到 Enable. 点击 OK 保存，如图所示。



Keep Installer on Client System: ☑ Inherit ○ Yes ○ No

Datagram Transport Layer Security (DTLS): ☑ Inherit ○ Enable ○ Disable

DTLS Compression: ☑ Inherit ○ Enable ○ Disable

SSL Compression: ☑ Inherit ○ Deflate ○ LZS ○ Disable

Ignore Don't Fragment(DF) Bit: ☑ Inherit ○ Enable ○ Disable

Client Bypass Protocol: □ Inherit ● Enable ○ Disable

FQDN of This Device: ☑ FQDN

MTU: ☑ Inherit

Keepalive Messages: ☑ Inherit □ Disable Interval: seconds

Optional Client Modules to Download: ☑ Inherit

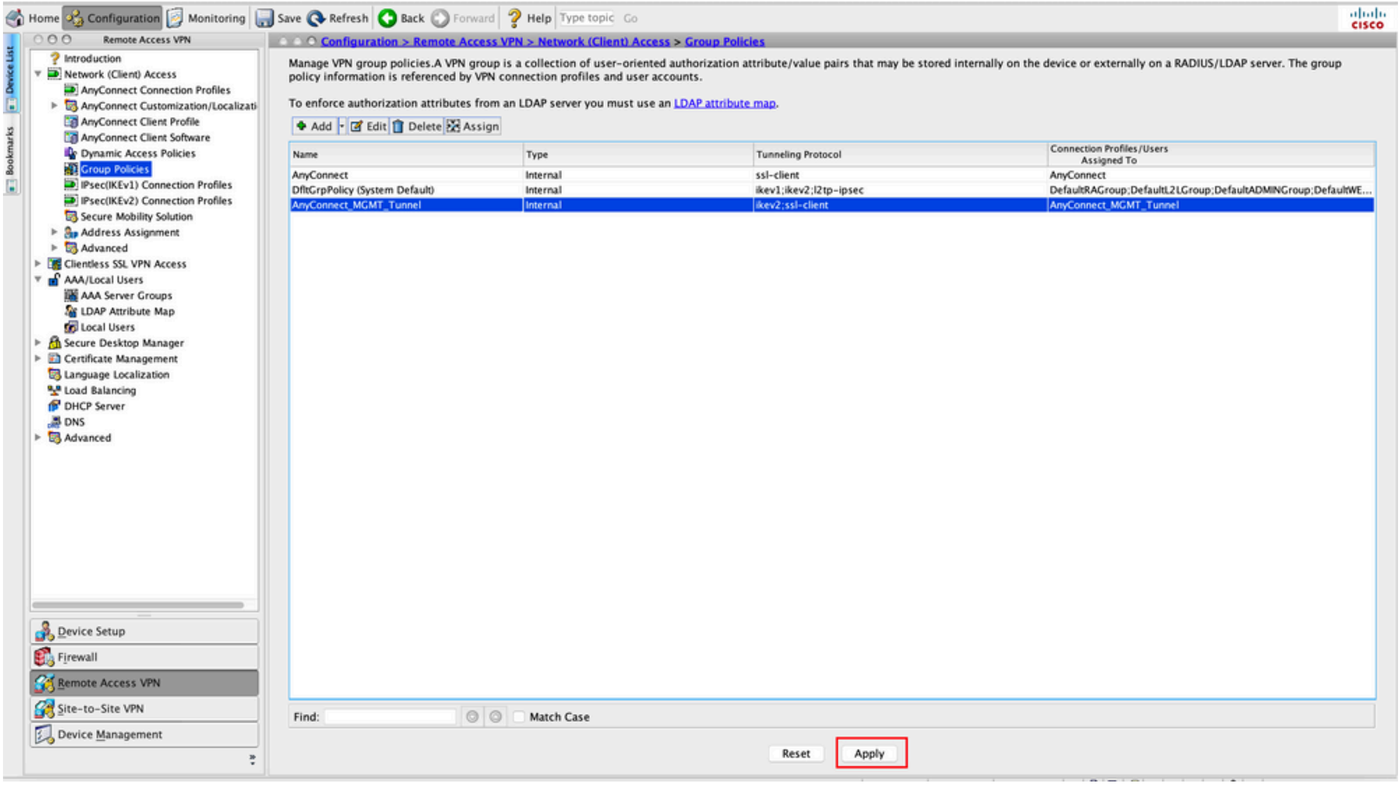
Always-On VPN: ☑ Inherit ○ Disable ○ Use AnyConnect Profile setting

Client Profiles to Download: ☑ Inherit

Add Delete

Profile Name	Profile Usage/Type

第五步：如图所示，单击 Apply 将配置推送到ASA。



Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

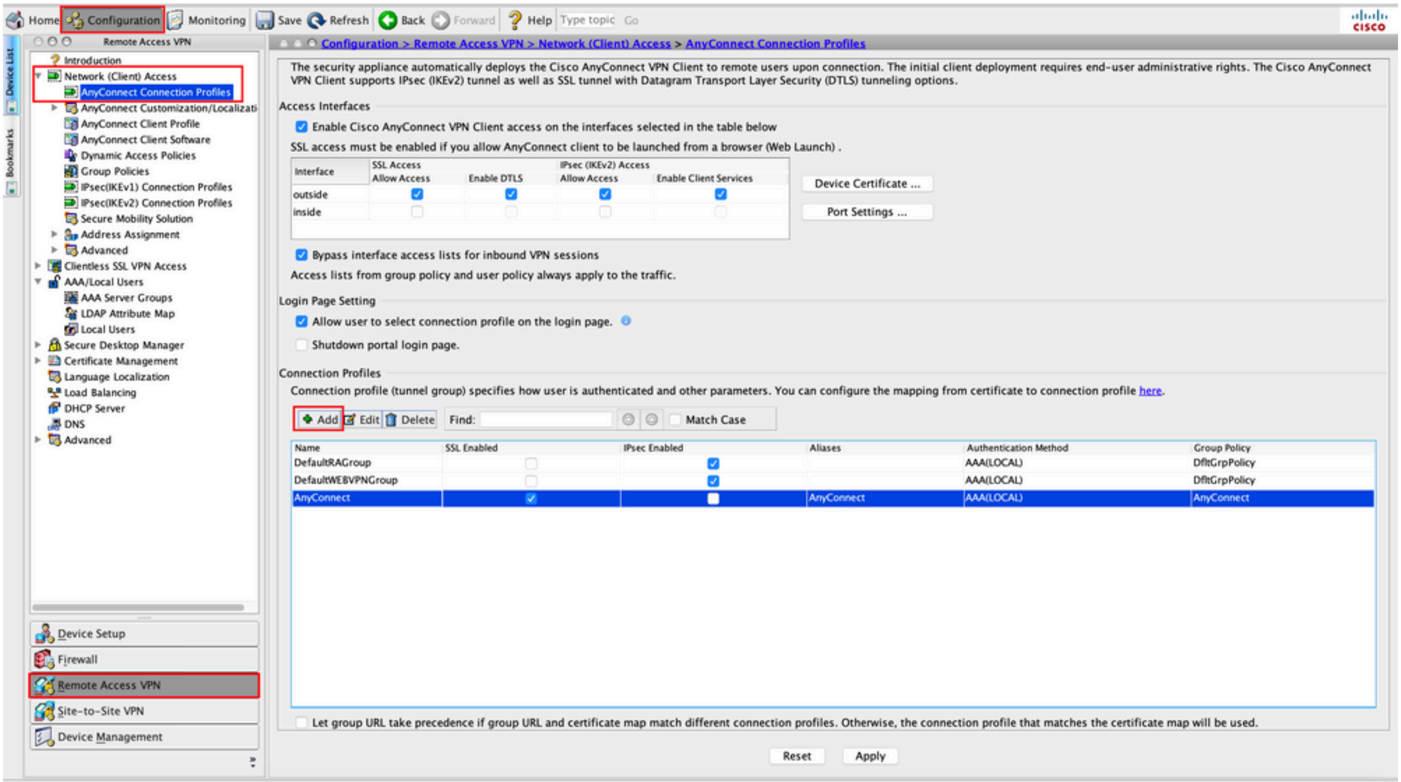
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
AnyConnect	Internal	ssl-client	AnyConnect
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE...
AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel

组策略的CLI配置：

```
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
```

第六步：创建AnyConnect连接配置文件导航至 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. 点击 Add.

注意：建议创建仅用于AnyConnect管理隧道的新AnyConnect连接配置文件。



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☑	☑
inside	□	□	□	□

Device Certificate ...

Port Settings ...

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile on the login page.

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

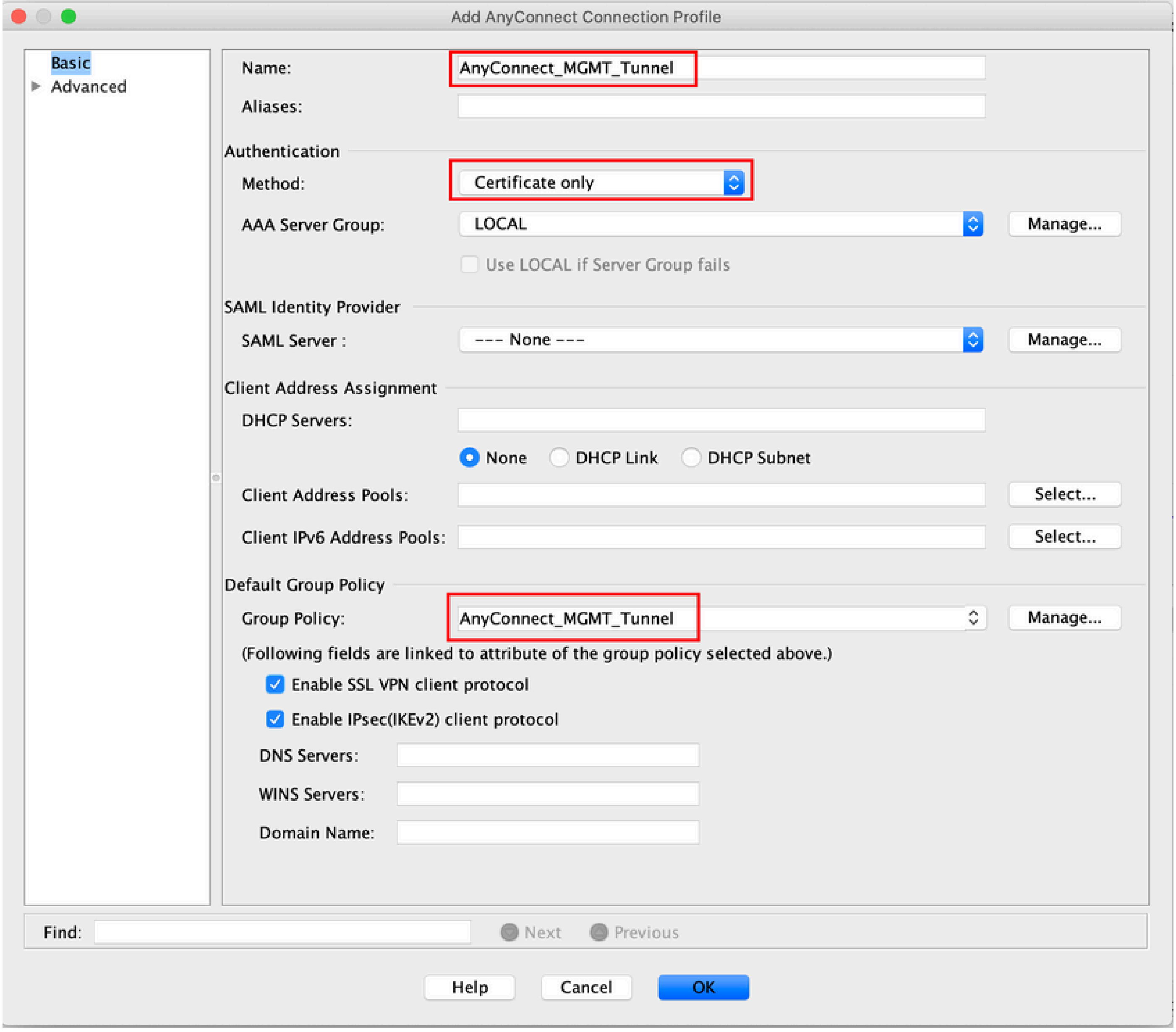
Add Edit Delete Find: Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
AnyConnect	☑	□	AnyConnect	AAA(LOCAL)	AnyConnect

□ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Reset Apply

步骤 7.提供 Name 连接配置文件，并设置 Authentication Method 作为 Certificate only.选择 Group Policy 作为 第1步中创建的配置。



Add AnyConnect Connection Profile

Basic

Advanced

Name: AnyConnect_MGMT_Tunnel

Aliases:

Authentication

Method: Certificate only

AAA Server Group: LOCAL

☐ Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : --- None ---

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: AnyConnect_MGMT_Tunnel

(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:

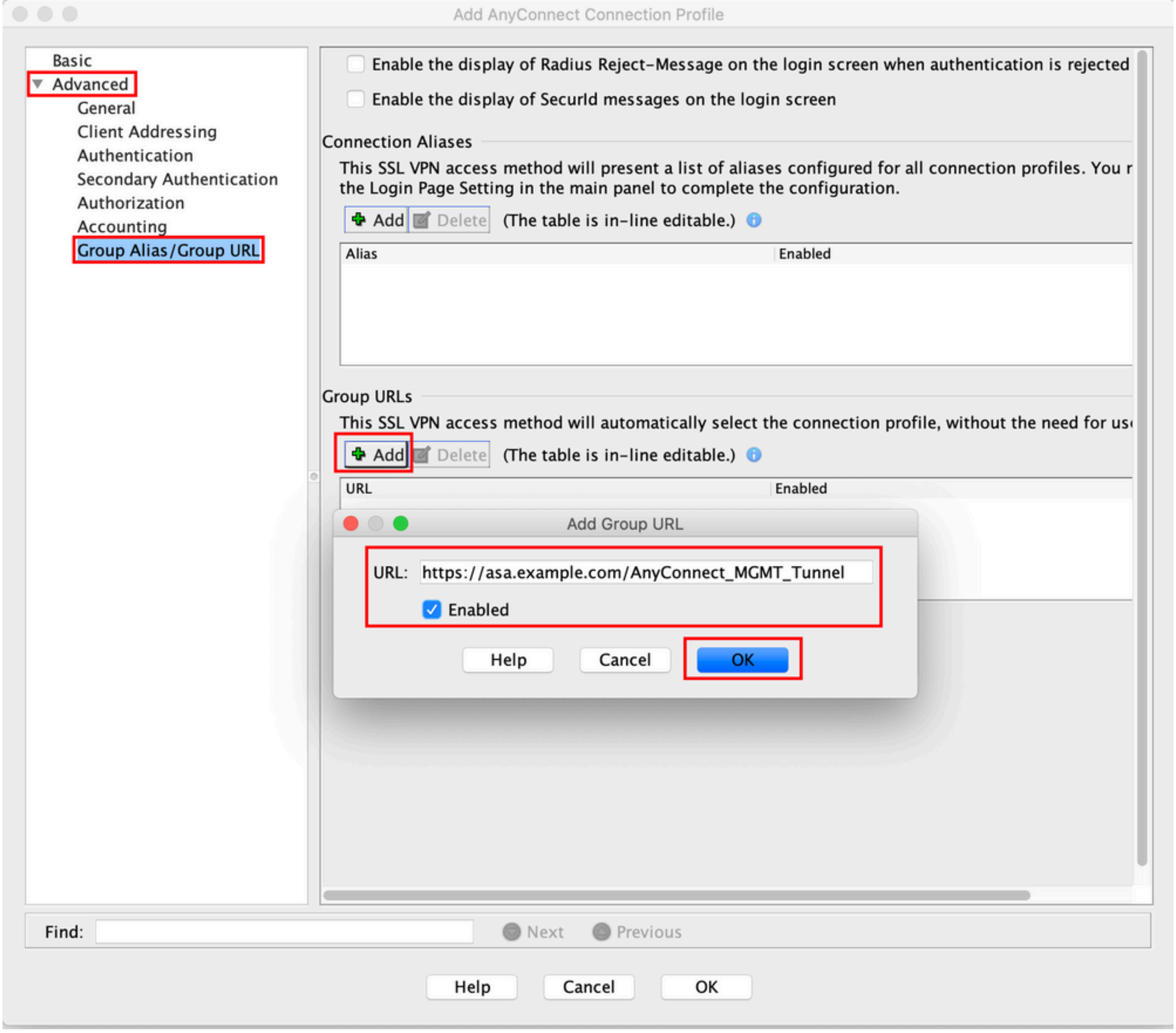
Domain Name:

Find:

注意：确保ASA上存在来自本地CA的根证书。 导航至 Configuration > Remote Access VPN > Certificate Management > CA Certificates 添加/查看证书。

注意：确保同一本地CA颁发的身份证书存在于计算机证书存储区（适用于Windows）和/或系统密钥链（适用于macOS）中。

步骤 8导航至 Advanced > Group Alias/Group URL.点击 Add 在 Group URLs 并添加 URL.确保 Enabled 已选中。点击 OK 保存，如图所示。



□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You r

the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

Group URLs

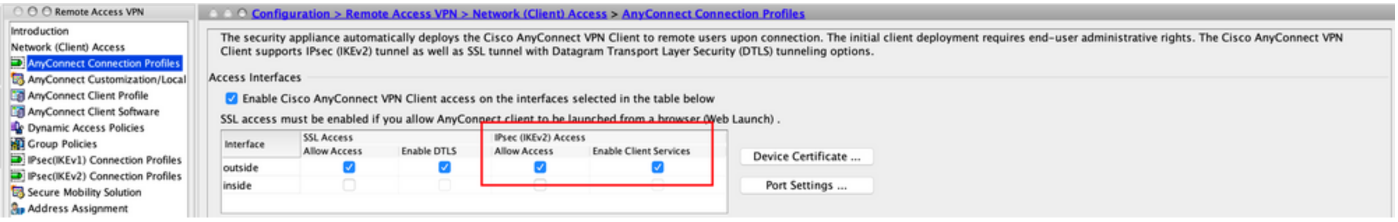
This SSL VPN access method will automatically select the connection profile, without the need for us

(The table is in-line editable.)

URL: https://asa.example.com/AnyConnect_MGMT_Tunnel

☑ Enabled

如果使用IKEv2，请确保 IPsec (IKEv2) Access 在用于AnyConnect的接口上启用。


Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Local
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
IPsec(IKEv2) Connection Profiles
Secure Mobility Solution
Address Assignment
Device Certificate ...
Port Settings ...

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

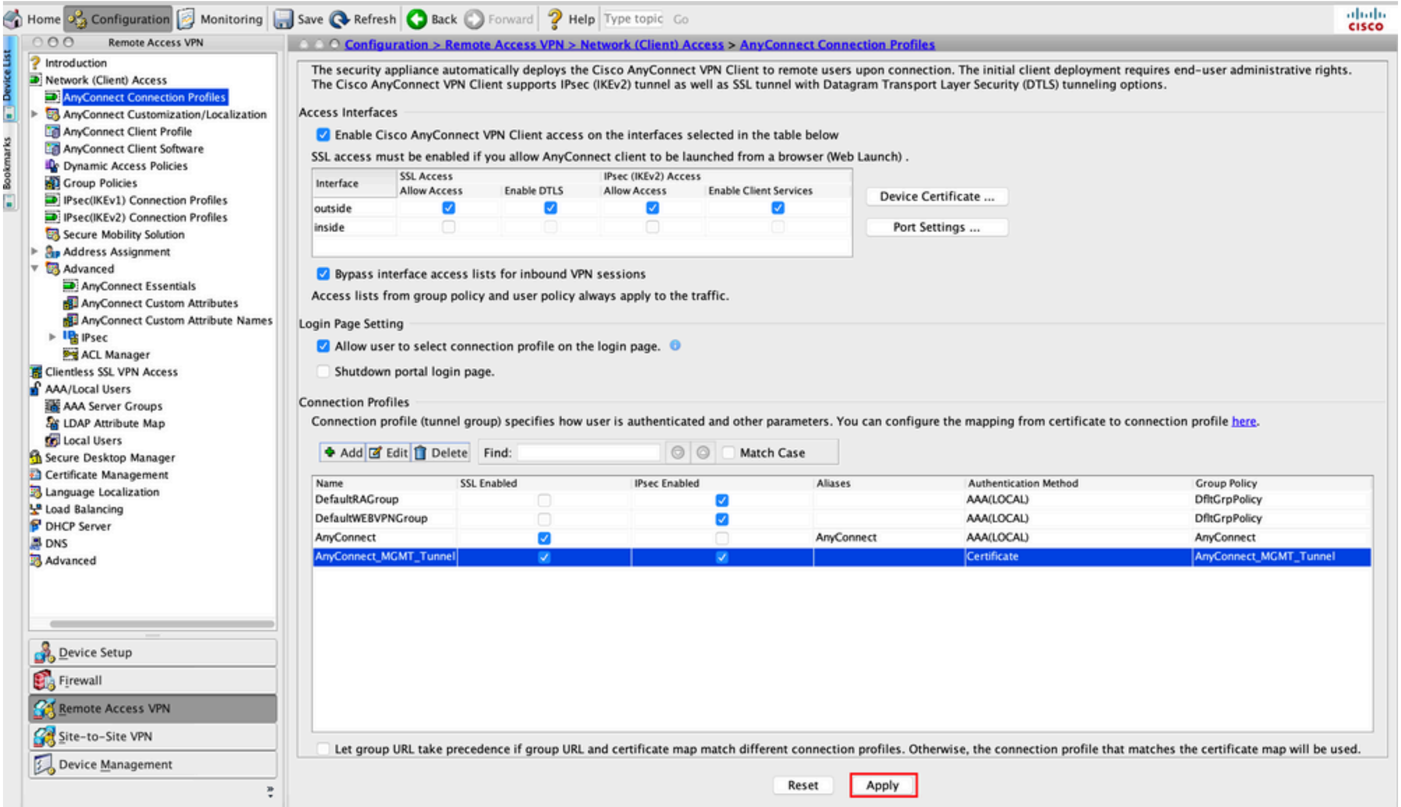
Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☑	☑
inside	□	□	□	□

步骤 9点击 Apply 将配置推送到ASA。



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☑	☑
inside	□	□	□	□

Device Certificate ...

Port Settings ...

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile on the login page.

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

Add Edit Delete Find: □ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
AnyConnect	☑	□	AnyConnect	AAA(LOCAL)	AnyConnect
AnyConnect_MGMT_Tunnel	☑	☑		Certificate	AnyConnect_MGMT_Tunnel

□ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

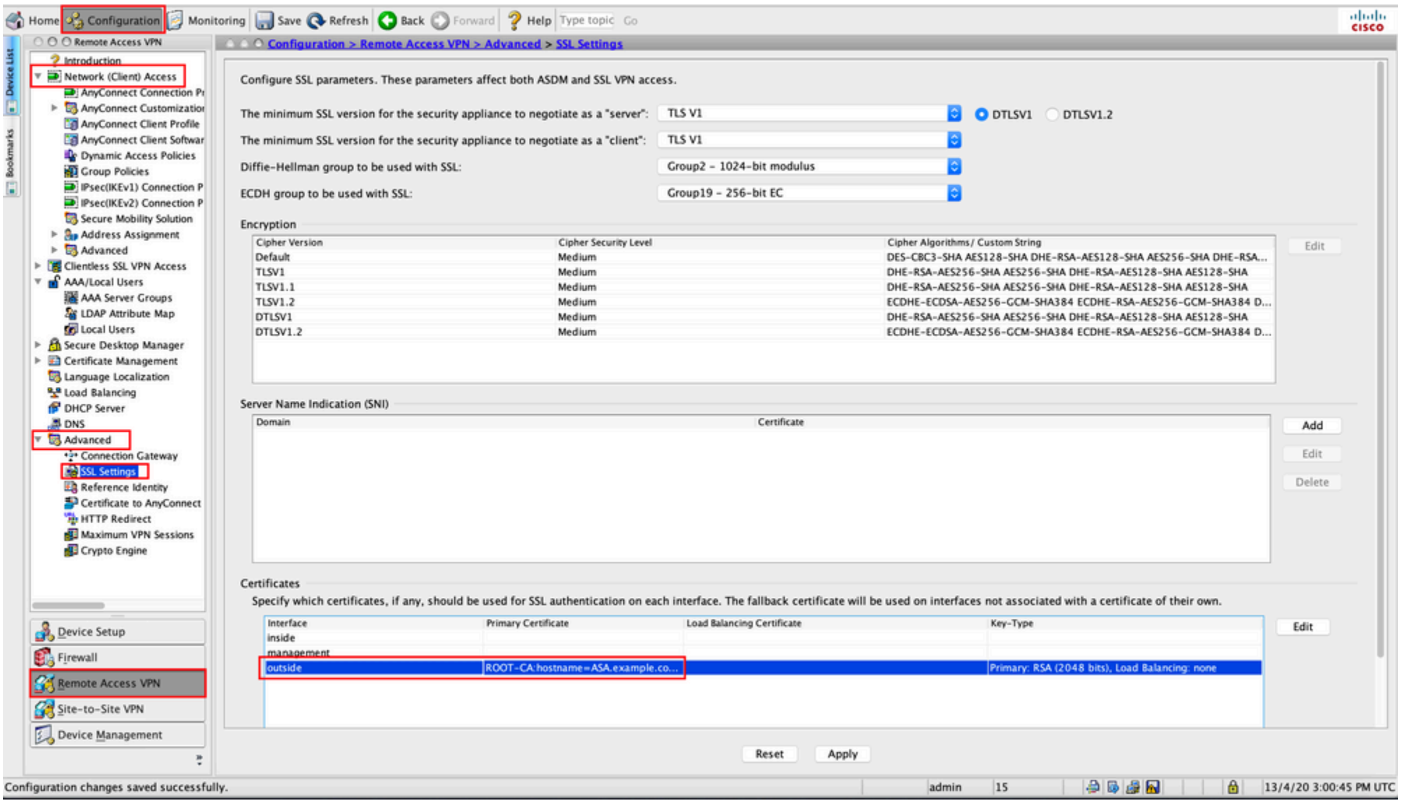
Reset Apply

连接配置文件（隧道组）的CLI配置：

```
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
```

步骤 10确保在ASA上安装受信任证书并绑定到用于AnyConnect连接的接口。导航至 Configuration > Remote Access VPN > Advanced > SSL Settings 添加/查看此设置。

> **注意：**请参阅在ASA上安装身份证书。



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": TLS V1 ● DTLSV1 ○ DTLSV1.2

The minimum SSL version for the security appliance to negotiate as a "client": TLS V1

Diffie-Hellman group to be used with SSL: Group2 - 1024-bit modulus

ECDH group to be used with SSL: Group19 - 256-bit EC

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

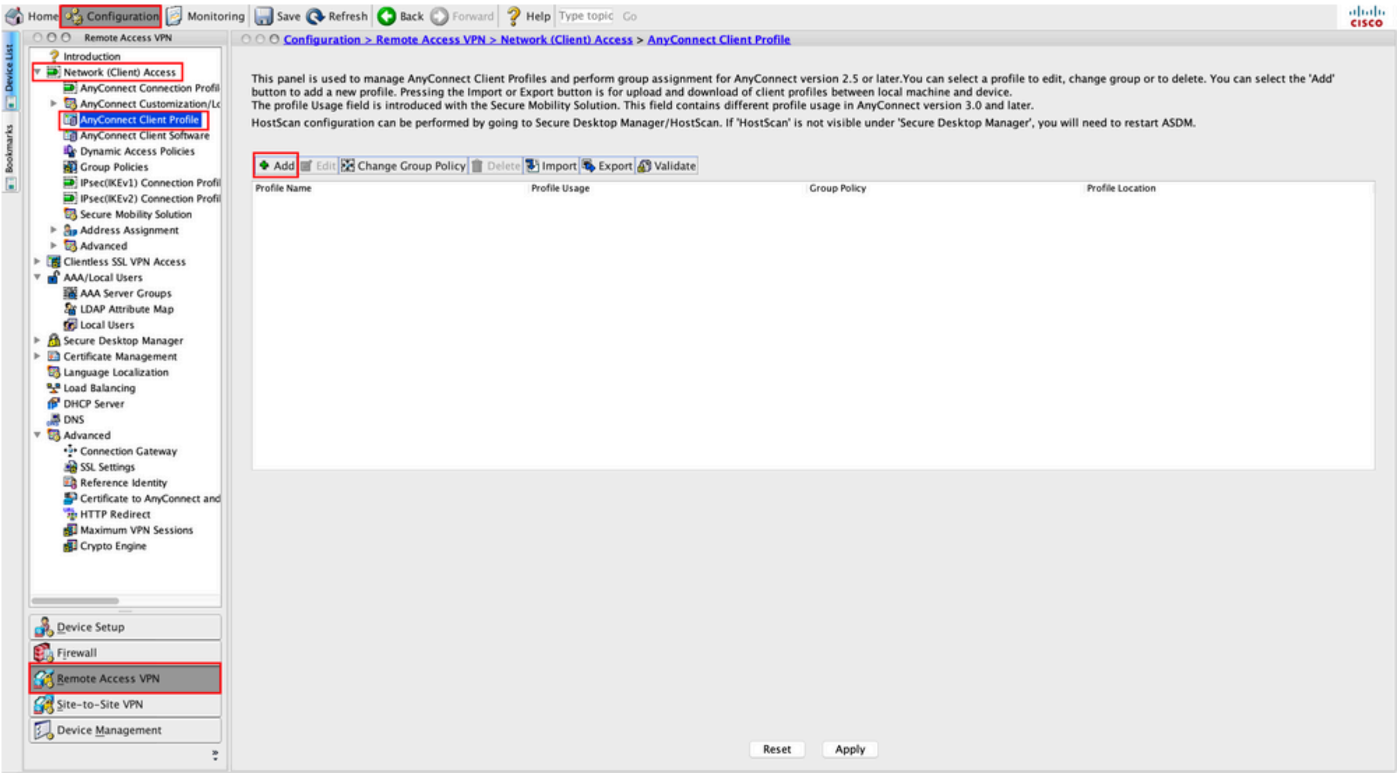
Configuration changes saved successfully. admin 15 13/4/20 3:00:45 PM UTC

SSL信任点的CLI配置：

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

创建AnyConnect管理VPN配置文件

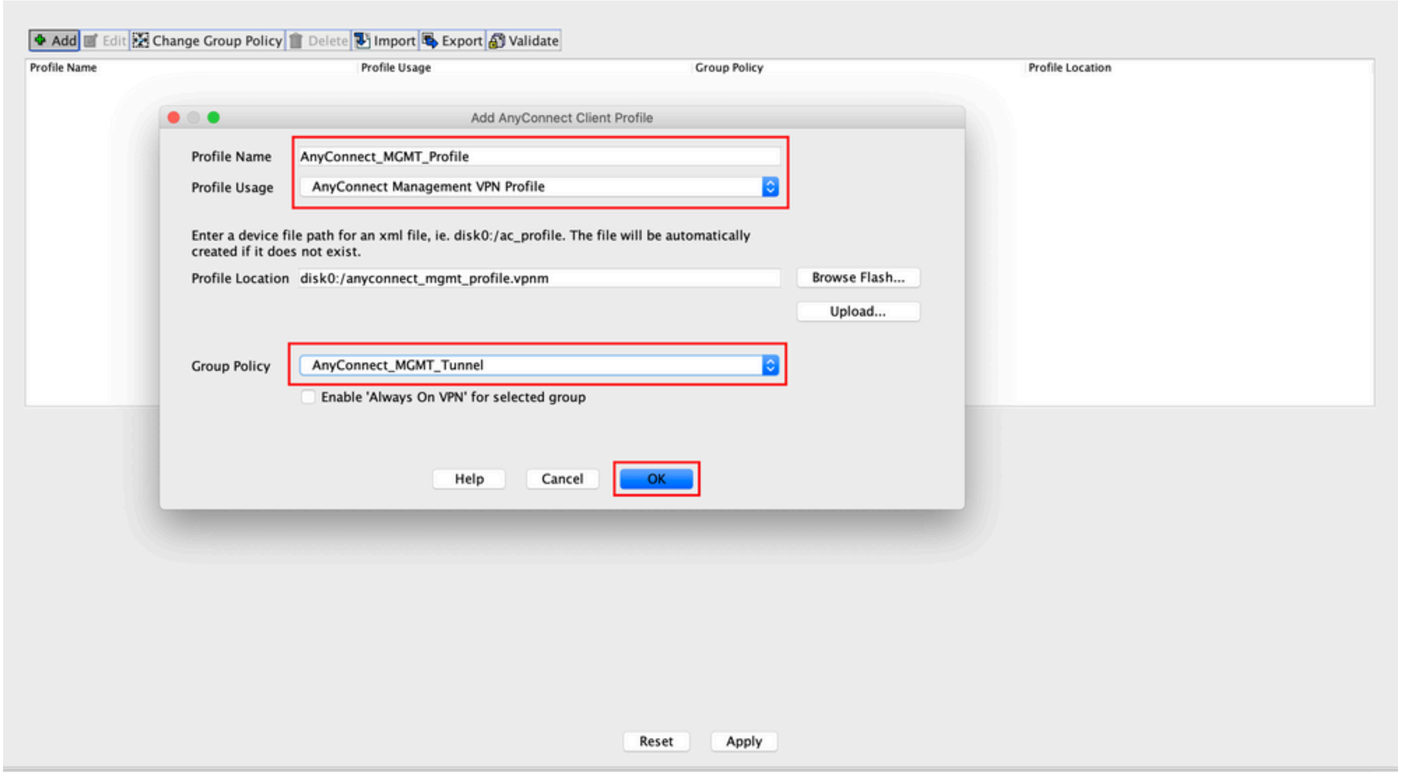
步骤1: 创建AnyConnect客户端配置文件。导航至 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.点击 Add,如图所示.



This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
HostScan configuration can be performed by going to Secure Desktop Manager/HostScan. If 'HostScan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Profile Name	Profile Usage	Group Policy	Profile Location

第二步：提供 Profile Name.选择 Profile Usage 作为 AnyConnect Management VPN profile.选择 Group Policy 第1步中创建。点击 OK ,如图所示.



Profile Name: AnyConnect_MGMT_Profile

Profile Usage: AnyConnect Management VPN Profile

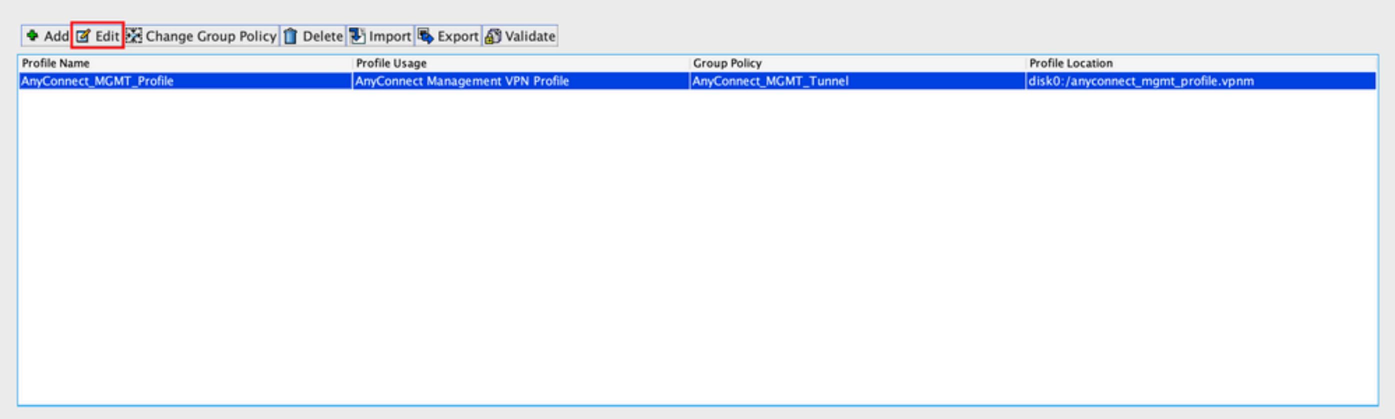
Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.

Profile Location: disk0:/anyconnect_mgmt_profile.vpnm

Group Policy: AnyConnect_MGMT_Tunnel

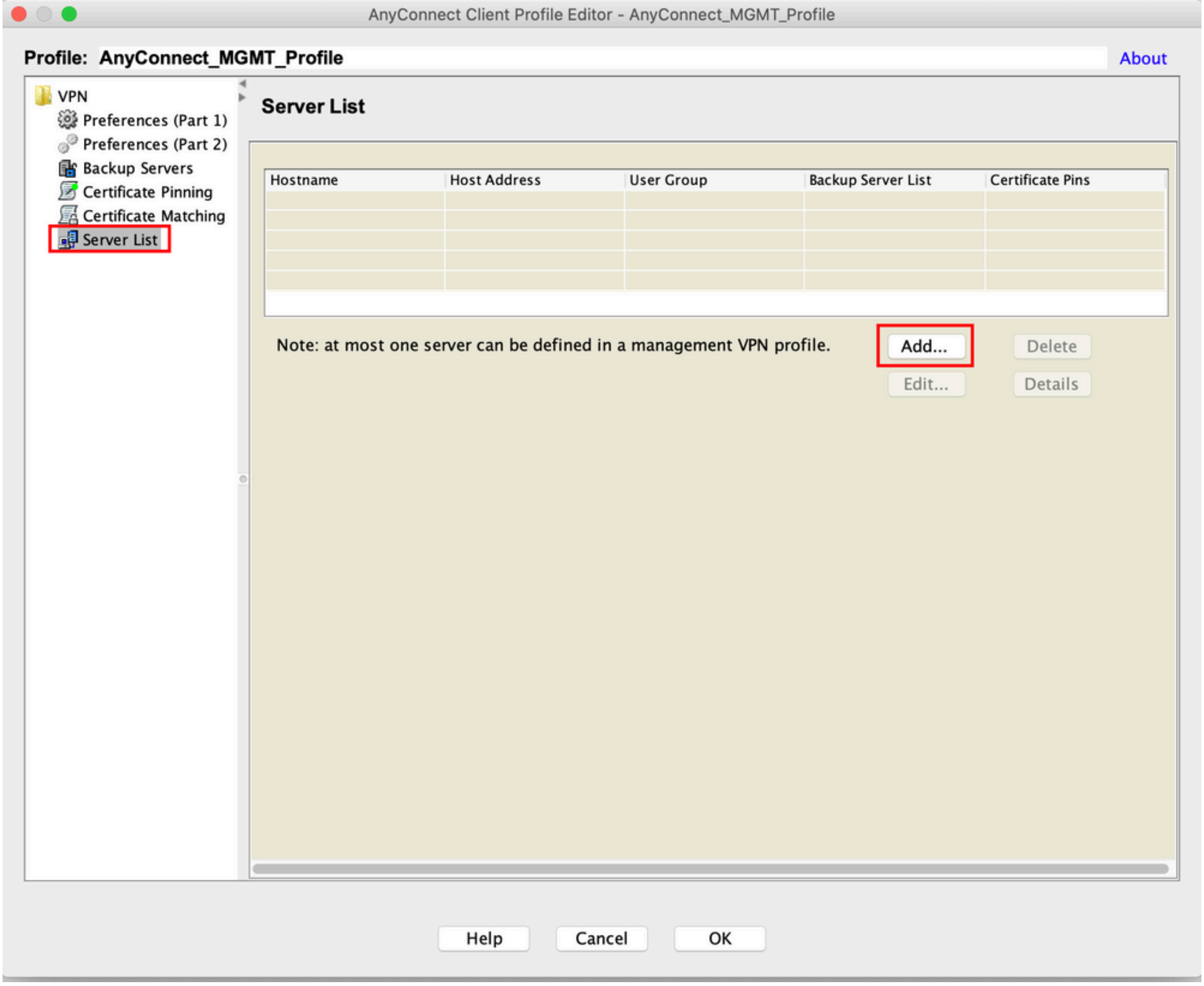
□ Enable 'Always On VPN' for selected group

第三步：选择已创建的配置文件，然后点击 Edit,如图所示.



Profile Name	Profile Usage	Group Policy	Profile Location
AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm

第四步：导航至 Server List.点击 Add 添加新的服务器列表条目，如图所示。



AnyConnect Client Profile Editor - AnyConnect_MGMT_Profile

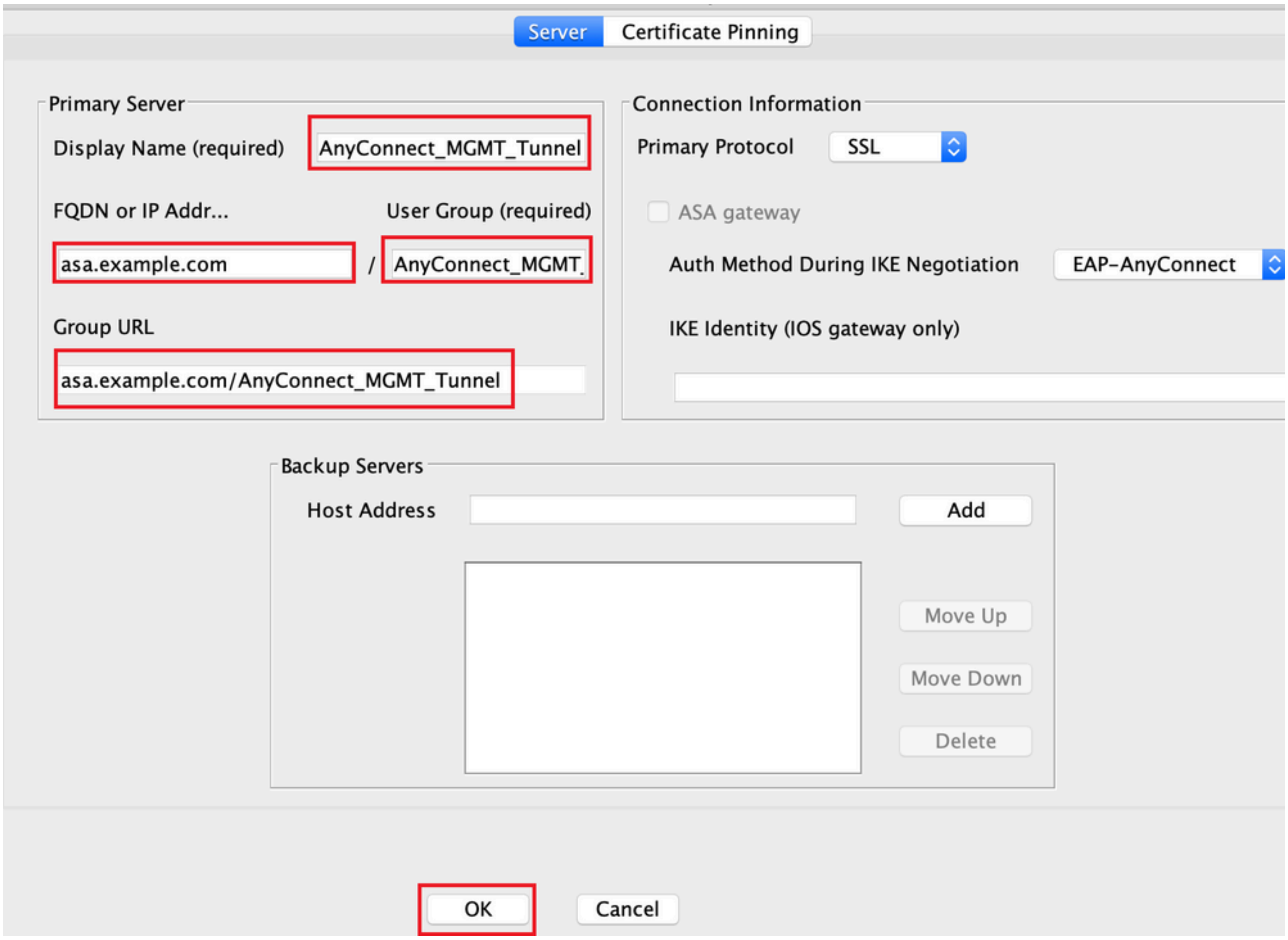
Profile: AnyConnect_MGMT_Profile

Server List

Hostname	Host Address	User Group	Backup Server List	Certificate Pins

Note: at most one server can be defined in a management VPN profile.

第五步：提供 Display Name.添加 FQDN/IP address 的ASA。提供 User Group 作为隧道组名称。 Group URL 自动填入 FQDN 和 User Group.点击 OK.



Display Name (required): AnyConnect_MGMT_Tunnel

FQDN or IP Addr...: asa.example.com / User Group (required): AnyConnect_MGMT_

Group URL: asa.example.com/AnyConnect_MGMT_Tunnel

Primary Protocol: SSL

□ ASA gateway

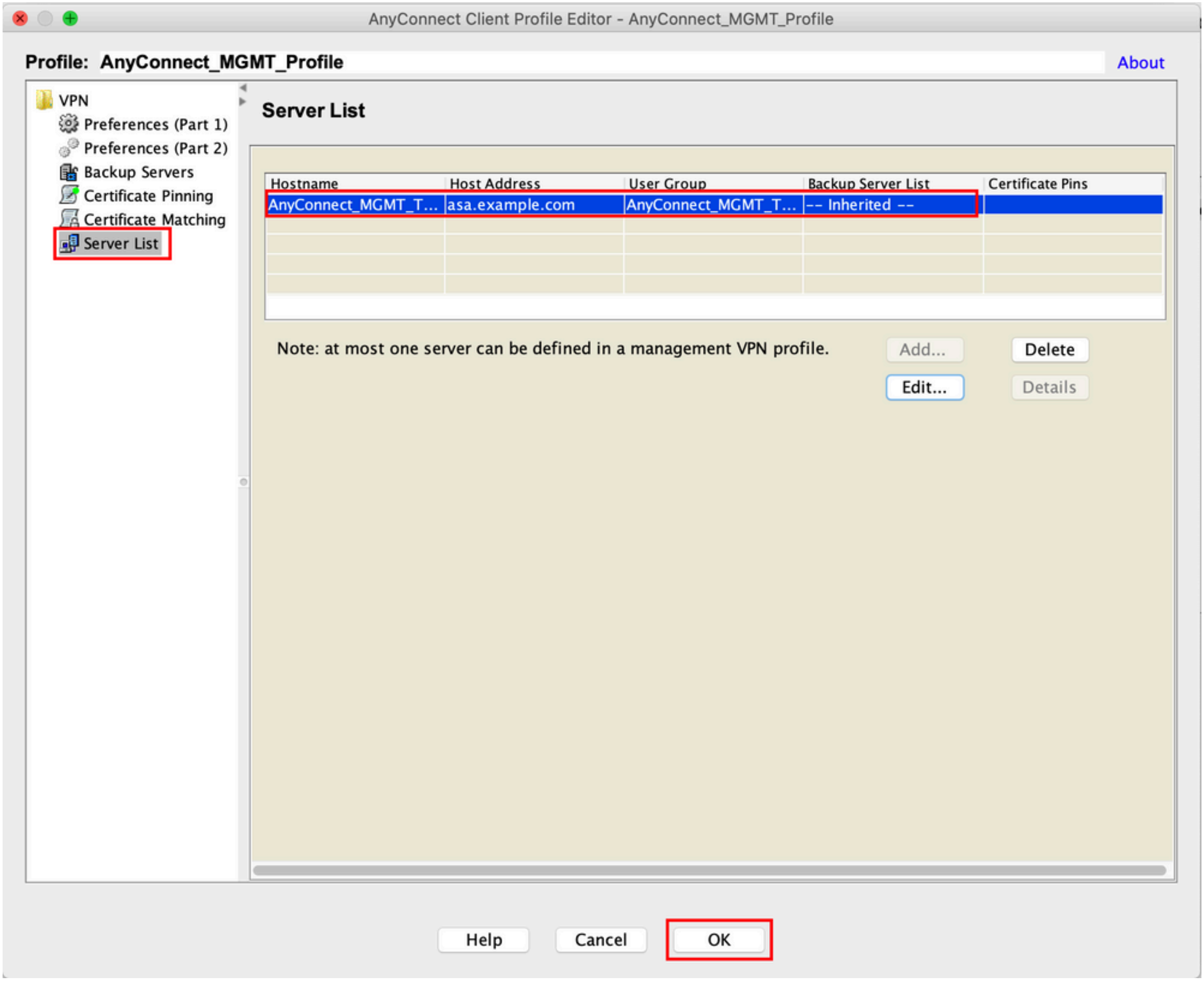
Auth Method During IKE Negotiation: EAP-AnyConnect

IKE Identity (IOS gateway only)

注意：FQDN/IP地址+用户组必须与步骤8中配置AnyConnect连接配置文件时提到的组URL相同。

注意：将IKEv2用作协议的AnyConnect也可用于建立到ASA的管理VPN。确保 Primary Protocol 设置为 IPsec 在步骤5中。

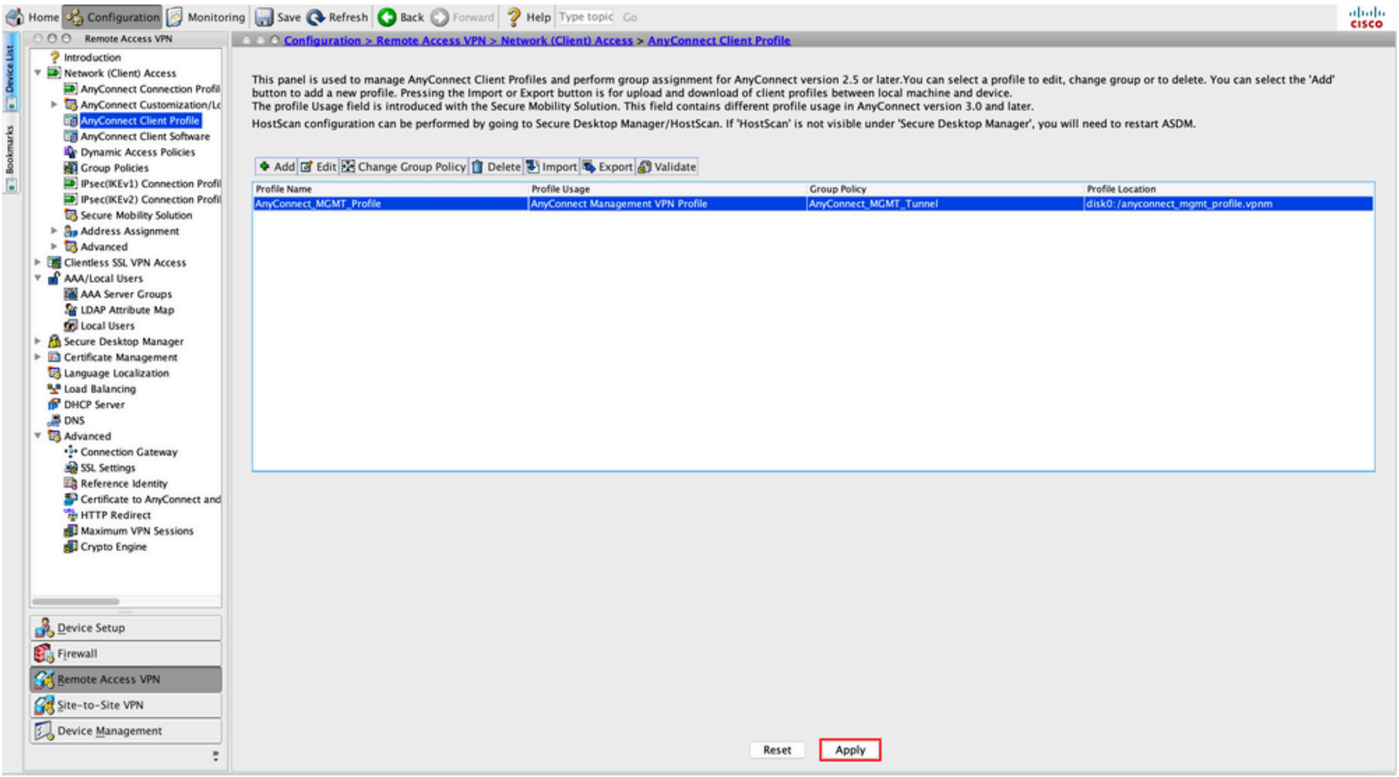
第六步：如图所示，单击 OK 保存。



Hostname	Host Address	User Group	Backup Server List	Certificate Pins
AnyConnect_MGMT_T...	asa.example.com	AnyConnect_MGMT_T...	-- Inherited --	

Note: at most one server can be defined in a management VPN profile.

步骤 7.点击 Apply t将配置推送到ASA，如图所示。



This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.

HostScan configuration can be performed by going to Secure Desktop Manager/HostScan. If 'HostScan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Profile Name	Profile Usage	Group Policy	Profile Location
AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm

添加AnyConnect管理VPN配置文件后的CLI配置。

```
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客户端计算机上的AnyConnect管理VPN配置文件：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>






       <ShowPreConnectMessage>false</ShowPreConnectMessage>






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

--- Output Omitted ---
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

```
</AnyConnectProfile>
```

注意：如果用户AnyConnect VPN配置文件中使用了受信任网络检测(TND)，则建议匹配管理VPN配置文件中相同的设置，以获得一致的用户体验。根据应用到用户VPN隧道配置文件的TND设置触发管理VPN隧道。 此外，管理VPN配置文件中的TND Connect操作（仅在管理VPN隧道处于活动状态时实施）始终应用于用户VPN隧道，以确保管理VPN隧道对最终用户透明。

注意：在任何最终用户PC上，如果管理VPN配置文件启用了TND设置，且用户VPN配置文件缺失，则它会考虑TND的默认首选项设置（在AC客户端应用中的默认首选项中禁用），以代替缺失的用户VPN配置文件。这种不匹配可能导致意外/未定义的行为。
默认情况下，TND设置在默认首选项中禁用。
要克服AnyConnect客户端应用中的默认首选项硬编码设置，最终用户PC必须拥有两个VPN配置文件，一个用户VPN配置文件和一个AC管理VPN配置文件，并且两者必须具有相同的TND设置。
管理VPN隧道连接和断开背后的逻辑是，为了建立管理VPN隧道，AC代理使用用户VPN配置文件TND设置，并且对于断开管理VPN隧道，它检查管理VPN配置文件TND设置。

AnyConnect管理VPN配置文件的部署方法

- 使用ASA连接配置文件成功完成用户VPN连接，以便从VPN网关下载AnyConnect管理VPN配置文件。

  注意：如果用于管理VPN隧道的协议是IKEv2，则需要通过SSL建立第一个连接（为了从ASA下载AnyConnect管理VPN配置文件）。

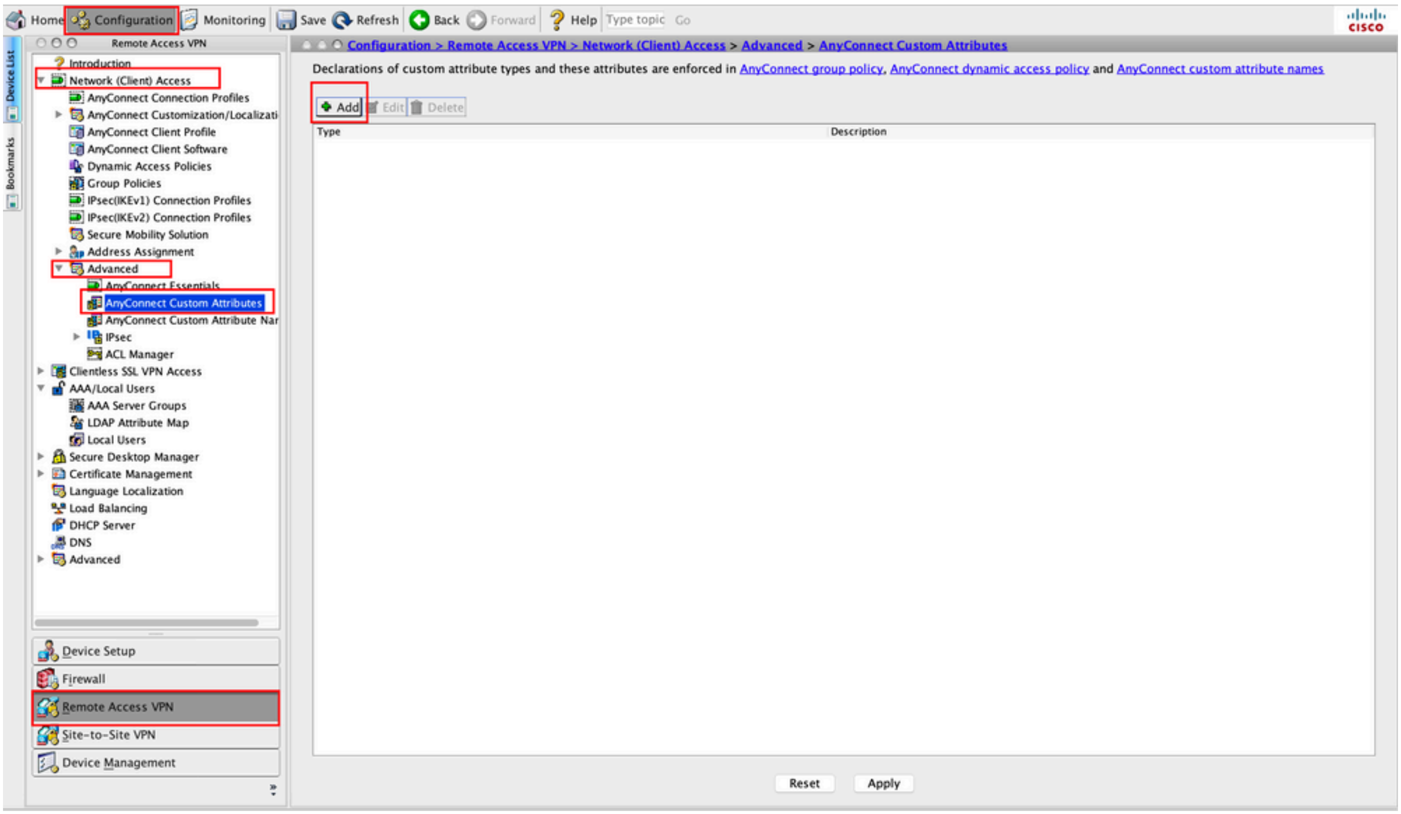
- AnyConnect管理VPN配置文件可以通过GPO推送或手动安装手动上传到客户端计算机(确保配置文件名称为 VpnMgmtTunProfile.xml影响。

  需要添加配置文件的文件夹位置：
  Windows 窗口版本: **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**
  macOS: /opt/cisco/anyconnect/profile/mgmttun/

（可选）配置自定义属性以支持全隧道配置

默认情况下，管理VPN隧道需要包括隧道配置的分割以避免对用户发起的网络通信的影响。在用于管理隧道连接的组策略中配置自定义属性时，可以覆盖此属性。

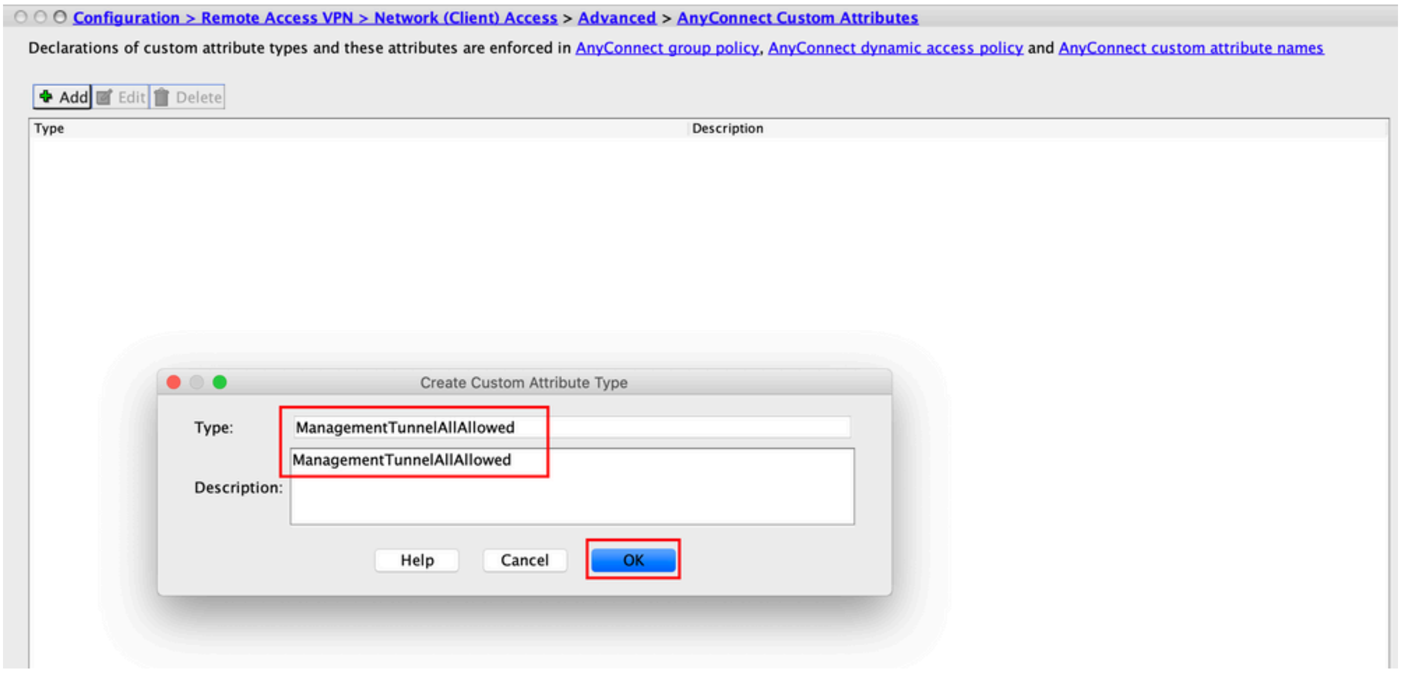
步骤1:导航至Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. 点击 Add,如图所示.



Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes

Declarations of custom attribute types and these attributes are enforced in AnyConnect group policy, AnyConnect dynamic access policy and AnyConnect custom attribute names

步骤 2将自定义属性Type设置为 ManagementTunnelAllAllowed 并提供 Description. 点击 OK,如图所示.



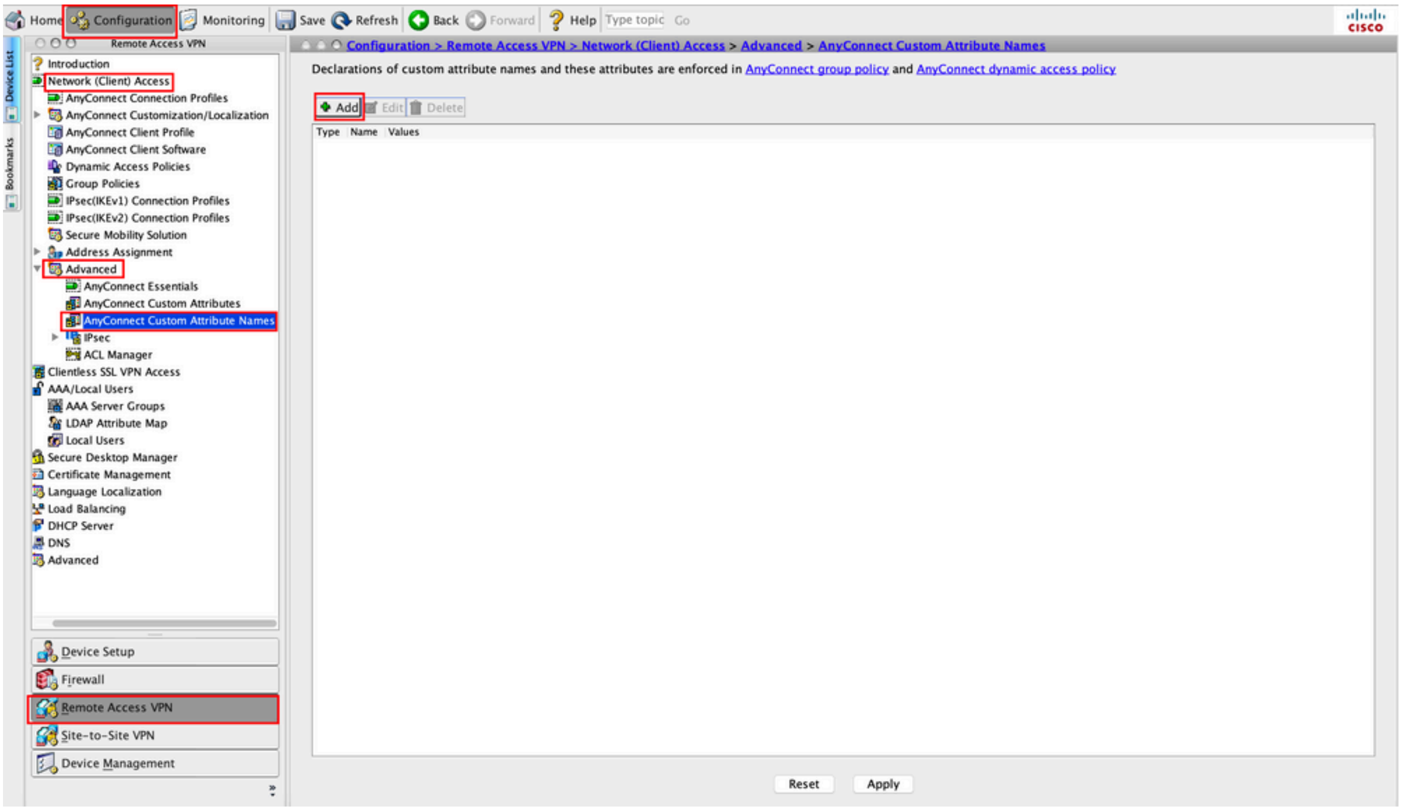
Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes

Declarations of custom attribute types and these attributes are enforced in AnyConnect group policy, AnyConnect dynamic access policy and AnyConnect custom attribute names

Type: ManagementTunnelAllAllowed

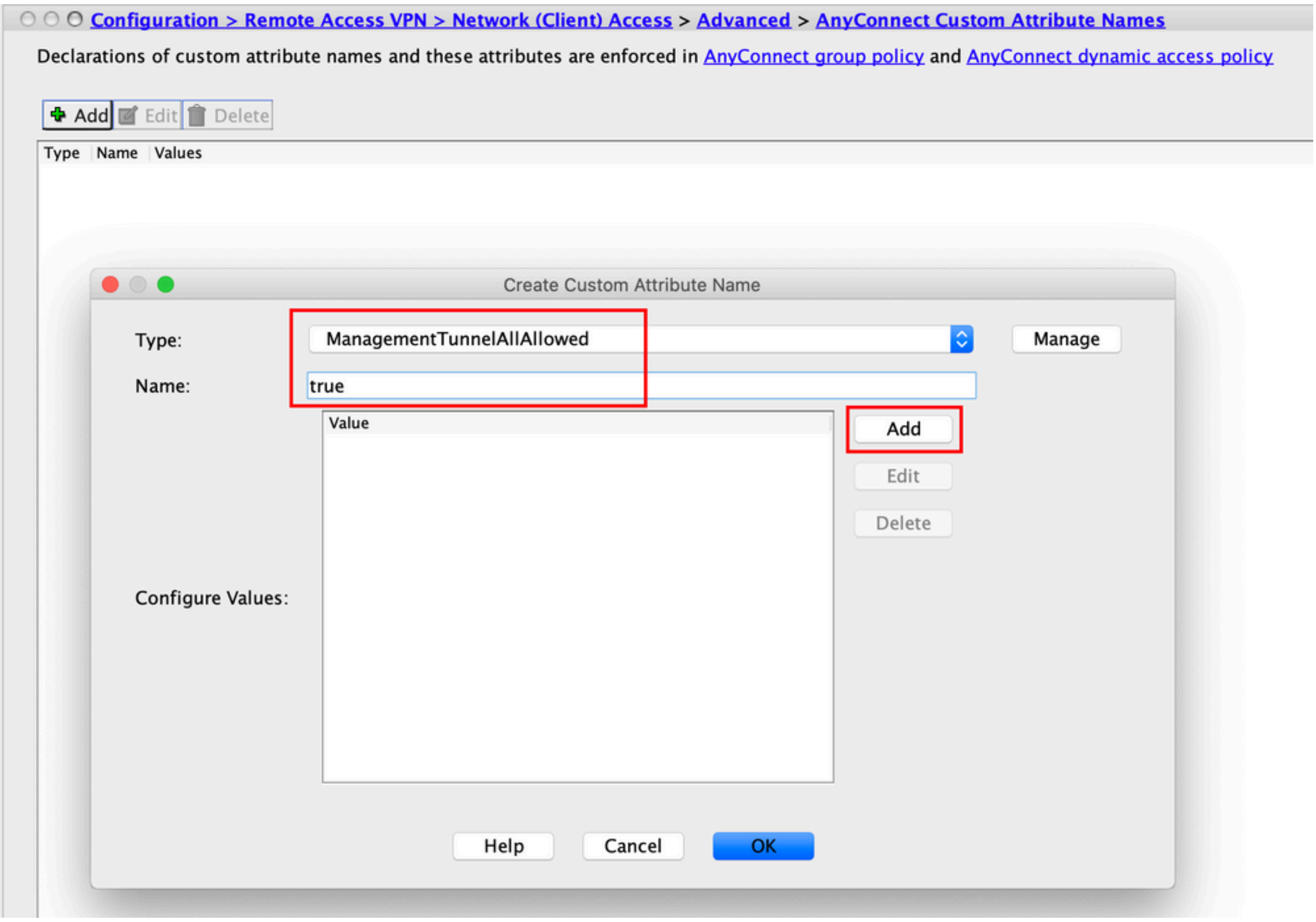
Description: ManagementTunnelAllAllowed

第三步： 导航至 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names**. 点击 Add,如图所示.



Declarations of custom attribute names and these attributes are enforced in AnyConnect group policy and AnyConnect dynamic access policy

第四步：选择“类型”作为 ManagementTunnelAllAllowed．将名称设置为 true.点击 Add提供自定义属性值，如图所示。

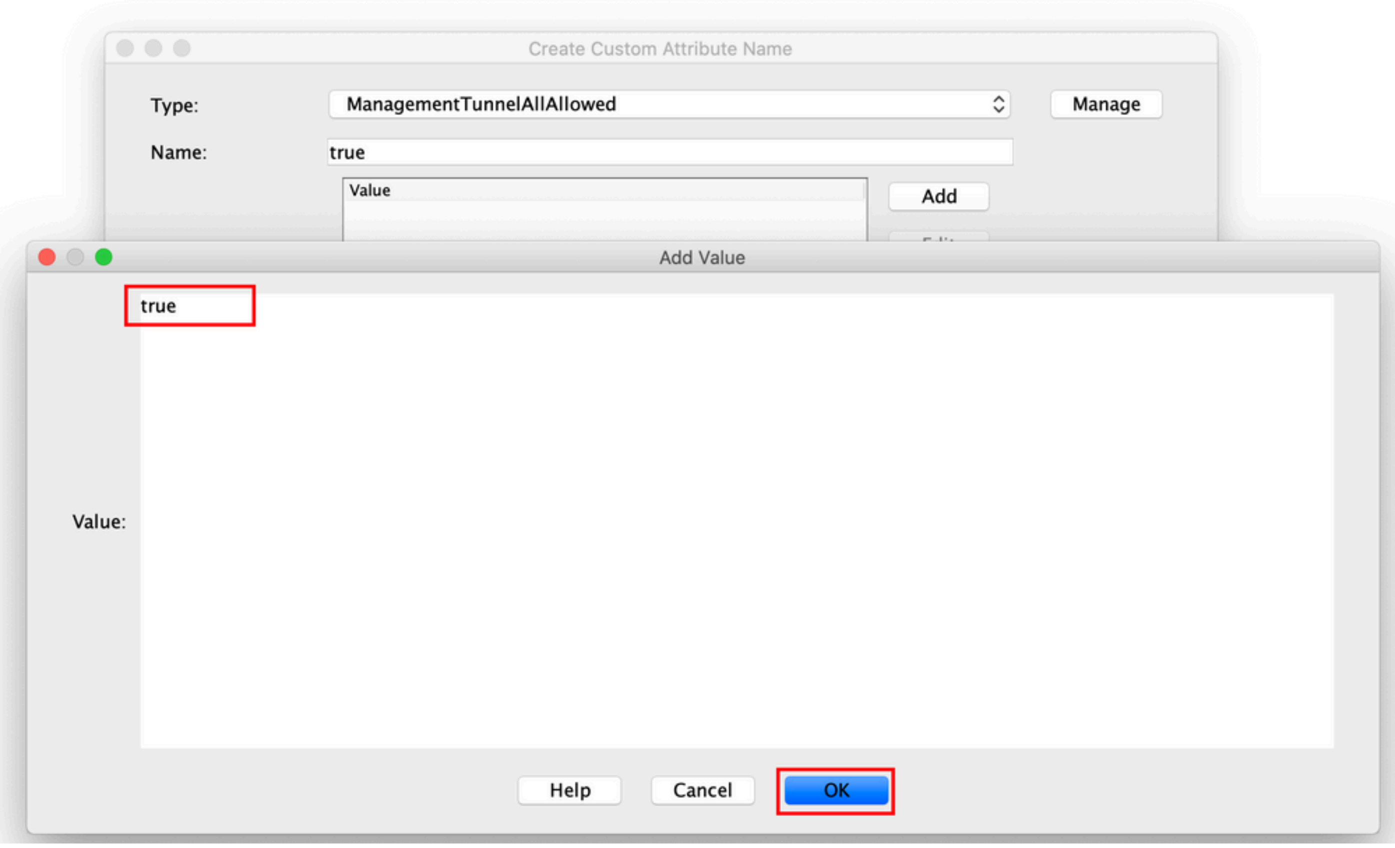

Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names
Add
Edit
Delete
Type
Name
Values
Create Custom Attribute Name
Manage
Value
Add
Edit
Delete
Configure Values:
Help
Cancel
OK

Declarations of custom attribute names and these attributes are enforced in AnyConnect group policy and AnyConnect dynamic access policy

Type: ManagementTunnelAllAllowed

Name: true

第五步：将值设置为 true.点击 OK,如图所示.

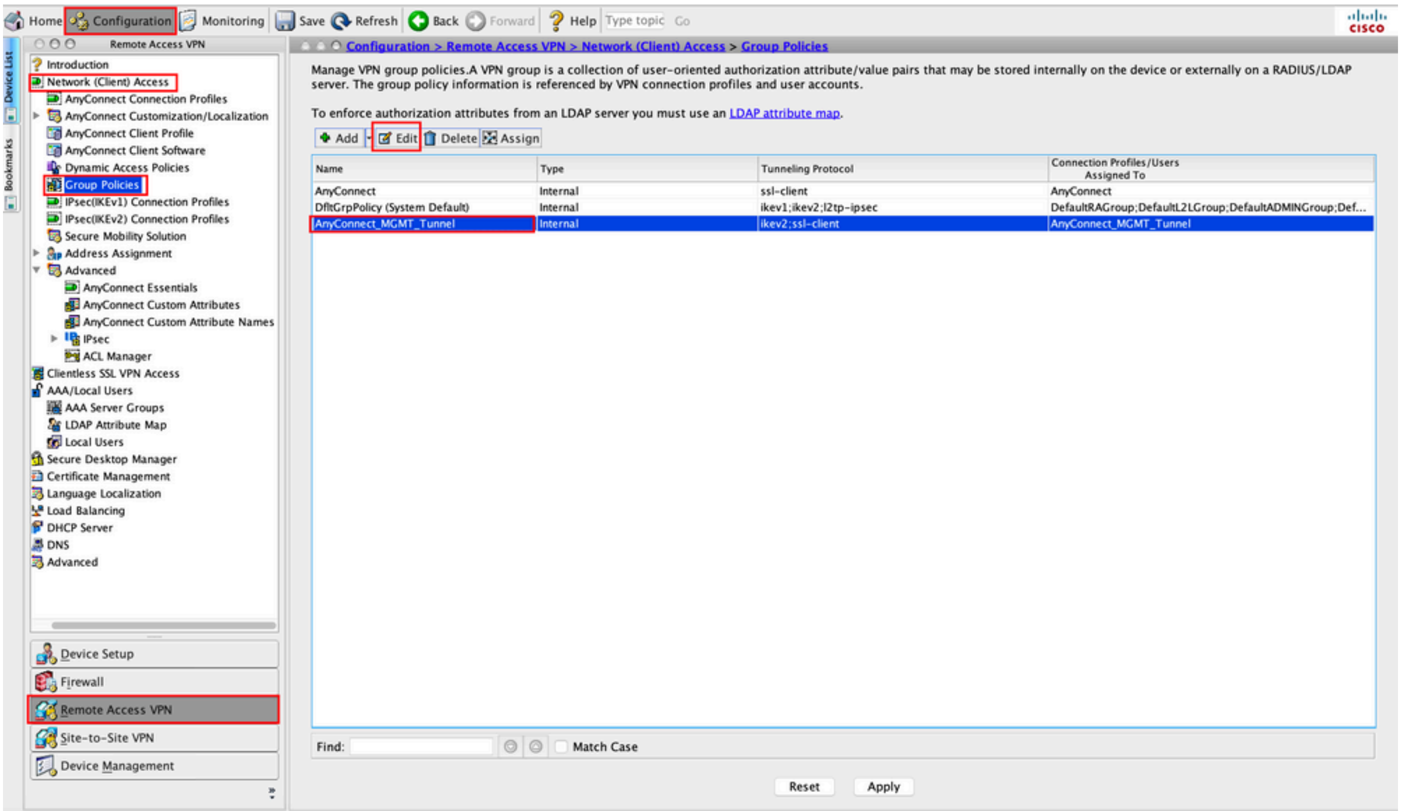


Type: ManagementTunnelAllAllowed

Name: true

Value: true

第六步：导航至 Configuration > Remote Access VPN > Network (Client) Access > Group Policies.选择Group Policy。点击 Edit ,如图所示.



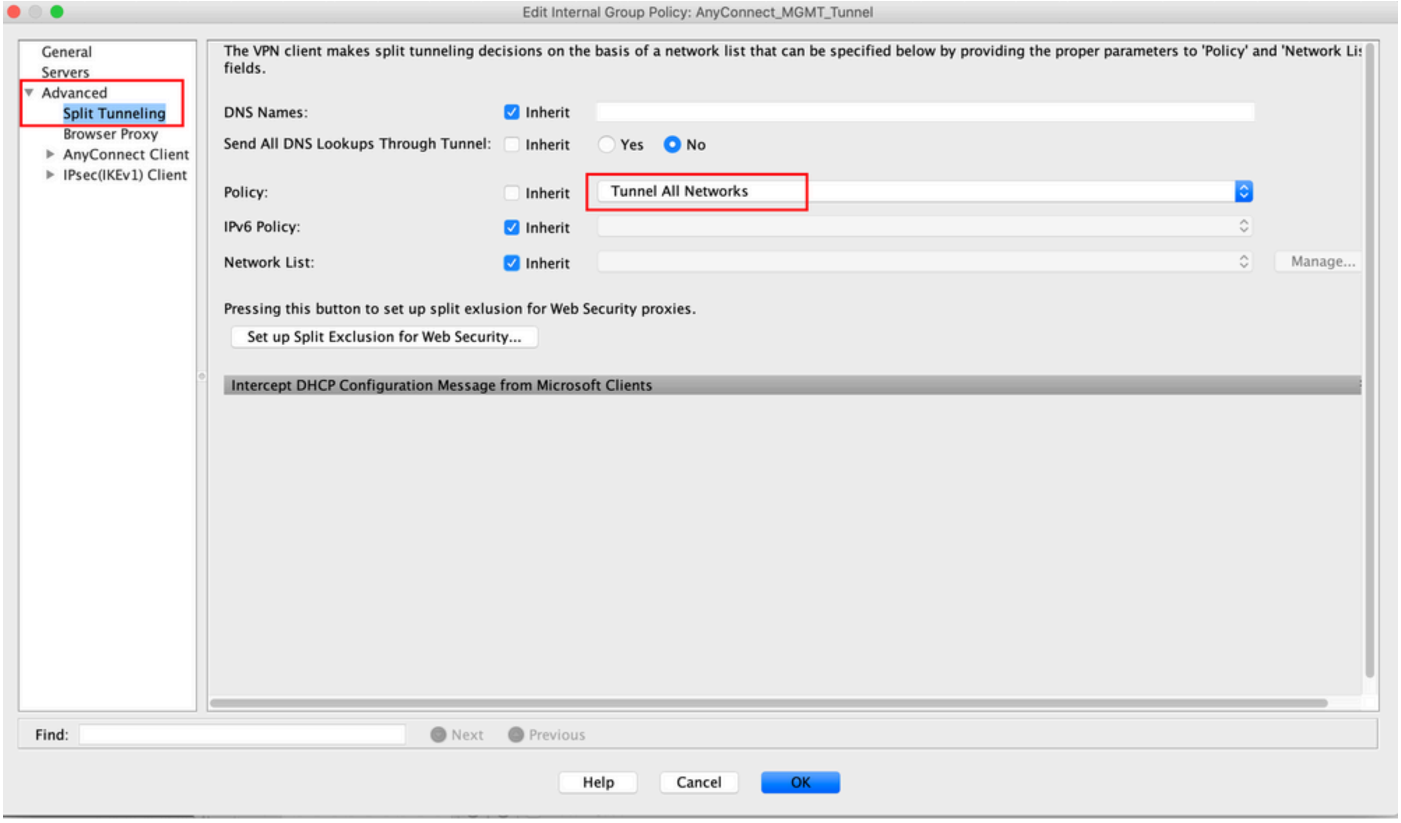
Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
AnyConnect	Internal	ssl-client	AnyConnect
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def...
AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel

步骤 7.如图所示，导航至 Advanced > Split Tunneling.将策略配置为 Tunnel All Networks.



Edit Internal Group Policy: AnyConnect_MGMT_Tunnel

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 Li: fields.

DNS Names: ☑ Inherit

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

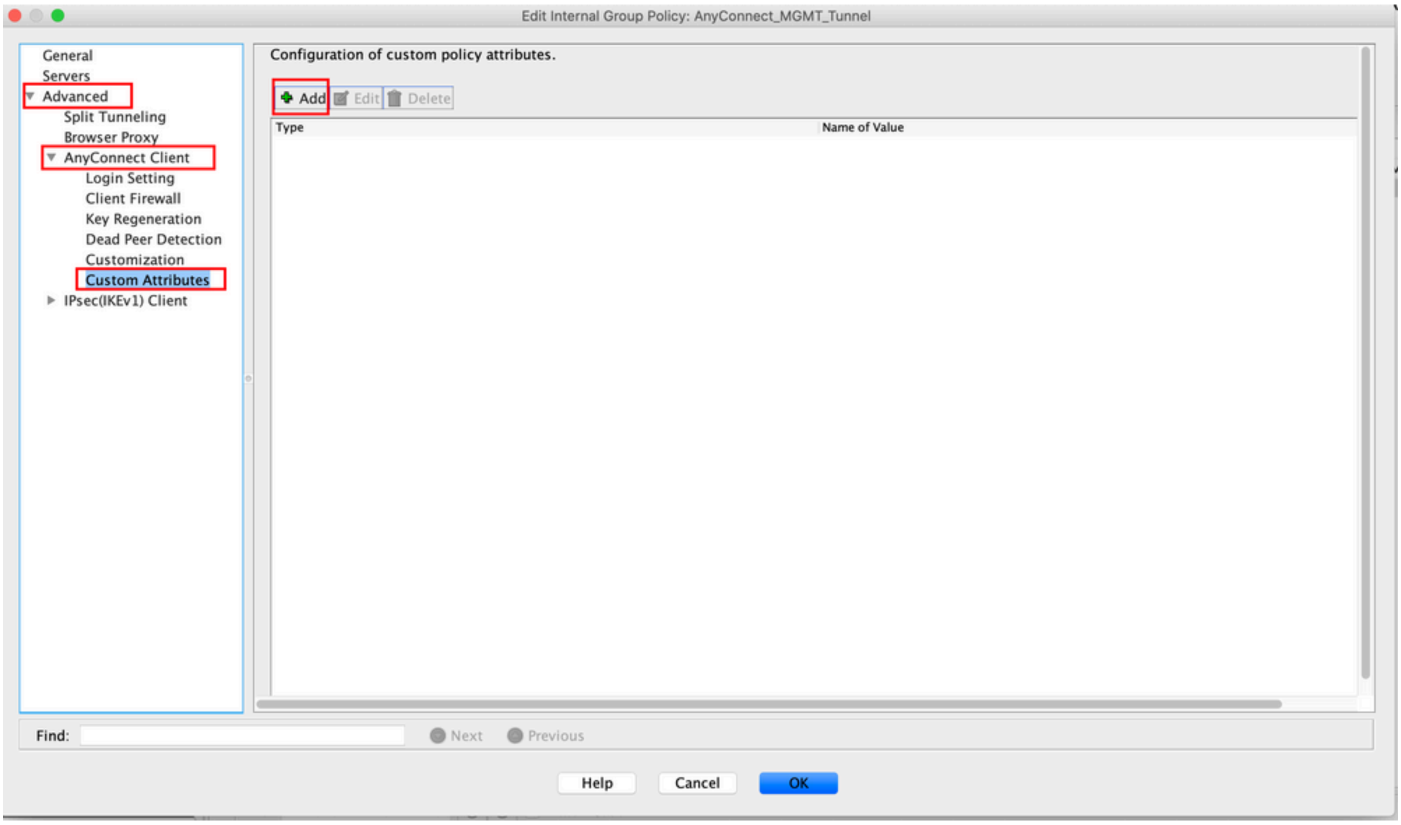
Policy: □ Inherit Tunnel All Networks

IPv6 Policy: ☑ Inherit

Network List: ☑ Inherit

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

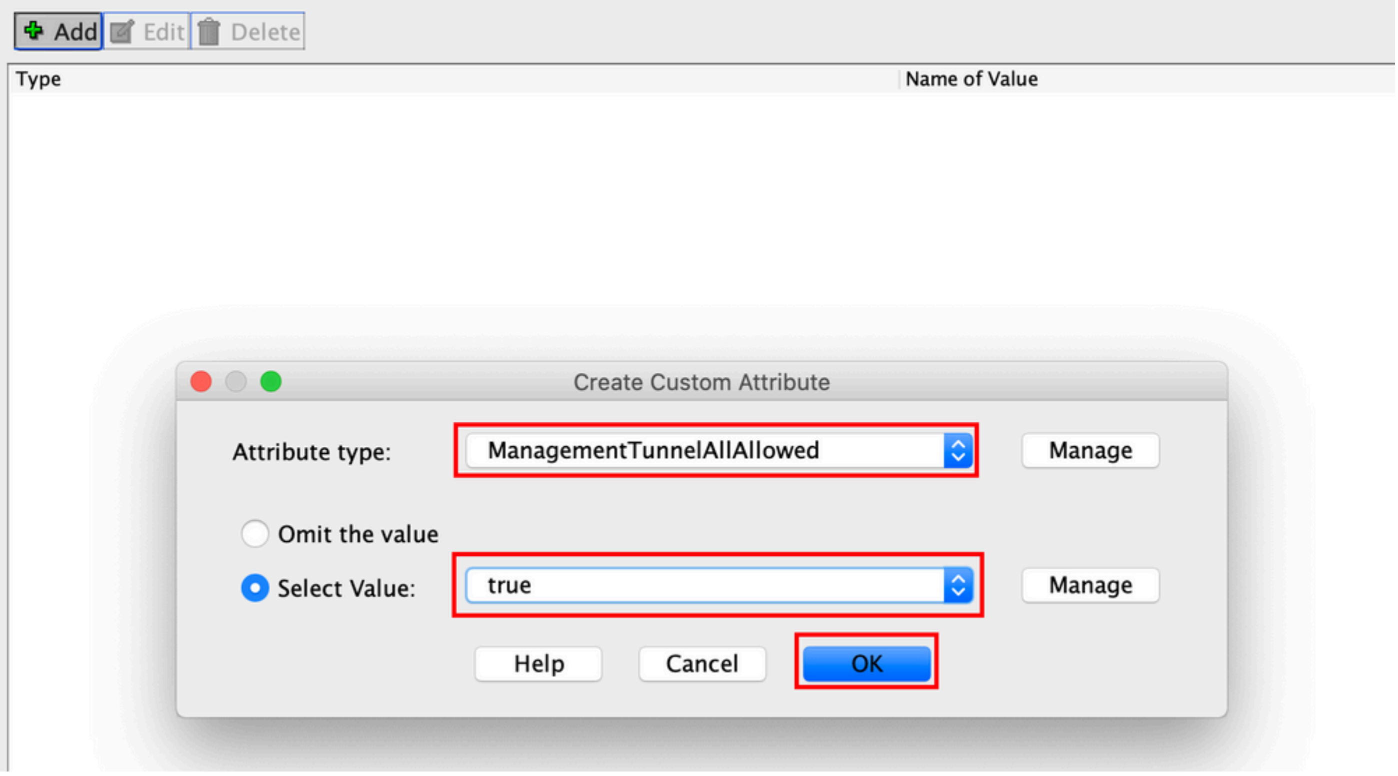
步骤 8导航至 Advanced > Anyconnect Client > Custom Attributes.点击 Add,如图所示.



Edit Internal Group Policy: AnyConnect_MGMT_Tunnel

Configuration of custom policy attributes.

步骤 9 选择属性类型作为 ManagementTunnelAllAllowed 并选择值作为 true.点击 OK,如图所示.

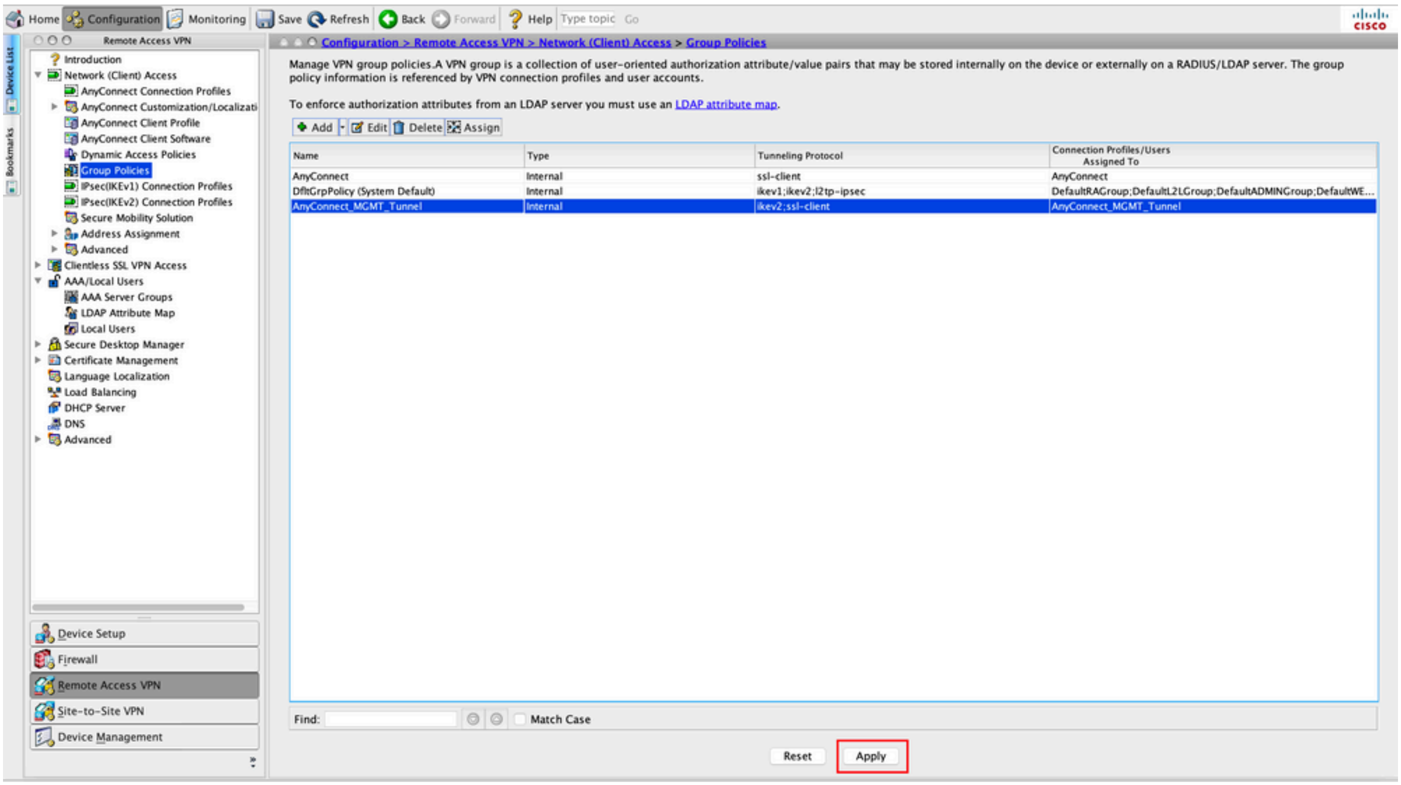


Attribute type: ManagementTunnelAllAllowed

○ Omit the value

● Select Value: true

步骤 10点击 Apply 将配置推送到ASA，如图所示。



Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
AnyConnect	Internal	ssl-client	AnyConnect
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE...
AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel

CLI配置 ManagementTunnelAllAllowed 添加自定义属性：

```
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
```

验证

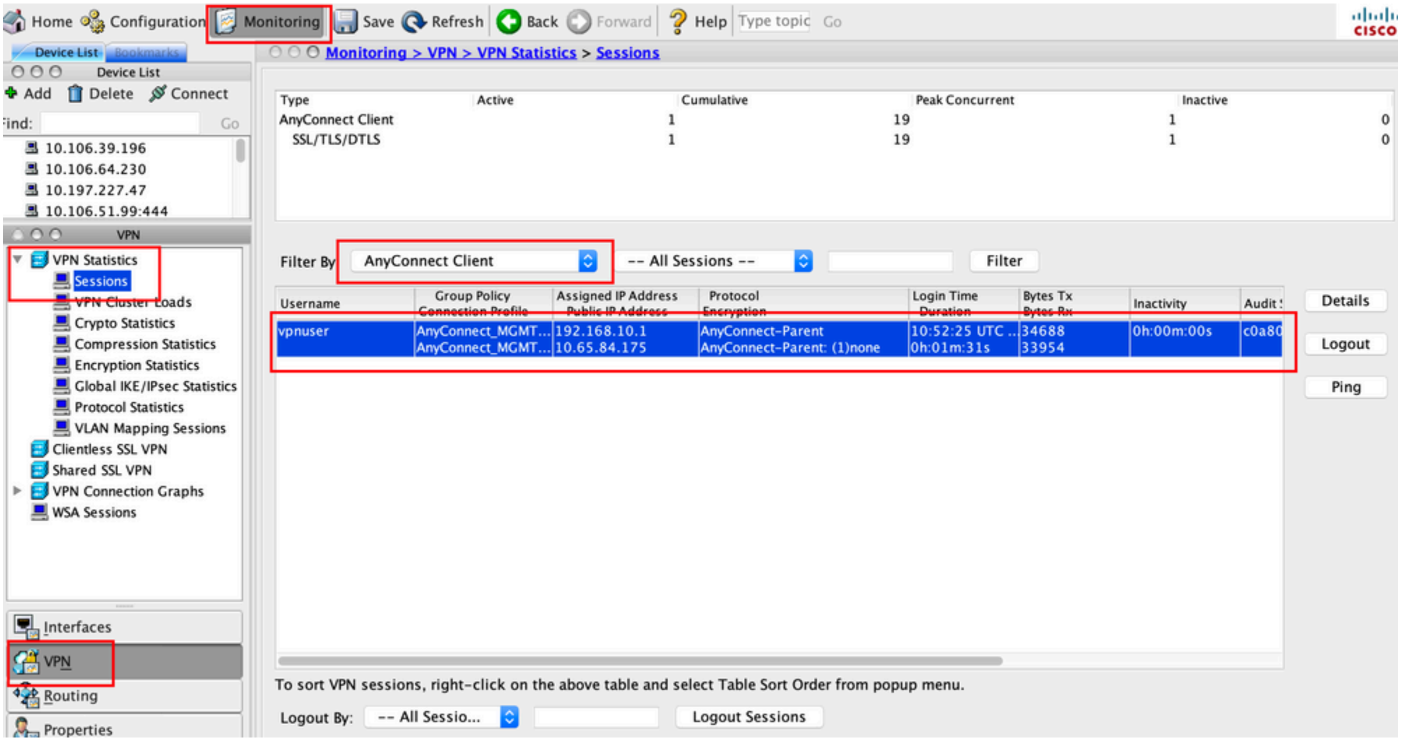
使用ASA CLI验证管理VPN隧道连接 show vpn-sessiondb detail anyconnect 命令。

```
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
```

验证ASDM上的管理VPN隧道连接。

导航到**Monitoring > VPN > VPN Statistics > Sessions**。按**AnyConnect客户端**过滤以查看客户端会话。



Monitoring > VPN > VPN Statistics > Sessions

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

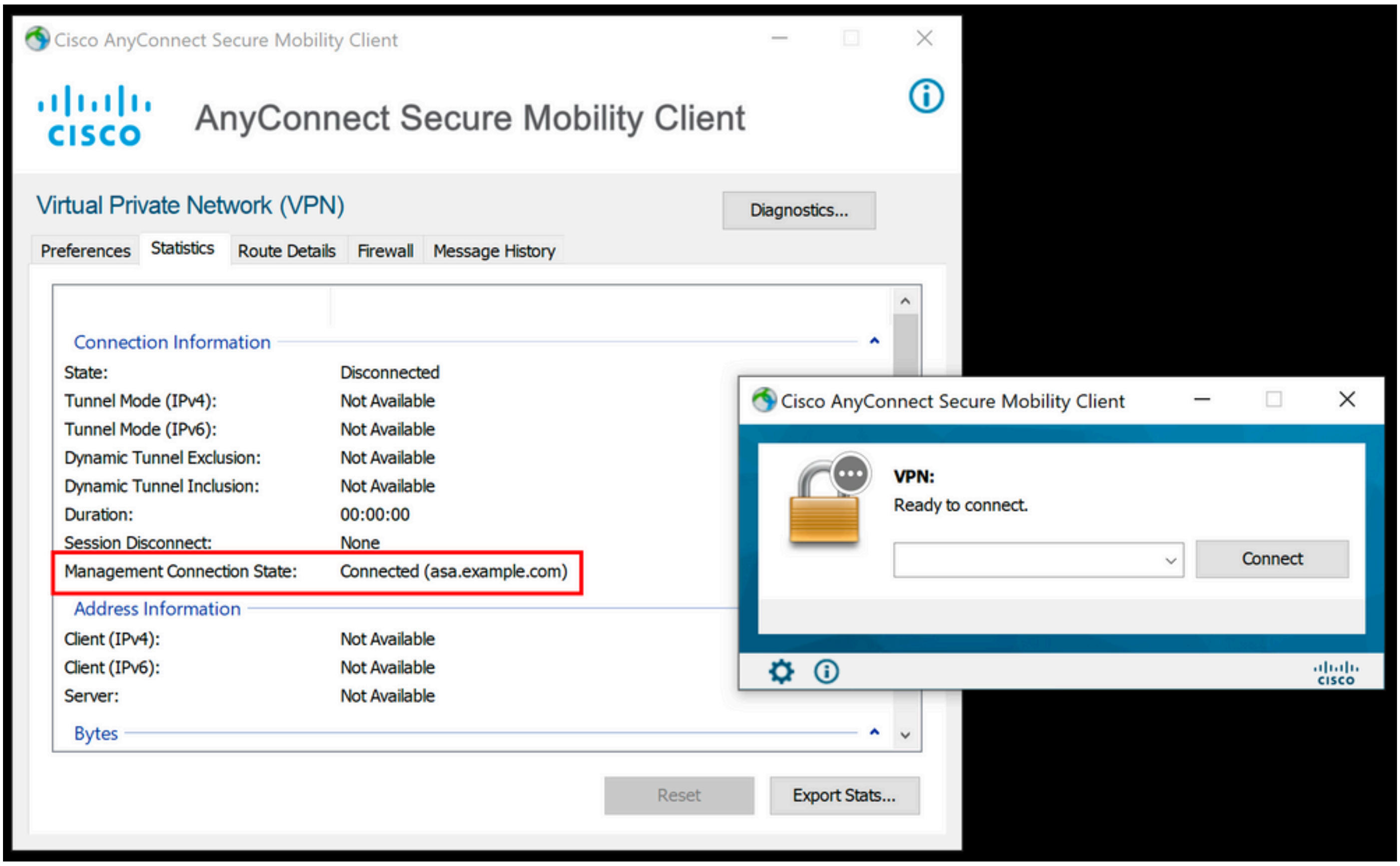
Filter By: AnyConnect Client | -- All Sessions -- | Filter

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

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

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

验证客户端计算机上的管理VPN隧道连接：


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History

Connection Information

State: Disconnected
Tunnel Mode (IPv4): Not Available
Tunnel Mode (IPv6): Not Available
Dynamic Tunnel Exclusion: Not Available
Dynamic Tunnel Inclusion: Not Available
Duration: 00:00:00
Session Disconnect: None
Management Connection State: Connected (asa.example.com)

Address Information

Client (IPv4): Not Available
Client (IPv6): Not Available
Server: Not Available

Bytes

VPN:
Ready to connect.

故障排除

新的UI统计行（管理连接状态）可用于排除管理隧道连接问题的故障。以下是常见的错误状态：

已断开连接（禁用）：

- 此功能已禁用。
- 确保管理VPN配置文件已通过用户隧道连接（要求您将管理VPN配置文件添加到用户隧道组策略）部署至客户端，或通过手动上传配置文件实现带外部署。
- 确保管理VPN配置文件配置有包含隧道组的单个主机条目。

已断开连接（受信任网络）：

- TND检测到受信任网络，因此未建立管理隧道。

已断开连接（用户隧道处于活动状态）：

- 用户VPN隧道当前处于活动状态。

已断开连接（进程启动失败）：

- 尝试管理隧道连接时遇到进程启动失败。

已断开连接（连接失败）：

- 建立管理隧道时遇到连接故障。
- 确保证书身份验证在隧道组中配置，组策略中不存在标语，并且服务器证书必须受信任。

已断开连接（无效的VPN配置）：

- 从VPN服务器收到无效的拆分隧道配置。
- 检查管理隧道组策略中的拆分隧道配置。

已断开连接（软件更新挂起）：

- AnyConnect软件更新当前处于挂起状态。

已断开连接：

- 管理隧道即将建立或由于其他原因无法建立。

收集DART以进一步排除故障。

相关信息

- 管理VPN隧道的配置
- 管理VPN隧道故障排除
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。