Konfigurieren des AnyConnect Management-VPN-Tunnel auf der ASA

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie eine ASA konfiguriert wird, wenn das VPN-Gateway Verbindungen vom Cisco AnyConnect Secure Mobility Client über den Management-VPN-Tunnel akzeptiert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- VPN-Konfiguration durch Adaptive Security Device Manager (ASDM)
- Grundlegende CLI-Konfiguration der Adaptive Security Appliance (ASA)
- X509-Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ASA Software Version 9.12(3)9
- Cisco ASDM Software Version 7.12.2

- Windows 10 mit Cisco AnyConnect Secure Mobility Client der Version 4.8.03036

  Hinweis: Laden Sie das AnyConnect VPN Web Deployment-Paket herunter (anyconnect-win*.pkg or anyconnect-macos*.pkg) aus dem Cisco Software Download (nur registrierte Kunden). Kopieren Sie den AnyConnect VPN-Client in den Flash-Speicher der ASA, die auf die Computer der Remote-Benutzer heruntergeladen werden soll, um die SSL VPN-Verbindung mit der ASA herzustellen. Weitere Informationen finden Sie im Abschnitt Installing the AnyConnect Client (Installieren des AnyConnect-Clients) im ASA-Konfigurationsleitfaden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Ein Management-VPN-Tunnel stellt die Verbindung zum Unternehmensnetzwerk sicher, wenn das Client-System hochgefahren wird, nicht nur, wenn der Endbenutzer eine VPN-Verbindung herstellt. Sie können das Patch-Management auf Endgeräten außerhalb des Büros durchführen, insbesondere auf Geräten, die vom Benutzer nur selten über VPN mit dem Büronetzwerk verbunden werden. Auch Betriebssystem-Anmeldeskripts für Endgeräte, die eine Verbindung mit dem Unternehmensnetzwerk benötigen, profitieren von dieser Funktion.

AnyConnect Management Tunnel ermöglicht es Administratoren, AnyConnect ohne Benutzereingriff anzuschließen, bevor sich der Benutzer anmeldet. Der AnyConnect Management-Tunnel kann zusammen mit der Erkennung vertrauenswürdiger Netzwerke eingesetzt werden und wird daher nur ausgelöst, wenn das Endgerät extern installiert und von einem benutzerinitiierten VPN getrennt ist. Der AnyConnect Management-Tunnel ist für den Endbenutzer transparent und trennt die Verbindung automatisch, wenn der Benutzer das VPN initiiert.

Betriebssystem/Anwendung	Mindestversionsanforderungen
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect-Version	4.7.00136
macOS AnyConnect-Version	4.7.01076
Linux	Nicht unterstützt

Betrieb eines Management-Tunnels

Der AnyConnect VPN-Agentendienst wird beim Systemstart automatisch gestartet. Es erkennt, dass die Management-Tunnel-Funktion aktiviert ist (über das Management-VPN-Profil), und startet daher die Management-Client-Anwendung, um eine Management-Tunnel-Verbindung zu initiieren. Die Management-Client-Anwendung verwendet den Hosteintrag aus dem Management-VPN-Profil, um die Verbindung zu initiieren. Dann wird wie üblich der VPN-Tunnel aufgebaut, mit einer Ausnahme: Während einer Management-Tunnel-Verbindung wird kein Software-Update durchgeführt, da der Management-Tunnel für den Benutzer transparent sein soll.

Der Benutzer initiiert über die AnyConnect-Benutzeroberfläche einen VPN-Tunnel, der die Beendigung des Management-Tunnels auslöst. Nach der Beendigung des Management-Tunnels wird die Einrichtung des Benutzertunnels wie gewohnt fortgesetzt.

Der Benutzer trennt den VPN-Tunnel, wodurch die automatische Wiederherstellung des Management-Tunnels ausgelöst wird.

Einschränkungen

- Es wird keine Benutzerinteraktion unterstützt
- Es wird nur die zertifikatbasierte Authentifizierung über den Machine Certificate Store (Windows) unterstützt
- Die strenge Überprüfung des Serverzertifikats wird erzwungen
- Ein privater Proxy wird nicht unterstützt.
- Ein öffentlicher Proxy wird nicht unterstützt (ProxyNative-Wert wird auf Plattformen unterstützt, auf denen die Einstellungen des systemeigenen Proxys nicht vom Browser abgerufen werden)
- AnyConnect-Anpassungsskripte werden nicht unterstützt

Hinweis: Weitere Informationen finden Sie unter Informationen zum Management-VPN-Tunnel.

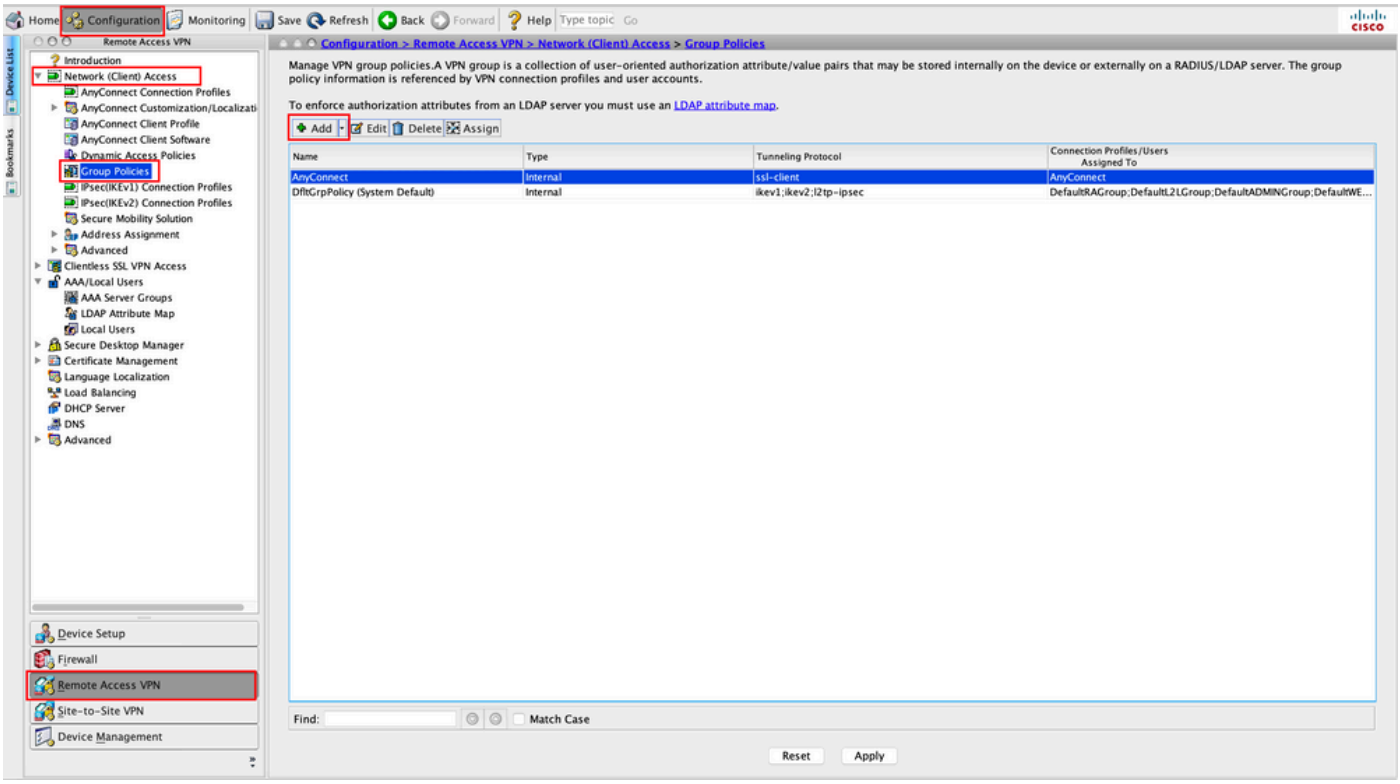
Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie Cisco ASA als VPN-Gateway konfigurieren, um Verbindungen von AnyConnect-Clients über den Management-VPN-Tunnel zu akzeptieren.

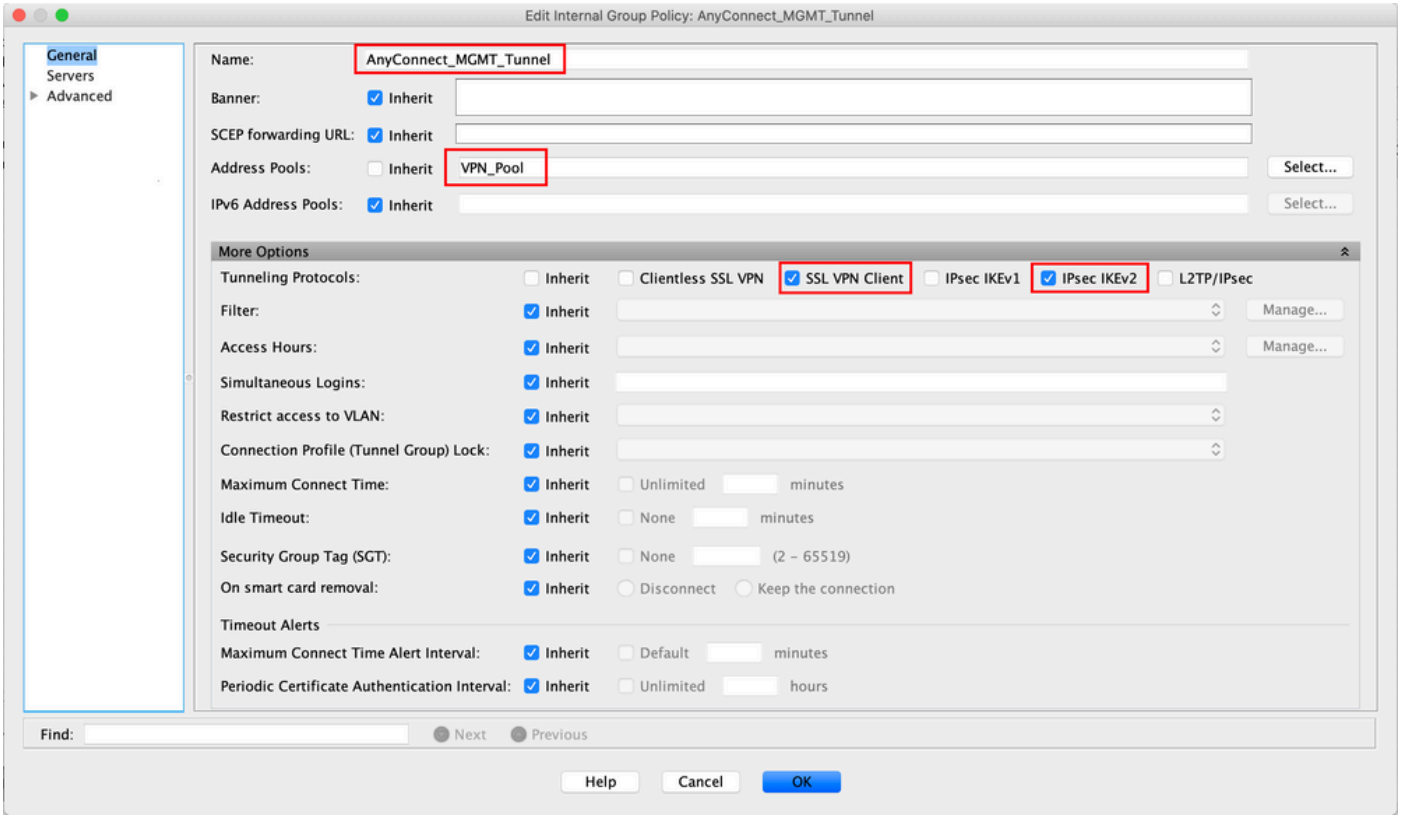
Konfiguration auf der ASA über ASDM/CLI

Schritt 1: Erstellen Sie die AnyConnect-Gruppenrichtlinie. Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Klicken Sie auf Add.

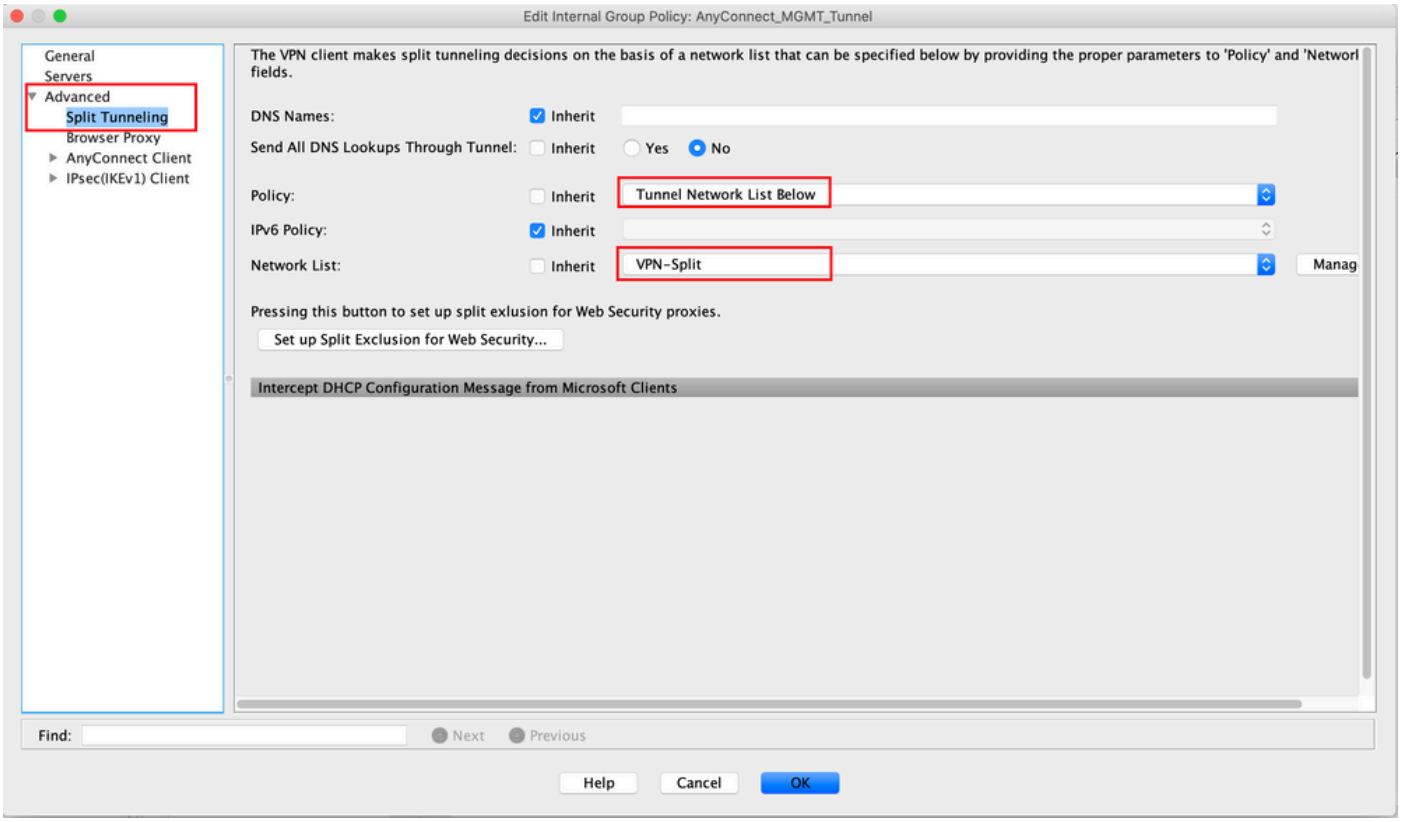
Hinweis: Es wird empfohlen, eine neue AnyConnect-Gruppenrichtlinie zu erstellen, die nur für den AnyConnect-Management-Tunnel verwendet wird.



Schritt 2: Bieten Sie Name für die Gruppenrichtlinie. Zuweisen/Erstellen eines Address Pool. Auswählen Tunneling Protocols als SSL VPN Client und/oder IPsec IKEv2, wie im Bild dargestellt.

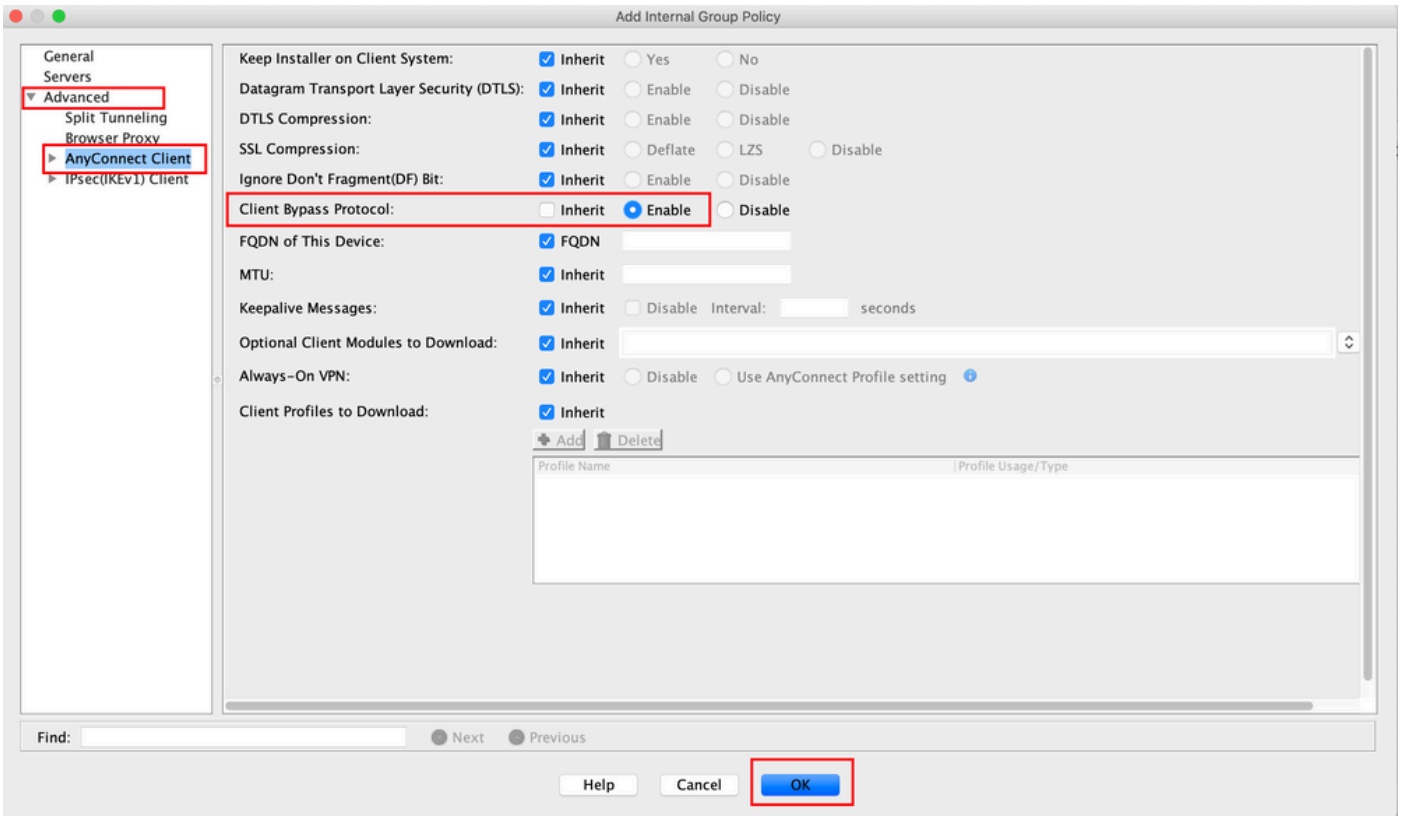


Schritt 3: Navigieren Sie zu Advanced > Split Tunneling. Konfigurieren Sie Policy als Tunnel Network List Below und wählen Sie Network List, wie im Bild dargestellt.

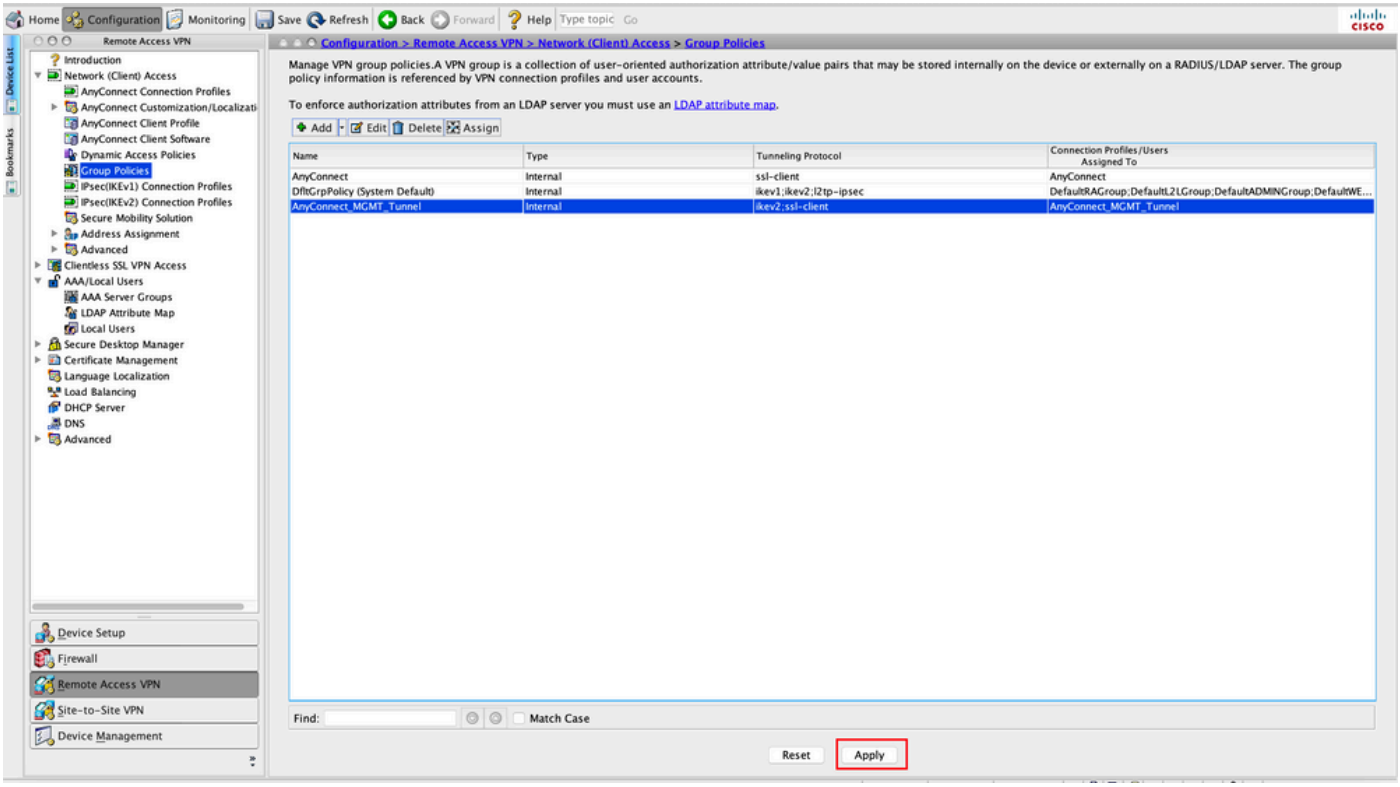


Hinweis: Wenn für beide IP-Protokolle (IPv4 und IPv6) keine Client-Adresse angefordert wird, **Client Bypass Protocol** Einstellung muss enabled sodass der entsprechende Datenverkehr nicht durch den Management-Tunnel unterbrochen wird. Weitere Informationen zur Konfiguration finden Sie in Schritt 4.

Schritt 4: Navigieren Sie zu Advanced > AnyConnect Client. Festlegen Client Bypass Protocol zu Enable. Klicken Sie auf OK um zu speichern, wie im Bild gezeigt.



Schritt 5: Klicken Sie wie in dieser Abbildung dargestellt auf Apply um die Konfiguration an die ASA weiterzuleiten.

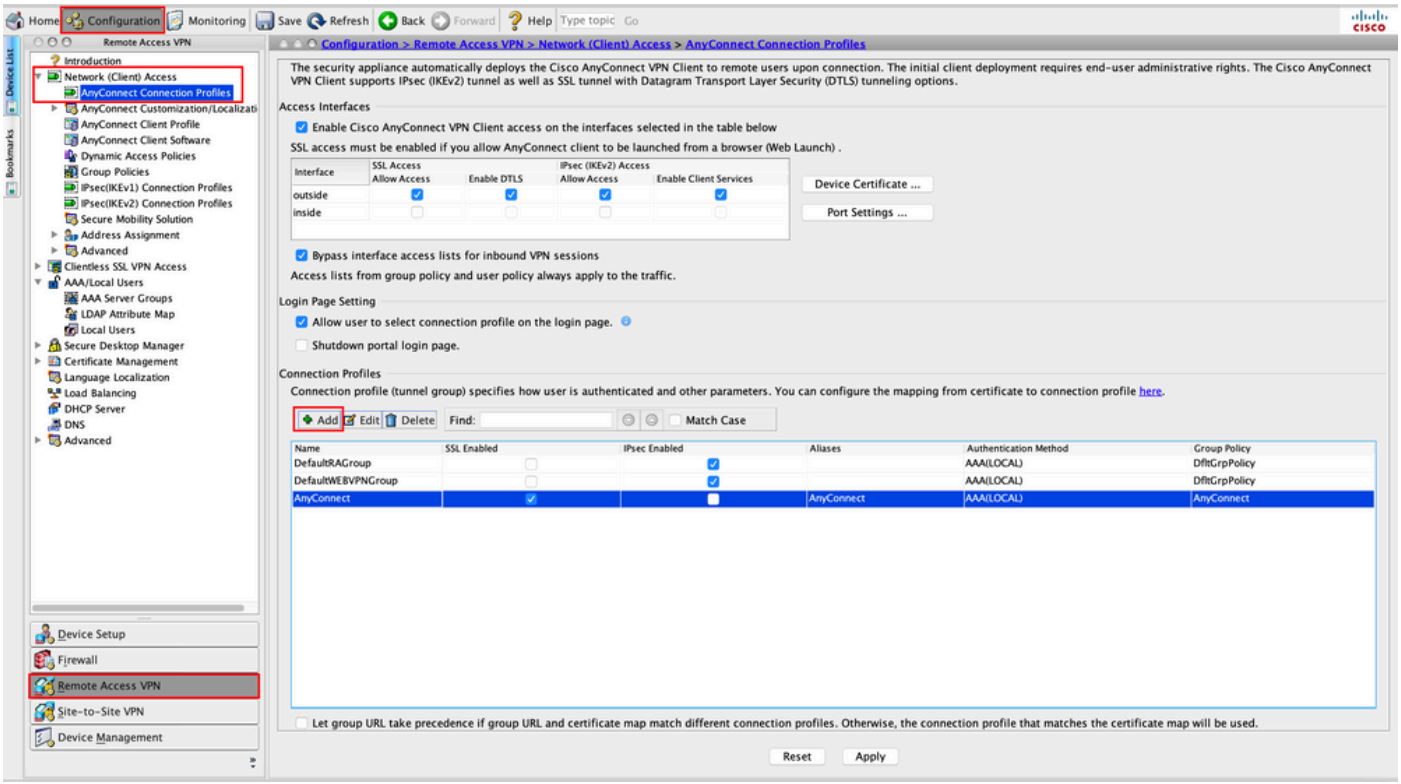


CLI-Konfiguration für die Gruppenrichtlinie:

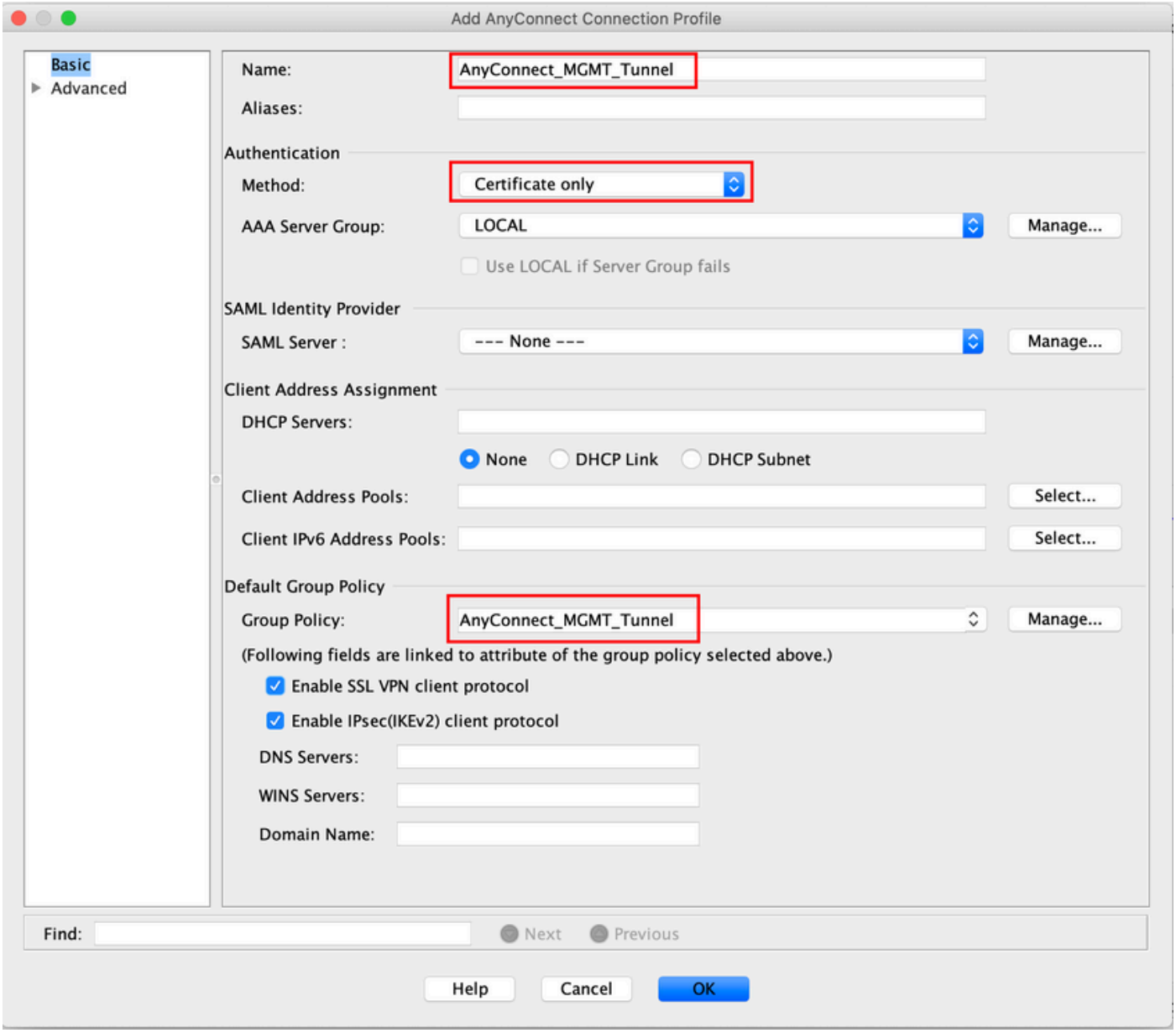
```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
```

Schritt 6: Erstellen Sie das AnyConnect-Verbindungsprofil. Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Klicken Sie auf Add.

> **Hinweis:** Es wird empfohlen, ein neues AnyConnect-Verbindungsprofil zu erstellen, das nur für den AnyConnect-Management-Tunnel verwendet wird.



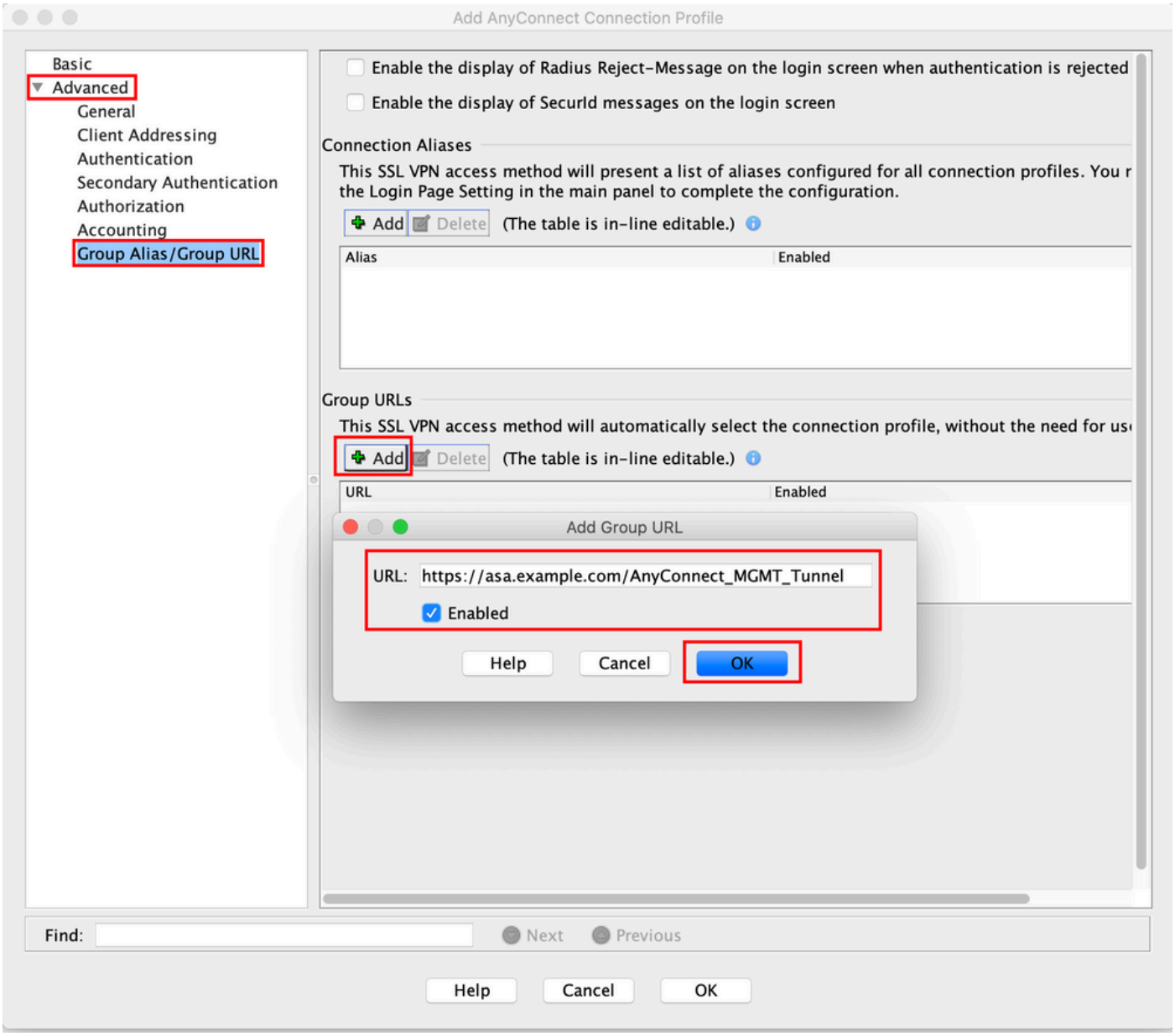
Schritt 7. Bieten Sie Name für das Verbindungsprofil, und legen Sie Authentication Method als Certificate only. Wählen Sie Group Policy wie in Schritt 1 erstellt.



Hinweis: Stellen Sie sicher, dass das Stammzertifikat der lokalen Zertifizierungsstelle (Certificate Authority, kurz „CA“) auf der ASA vorhanden ist. Navigieren Sie zu Configuration > Remote Access VPN > Certificate Management > CA Certificates um das Zertifikat hinzuzufügen/anzuzeigen.

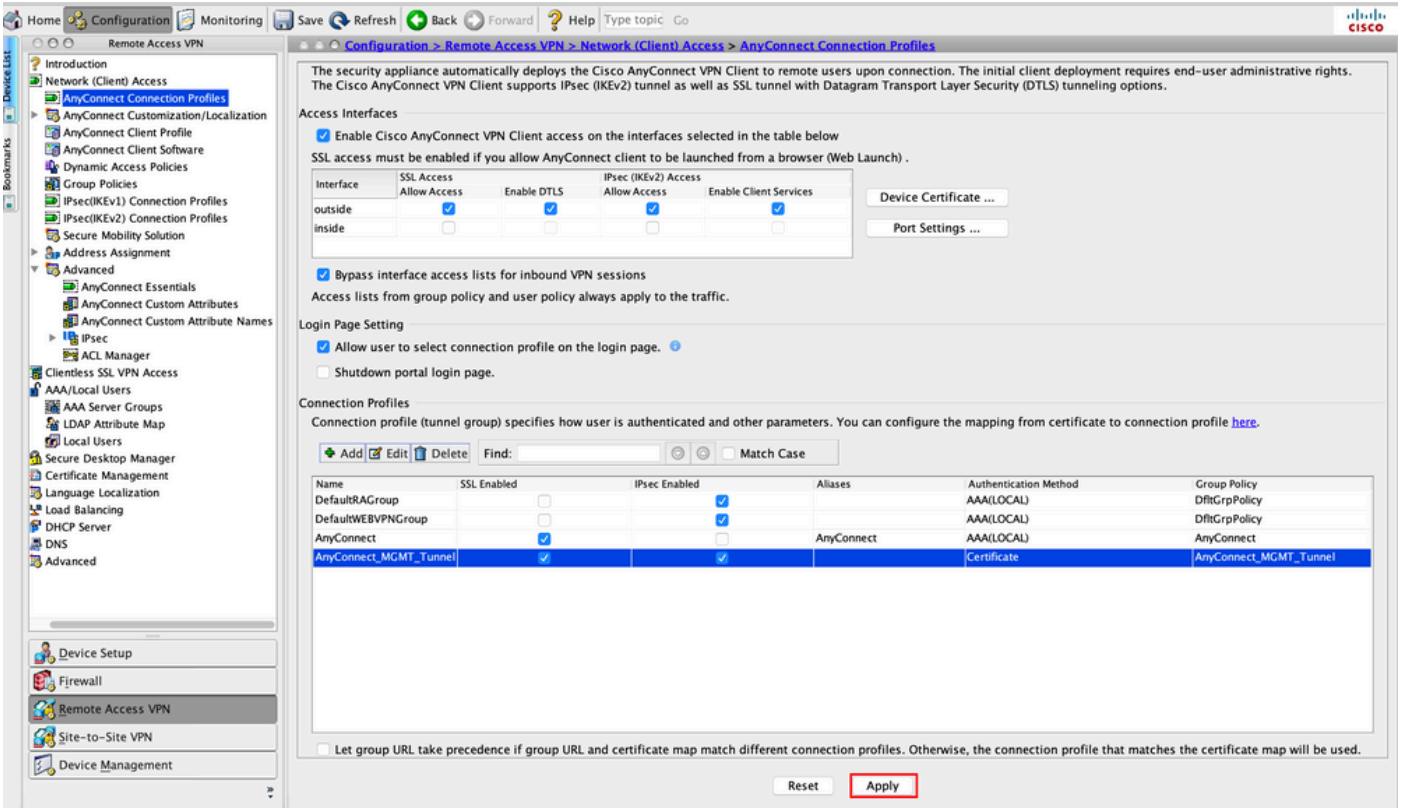
Hinweis: Stellen Sie sicher, dass ein Identitätszertifikat, das von derselben lokalen CA ausgestellt wurde, im Machine Certificate Store (unter Windows) und/oder in der Keychain-Verwaltung des Systems (unter macOS) vorhanden ist.

Schritt 8: Navigieren Sie zu Advanced > Group Alias/Group URL. Klicken Sie auf Add unter Group URLs und eine URL. Sicher Enabled ist aktiviert. Klicken Sie auf OK um zu speichern, wie im Bild gezeigt.



Wenn IKEv2 verwendet wird, stellen Sie sicher, IPsec (IKEv2) Access ist auf der für AnyConnect verwendeten Schnittstelle aktiviert.

Schritt 9. Klicken Sie auf Apply um die Konfiguration an die ASA weiterzuleiten.

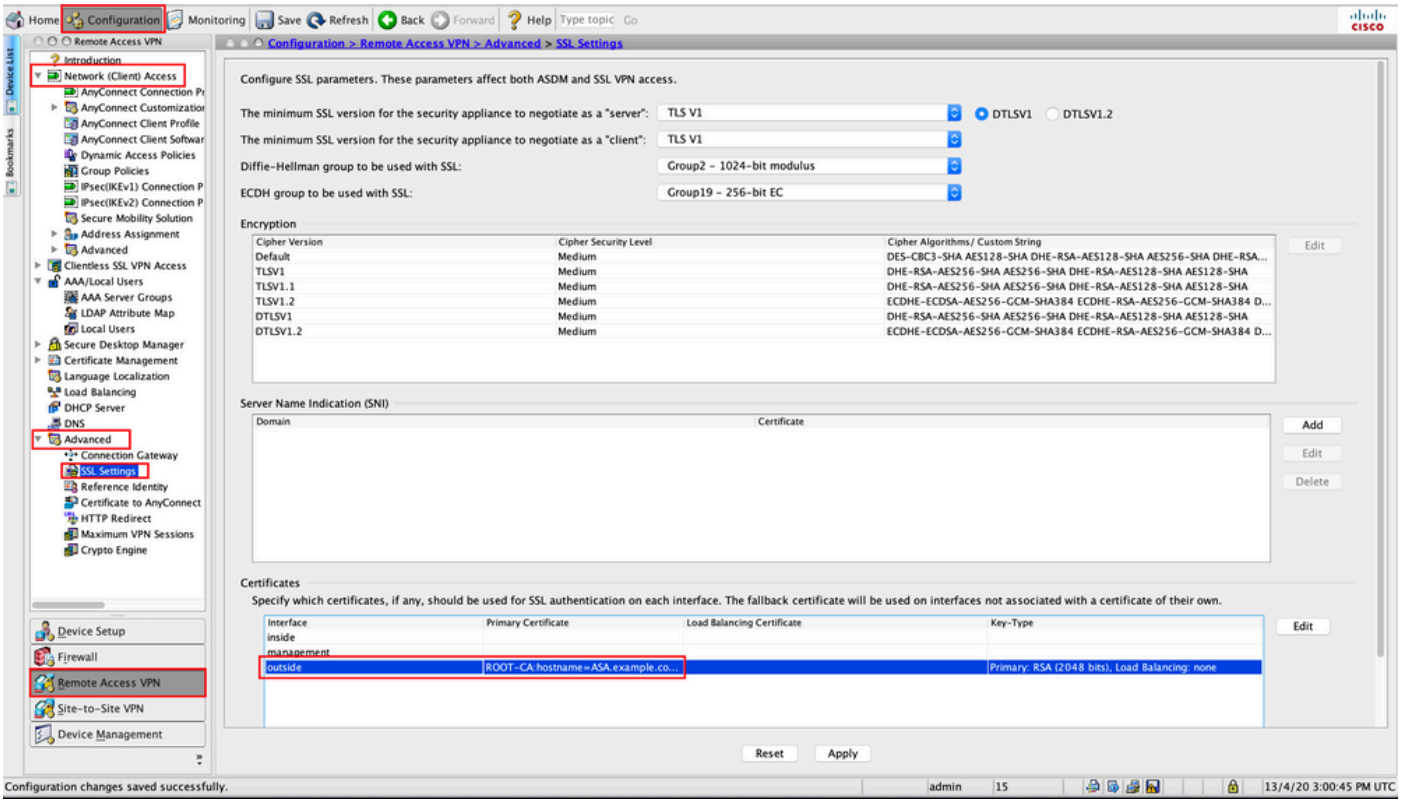


CLI-Konfiguration für das Verbindungsprofil (tunnel-group):

```
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
```

Schritt 10. Stellen Sie sicher, dass ein vertrauenswürdiges Zertifikat auf der ASA installiert und an die für AnyConnect-Verbindungen verwendete Schnittstelle gebunden ist. Navigieren Sie zu Configuration > Remote Access VPN > Advanced > SSL Settings um diese Einstellung hinzuzufügen/anzuzeigen.

> **Hinweis:** Weitere Informationen finden Sie unter Installation des Identitätszertifikats auf der ASA.

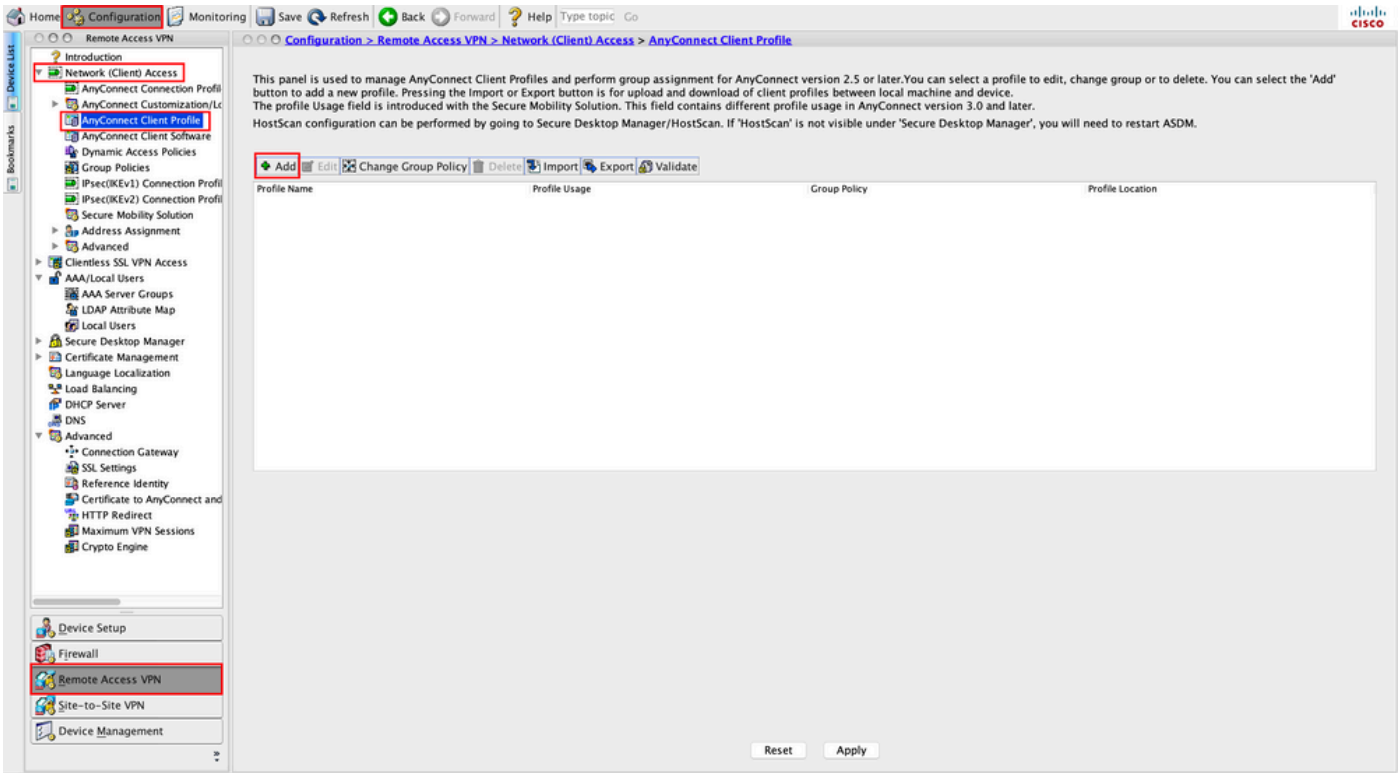


CLI-Konfiguration für SSL-Trustpoint:

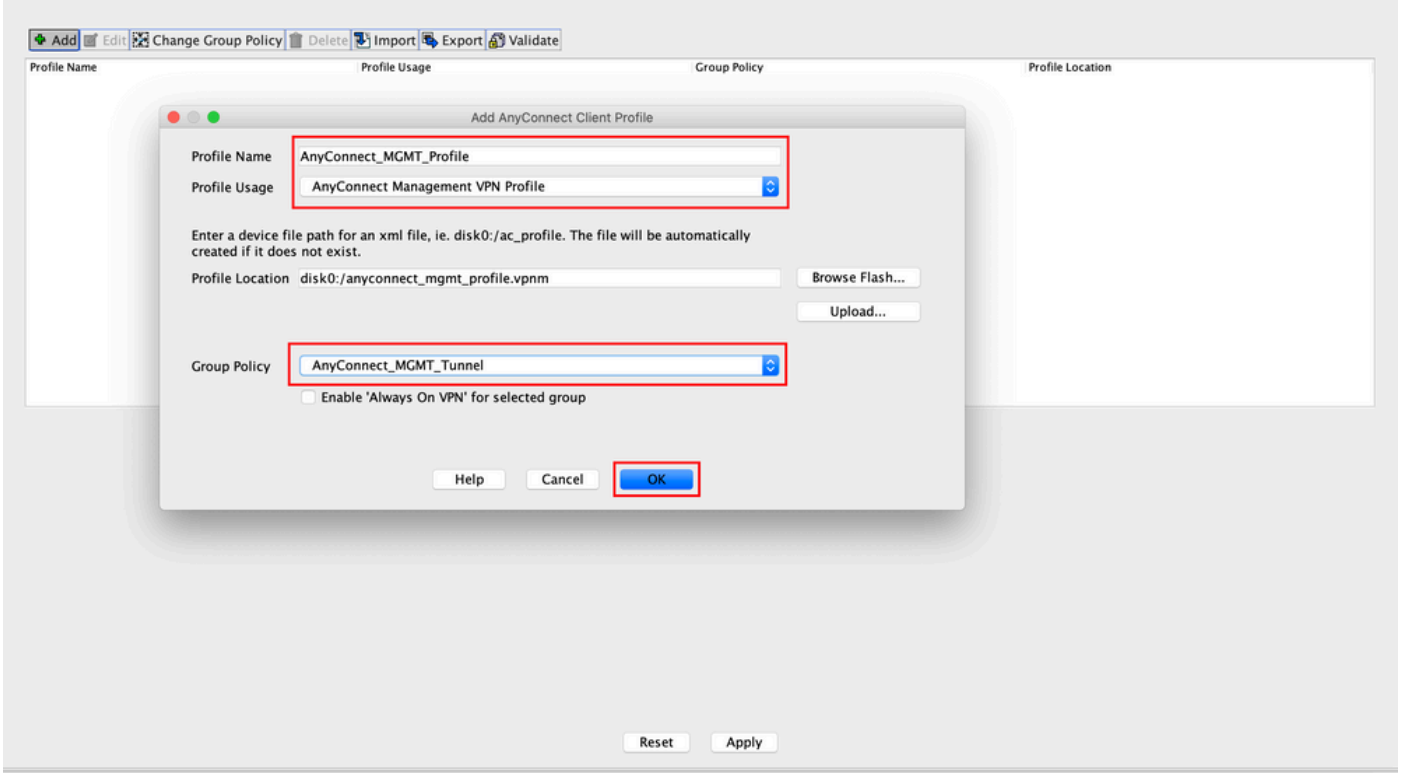
```
ssl trust-point ROOT-CA outside
```

Erstellung des AnyConnect-Management-VPN-Profils

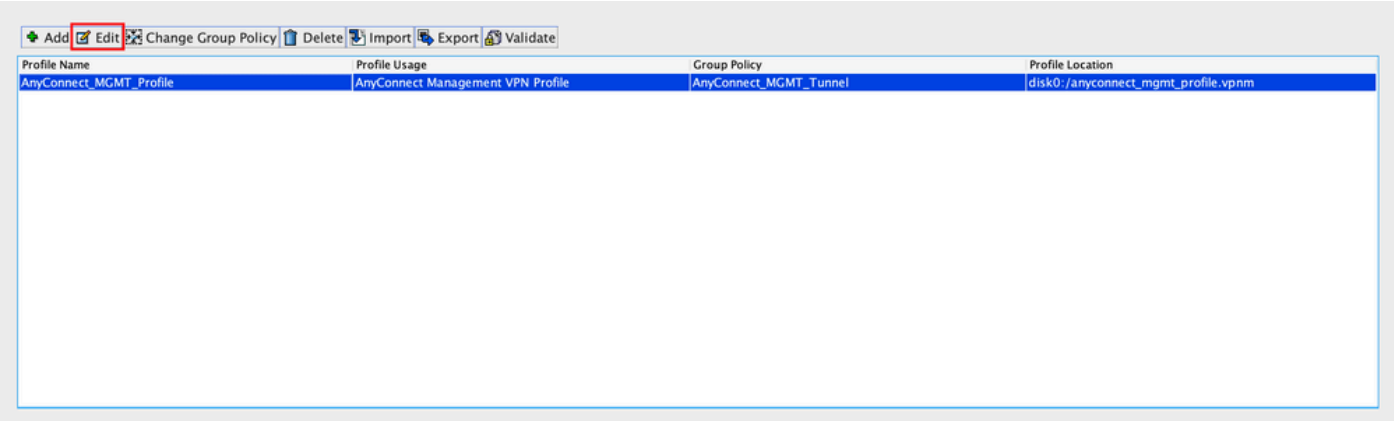
Schritt 1: Erstellen Sie das AnyConnect-Client-Profil. Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Klicken Sie auf Add, wie im Bild dargestellt.



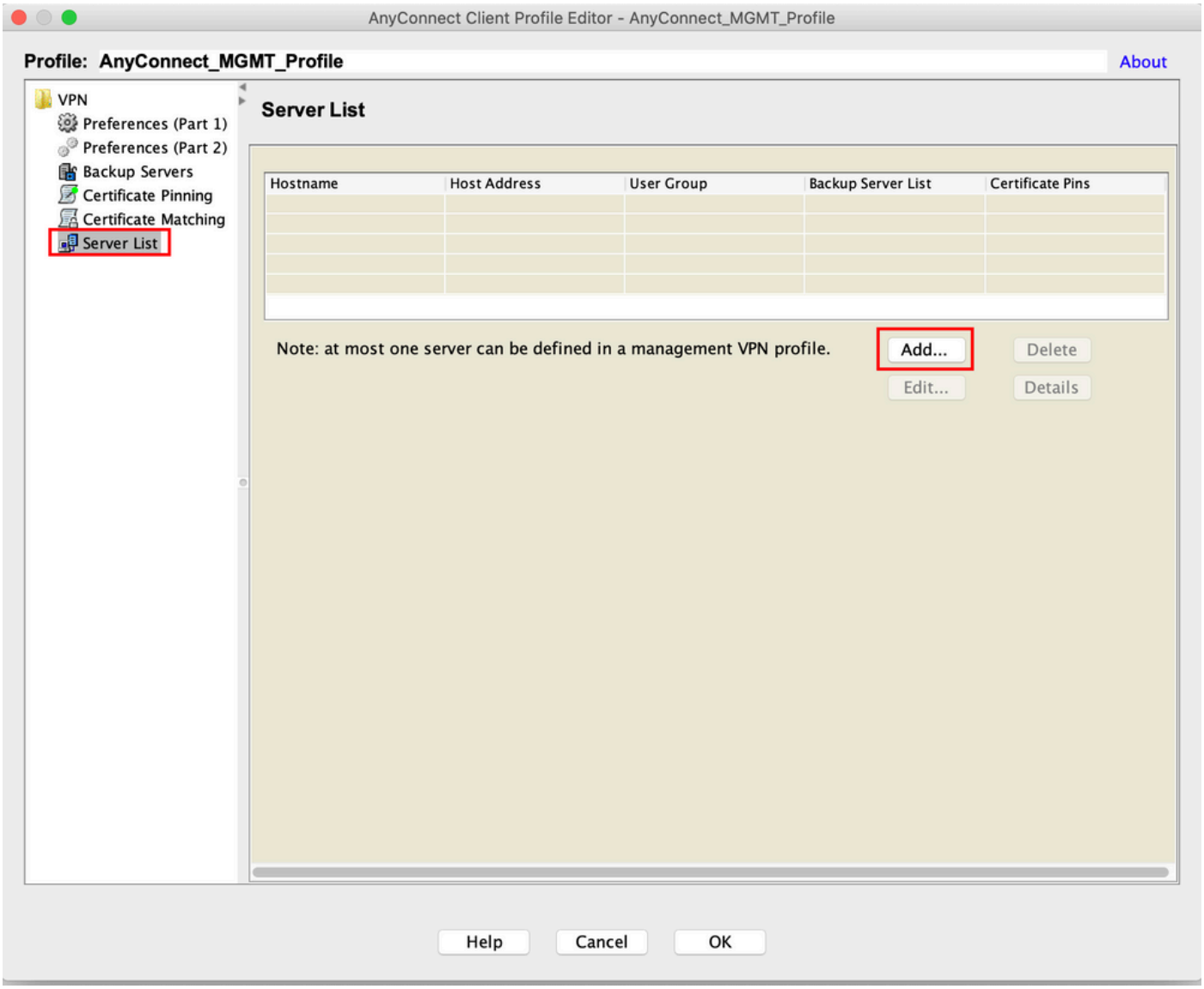
Schritt 2: Bieten Sie Profile Name. Wählen Sie Profile Usage als AnyConnect Management VPN profile. Wählen Sie Group Policy in Schritt 1 erstellt. Klicken Sie auf OK , wie im Bild dargestellt.



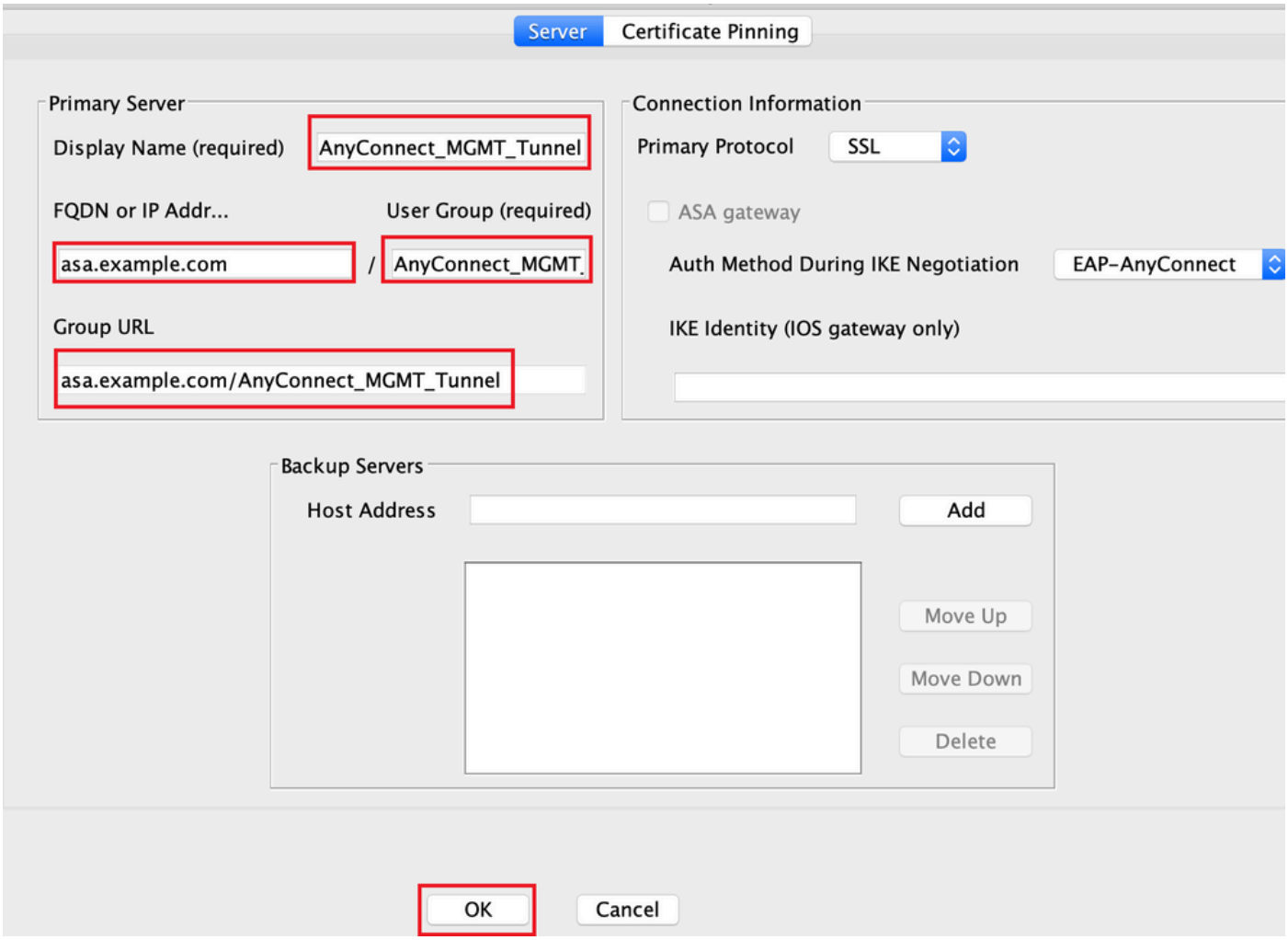
Schritt 3: Wählen Sie das erstellte Profil aus, und klicken Sie auf Edit, wie im Bild dargestellt.



Schritt 4: Navigieren Sie zu Server List. Klicken Sie auf Add um einen neuen Server-Listeneintrag hinzuzufügen, wie im Bild gezeigt.



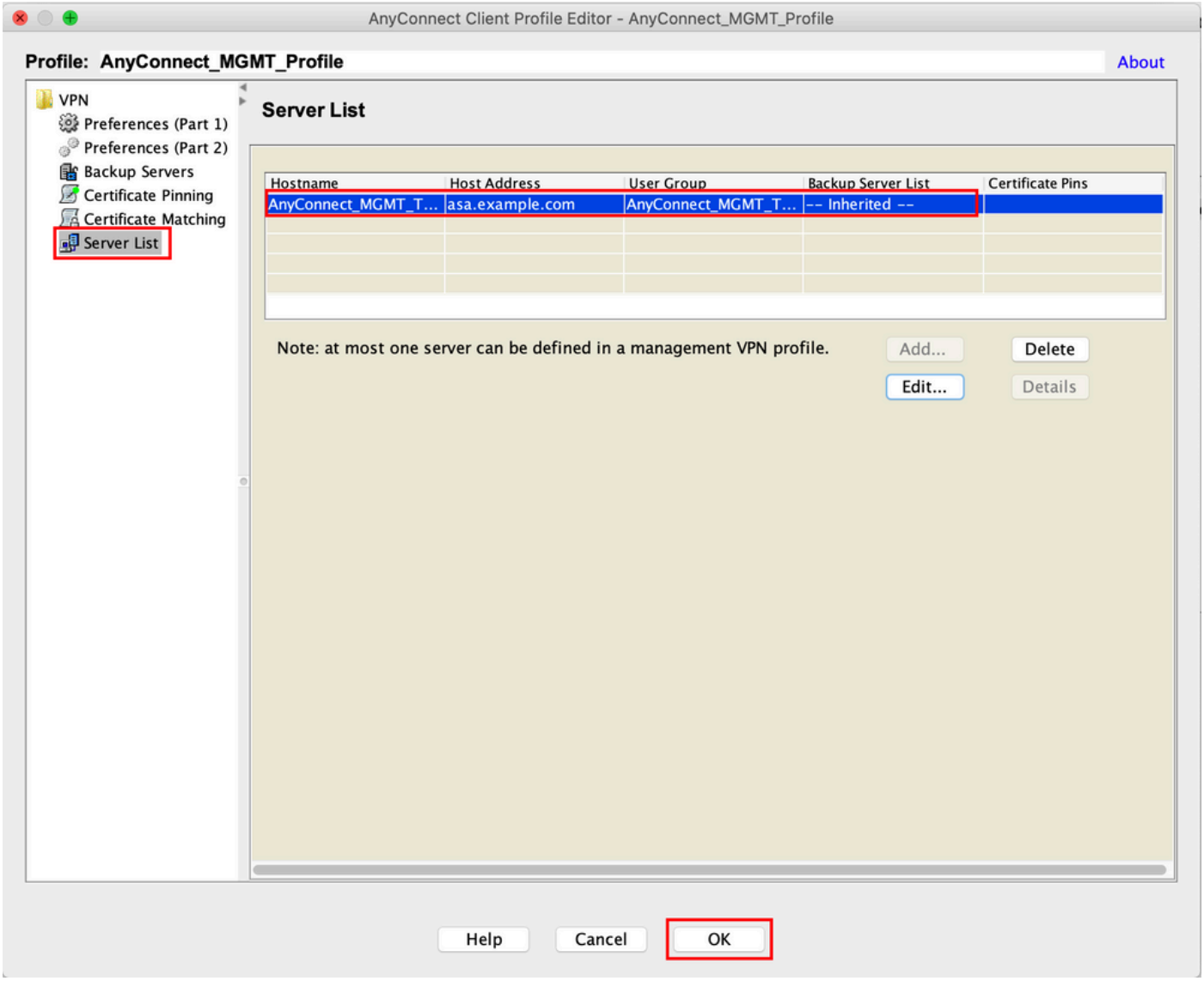
Schritt 5: Bieten Sie Display Name. Fügen Sie FQDN/IP address der ASA. Stellen Sie die User Group als Name der Tunnelgruppe. Group URL wird automatisch mit dem FQDN und User Group. Klicken Sie auf OK.



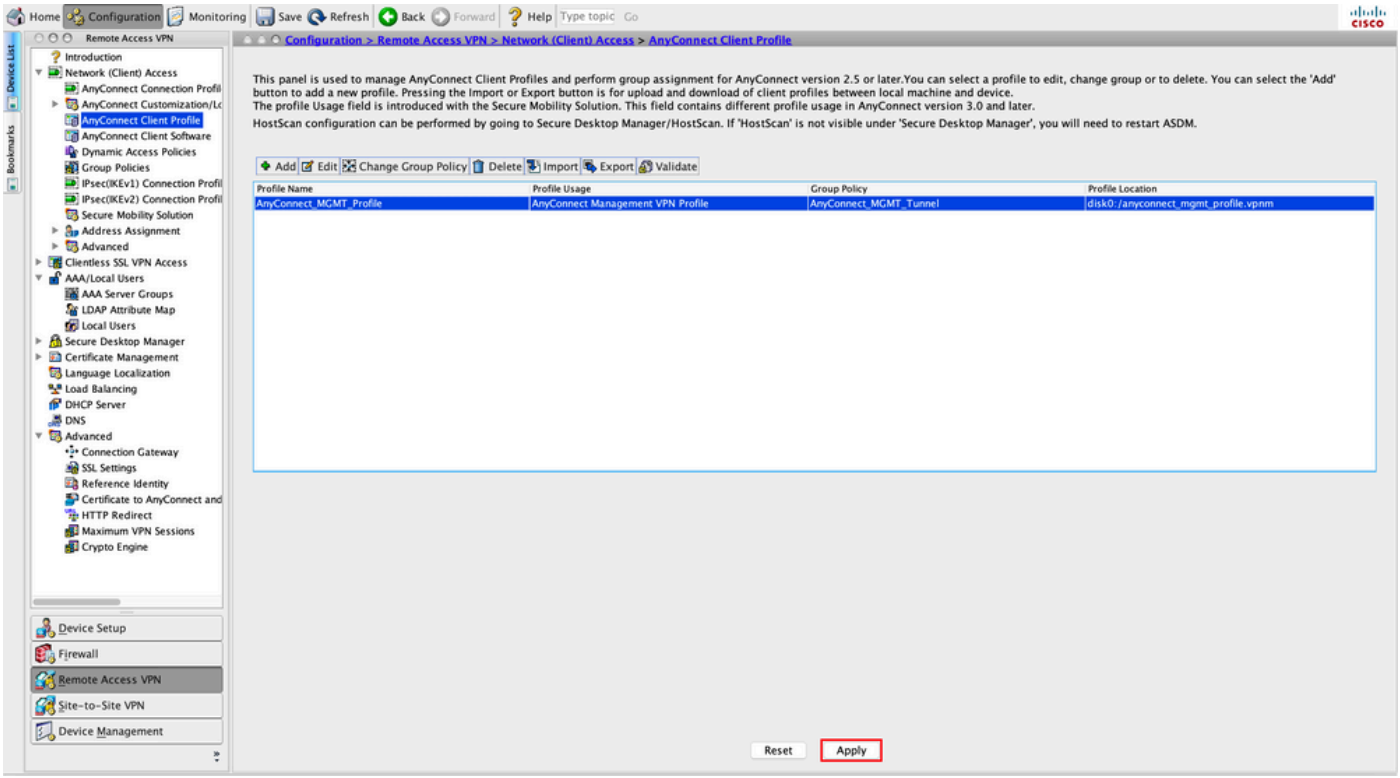
Hinweis: Die FQDN/IP-Adresse + Benutzergruppe muss mit der Gruppen-URL übereinstimmen, die bei der Konfiguration des AnyConnect-Verbindungsprofils in Schritt 8 erwähnt wird.

Hinweis: AnyConnect mit IKEv2 als Protokoll kann auch zum Einrichten eines Management-VPNs zur ASA verwendet werden. Sicher Primary Protocol ist auf IPsec in Schritt 5.

Schritt 6: Klicken Sie wie in der Abbildung dargestellt auf OK zum Speichern.



Schritt 7. Klicken Sie auf Apply to Übertragen Sie die Konfiguration an die ASA, wie im Abbild dargestellt.



CLI-Konfiguration nach dem Hinzufügen des AnyConnect-Management-VPN-Profils.

```
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-Management-VPN-Profil auf dem AnyConnect-Client-Computer:

```
<?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>
```

Hinweis: Wenn Trusted Network Detection (TND) im AnyConnect VPN-Benutzerprofil verwendet wird, ist es ratsam, die gleichen Einstellungen im VPN-Verwaltungsprofil vorzunehmen, um eine einheitliche Benutzererfahrung zu gewährleisten. Der Management-VPN-Tunnel wird auf Basis der TND-Einstellungen ausgelöst, die auf das Profil des Benutzer-VPN-Tunnels angewendet werden. Außerdem gilt die TND Connect-Aktion im Management-VPN-Profil (wird nur durchgesetzt, wenn der Management-VPN-Tunnel aktiv ist) immer für den Benutzer-VPN-Tunnel, um sicherzustellen, dass der Management-VPN-Tunnel für den Endbenutzer transparent ist.

Hinweis: Wenn auf einem Endbenutzer-PC im Management-VPN-Profil die TND-Einstellungen aktiviert sind und das Benutzer-VPN-Profil fehlt, werden die Standard-Voreinstellungseinstellungen für den TND (diese sind in den Standardeinstellungen in der AC-Client-Anwendung deaktiviert) anstelle des fehlenden Benutzer-VPN-Profils berücksichtigt. Diese Diskrepanz kann zu unerwartetem/undefiniertem Verhalten führen. Standardmäßig sind die TND-Einstellungen in den Standardeinstellungen deaktiviert.
Um die hardcodierten Standardeinstellungen in der AnyConnect Client-Anwendung zu überwinden, müssen auf dem Endbenutzer-PC zwei VPN-Profile, ein Benutzer-VPN-Profil und ein AC-Management-VPN-Profil vorhanden sein. Beide müssen die gleichen TND-Einstellungen aufweisen.
Die Logik hinter der Verbindung und Trennung des Management-VPN-Tunnels besteht darin, dass der AC-Agent zum Einrichten eines Management-VPN-Tunnels die TND-Einstellungen für das Benutzer-VPN-Profil verwendet und zum Trennen der Verbindung zum Management-VPN-Tunnel nach TND-Einstellungen für das Management-VPN-Profil sucht.

Bereitstellungsmethoden für das AnyConnect-Management-VPN-Profil

- Eine erfolgreiche Benutzer-VPN-Verbindung wird mit dem ASA-Verbindungsprofil hergestellt, um das AnyConnect-Management-VPN-Profil vom VPN-Gateway herunterzuladen.

  Hinweis: Wenn das Protokoll für den Management-VPN-Tunnel IKEv2 ist, muss die erste Verbindung über SSL hergestellt werden (um das AnyConnect-Management-VPN-Profil von der ASA herunterzuladen).

- Das AnyConnect Management VPN-Profil kann manuell auf die Client-Computer hochgeladen werden, entweder durch GPO-Push oder durch manuelle Installation (Stellen Sie sicher, dass der Name des Profils `VpnMgmtTunProfile.xml`).

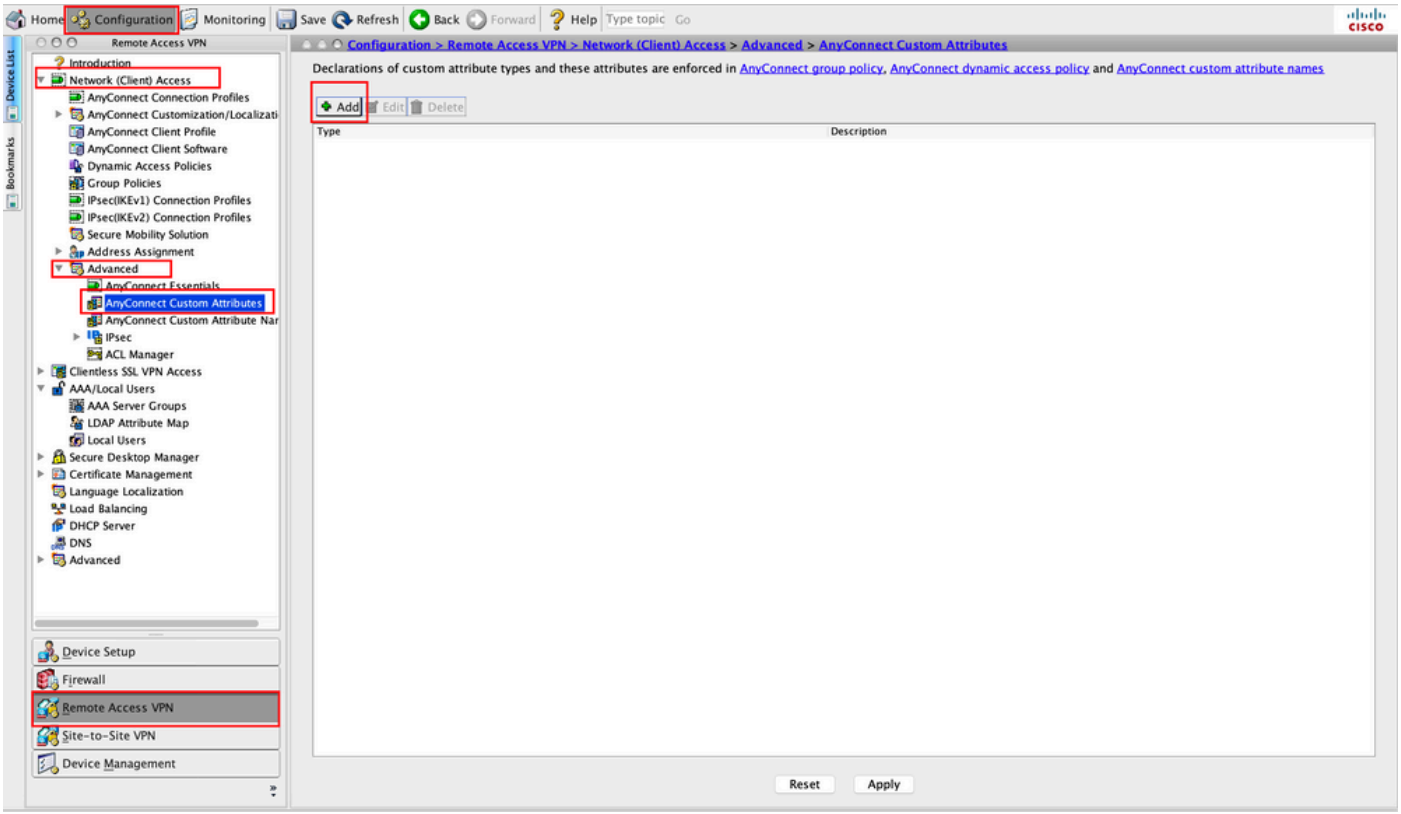
  Speicherort des Ordners, in dem das Profil hinzugefügt werden muss:
  Windows: **`C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun`**
  MacOS: `/opt/cisco/anyconnect/profile/mgmttun/`

(Optional) Konfigurieren eines benutzerdefinierten Attributs zur Unterstützung der Tunnel-All-Konfiguration

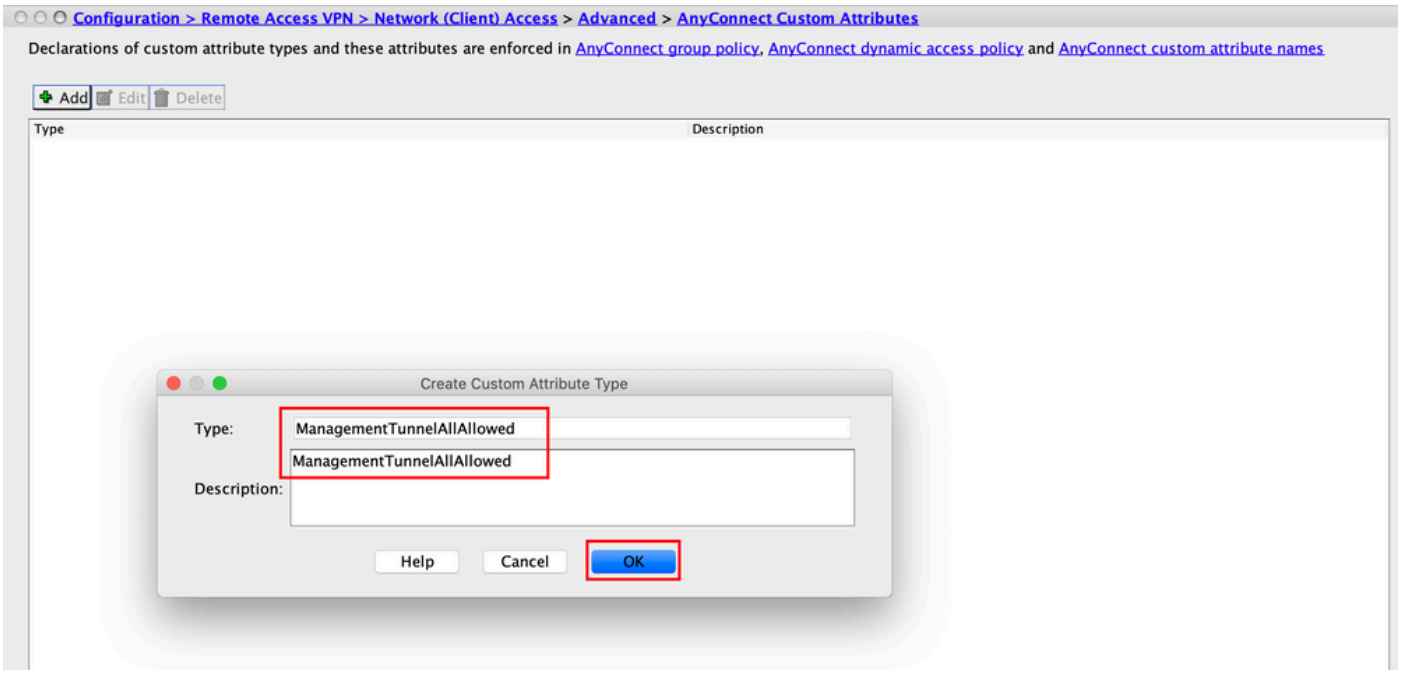
Management-VPN-Tunnel erfordern einen Split, der standardmäßig eine Tunneling-Konfiguration umfasst, um Auswirkungen auf die vom Benutzer initiierte Netzwerkkommunikation zu vermeiden. Dies kann überschrieben werden, wenn Sie das benutzerdefinierte Attribut in der Gruppenrichtlinie

konfigurieren, die von der Verwaltungstunnelverbindung verwendet wird.

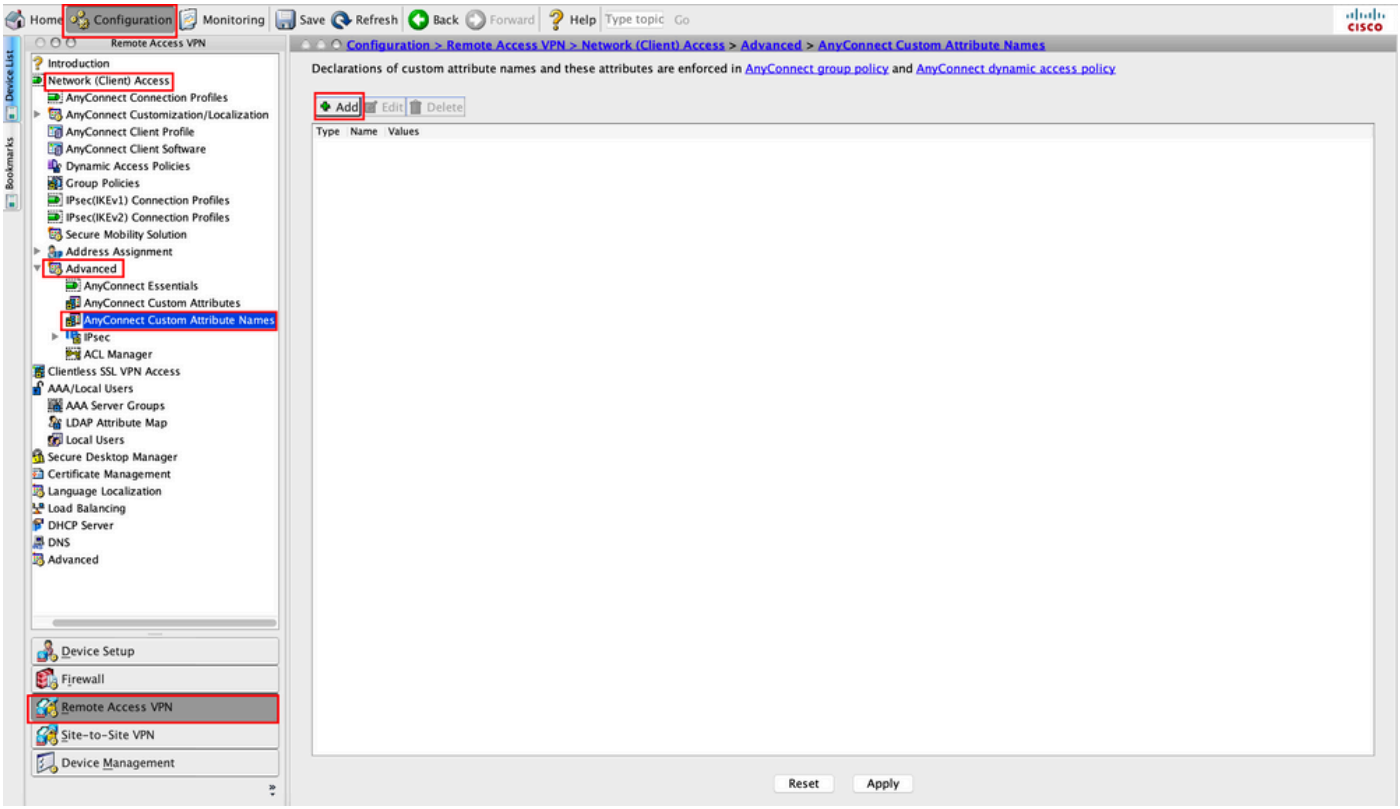
Schritt 1: Navigieren Sie zuConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Klicken Sie auf Add, wie im Bild dargestellt.



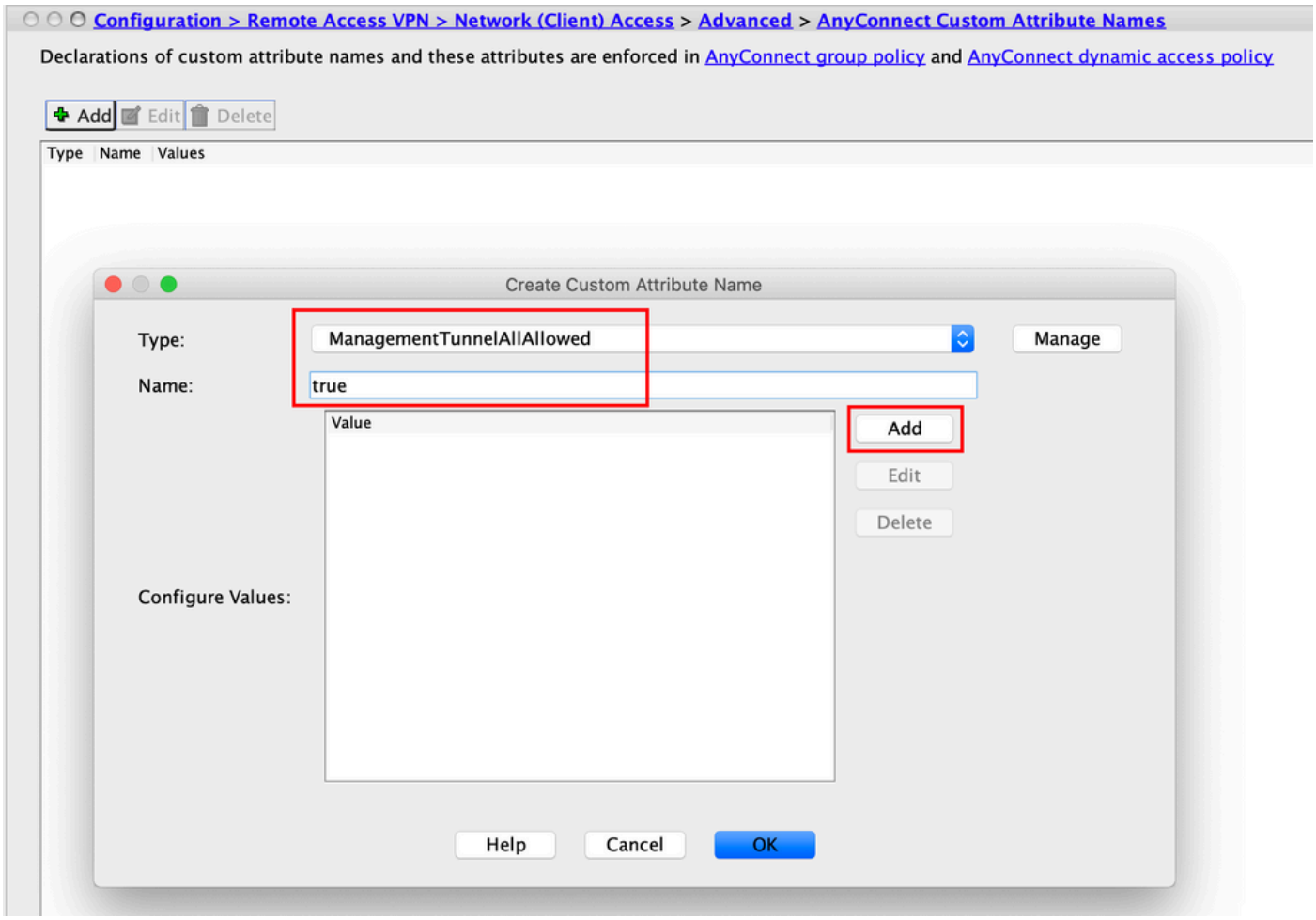
Schritt 2: Legen Sie das benutzerdefinierte Attribut Type auf ManagementTunnelAllAllowed und bieten eine Description. Klicken Sie auf OK, wie im Bild dargestellt.



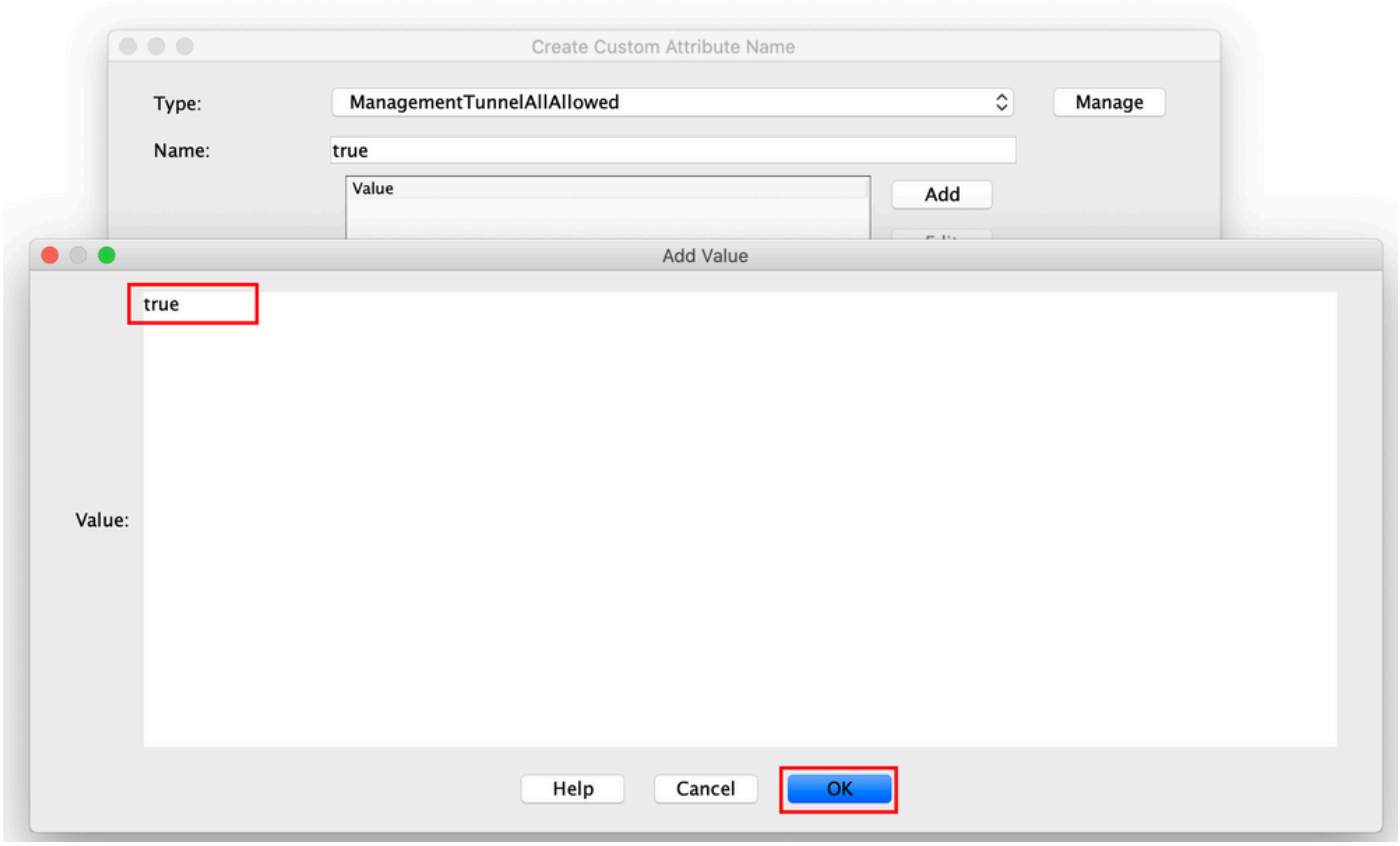
Schritt 3: Navigieren Sie zu **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.** Klicken Sie auf Add, wie im Bild dargestellt.



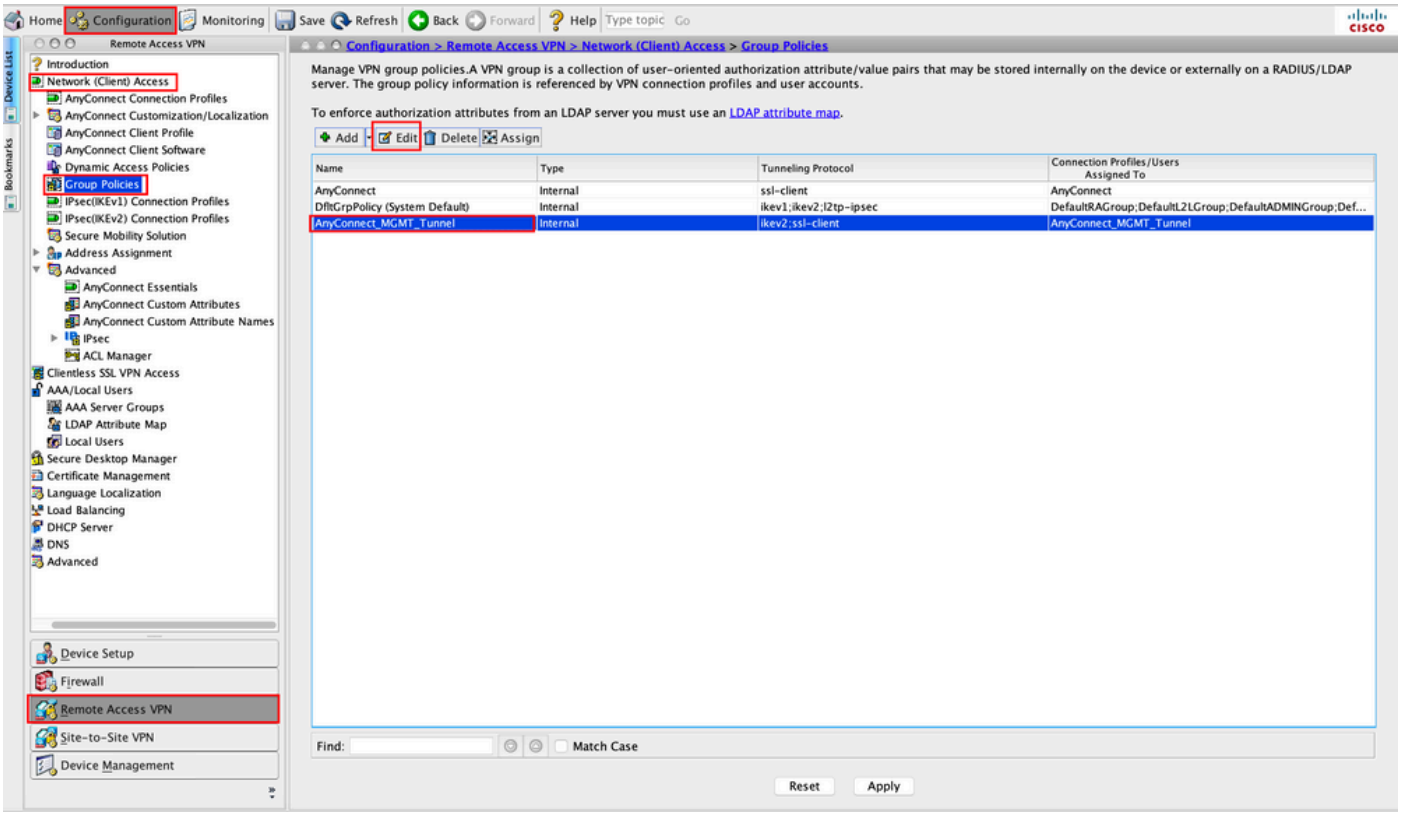
Schritt 4: Wählen Sie den Typ **ManagementTunnelAllAllowed** . Legen Sie den Namen fest als true. Klicken Sie auf Addum einen benutzerdefinierten Attributwert bereitzustellen, wie im Bild dargestellt.



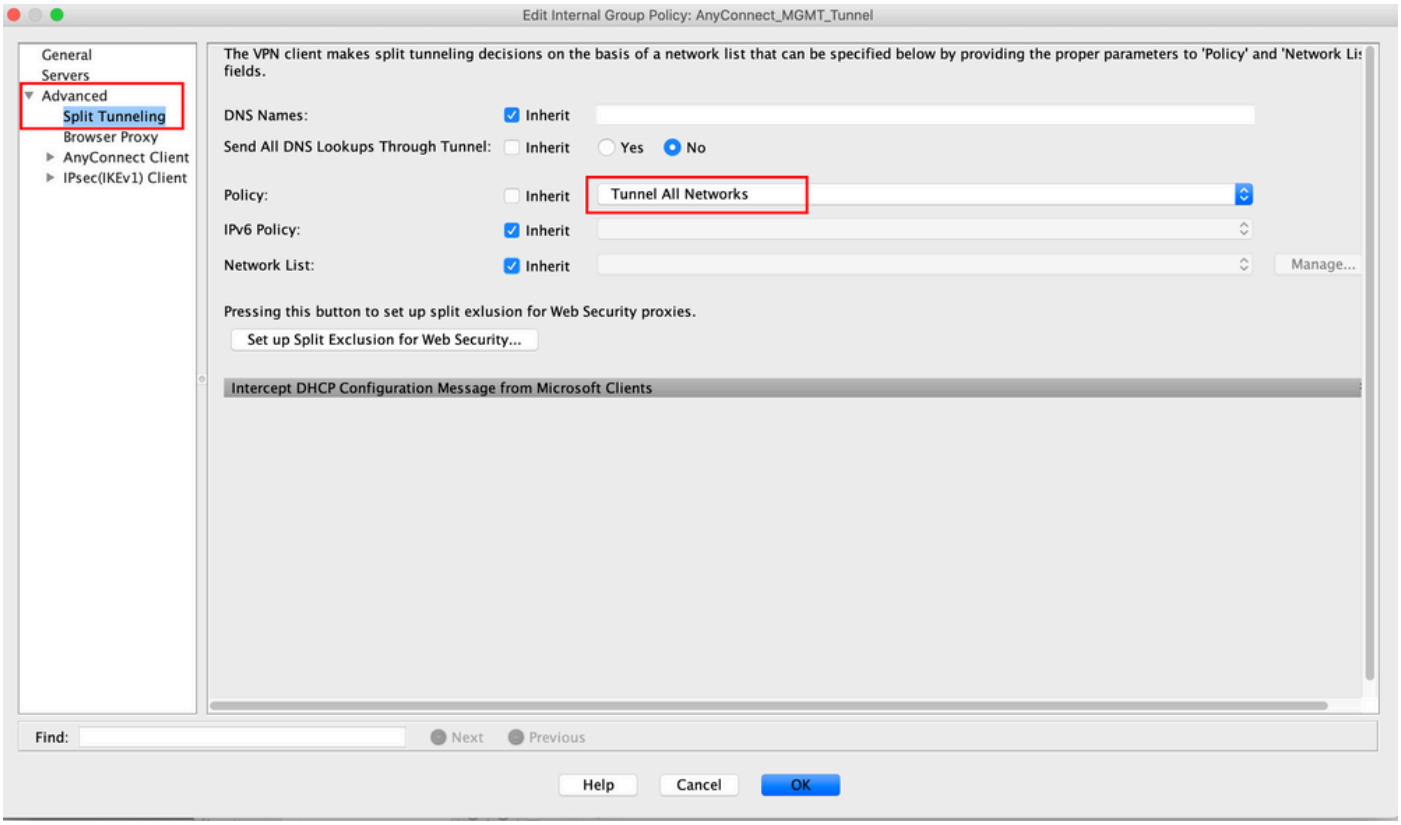
Schritt 5: Wert festlegen als true. Klicken Sie auf OK, wie im Bild dargestellt.



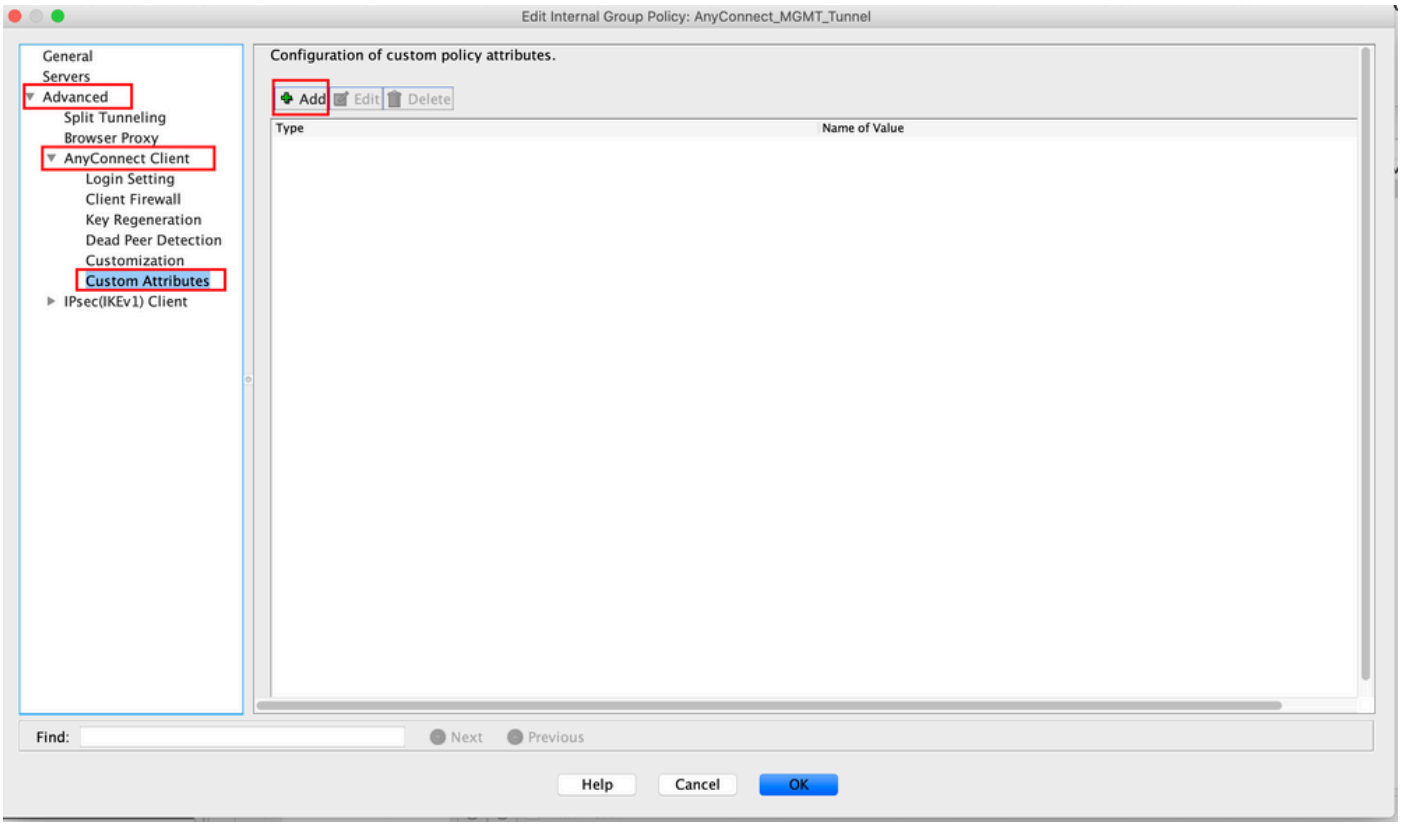
Schritt 6: Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Wählen Sie die Gruppenrichtlinie aus. Klicken Sie auf Edit , wie im Bild dargestellt.



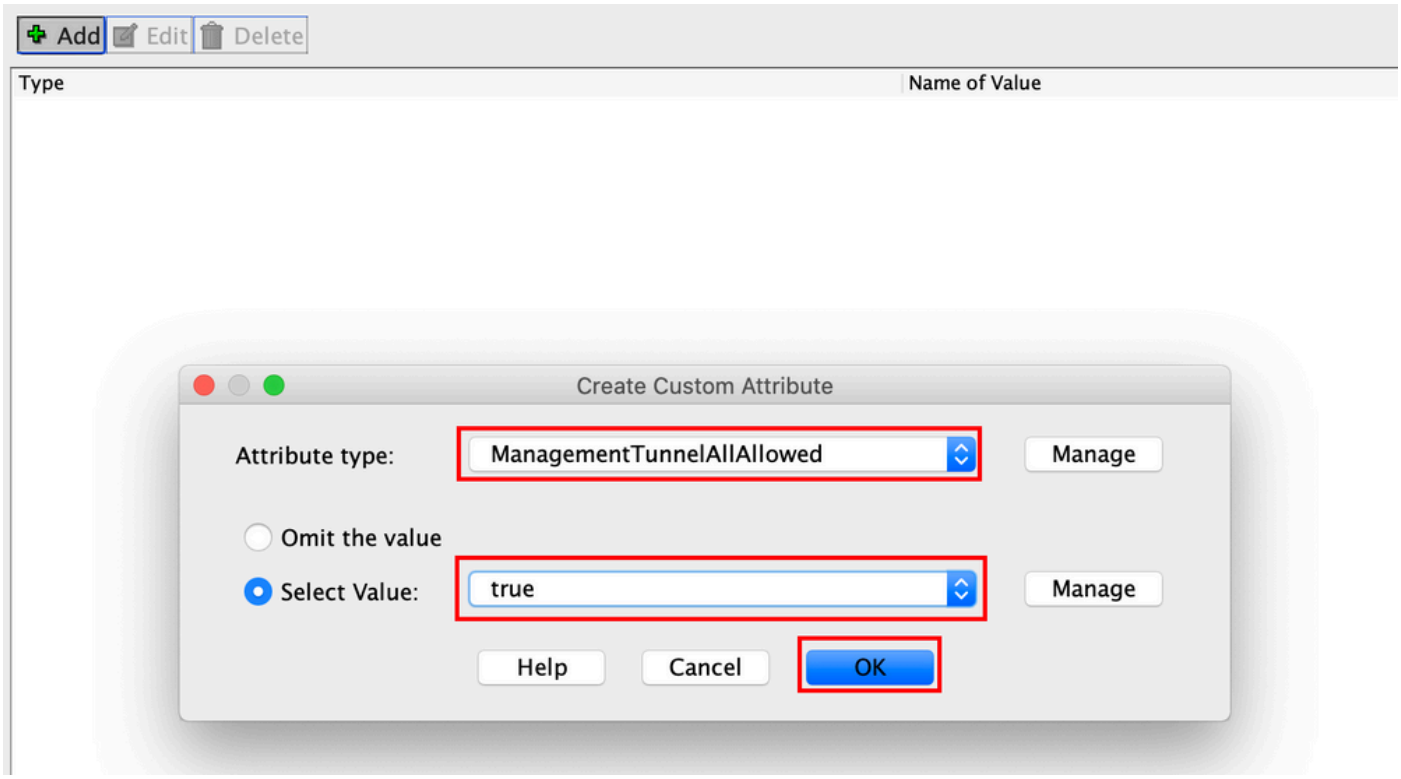
Schritt 7. Navigieren Sie, wie in dieser Abbildung dargestellt, zu Advanced > Split Tunneling. Konfigurieren Sie die Richtlinie als Tunnel All Networks.



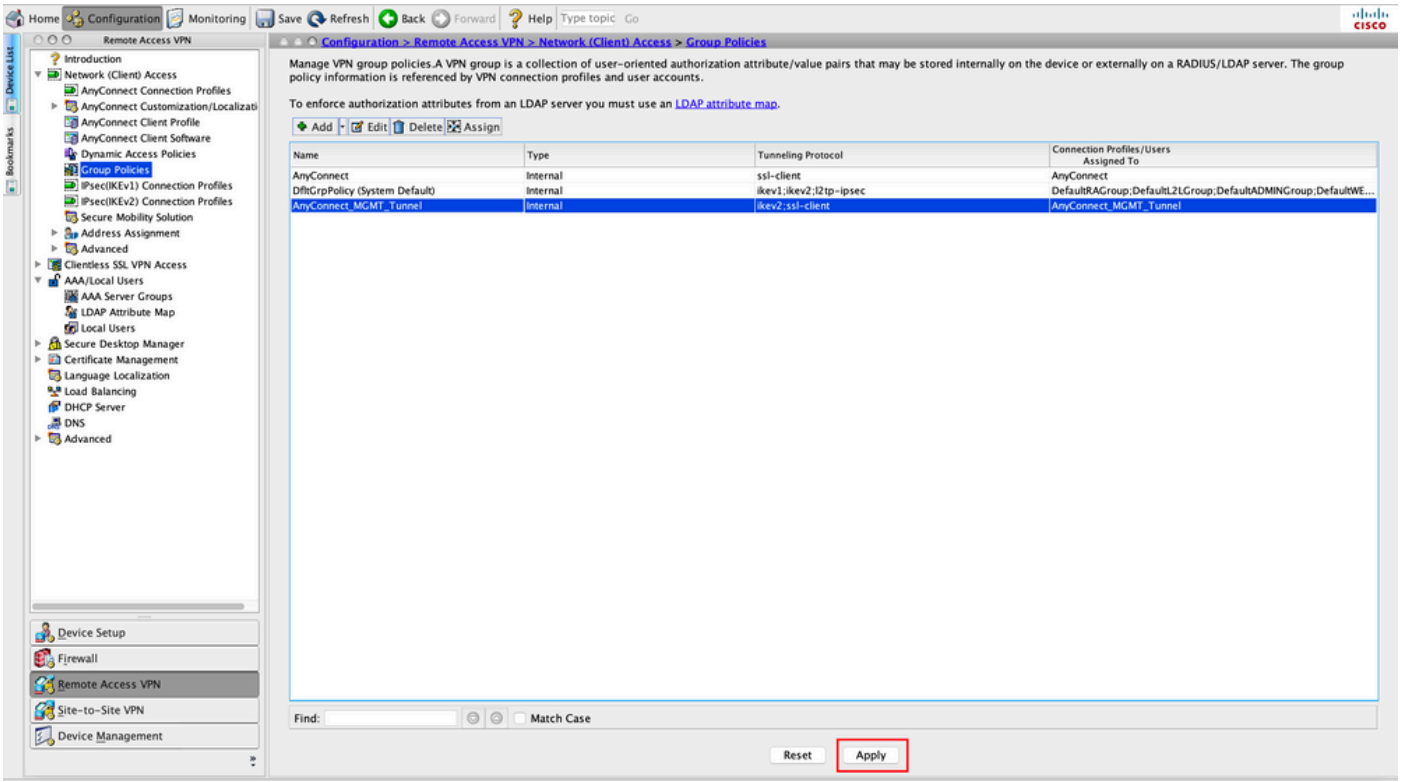
Schritt 8: Navigieren Sie zu Advanced > Anyconnect Client > Custom Attributes. Klicken Sie auf Add, wie im Bild dargestellt.



Schritt 9. Wählen Sie den Attributtyp ManagementTunnelAllAllowed und wählen Sie den Wert als true. Klicken Sie auf OK, wie im Bild dargestellt.



Schritt 10. Klicken Sie auf Apply um die Konfiguration an die ASA weiterzuleiten (siehe Abbildung).



CLI-Konfiguration nach dem ManagementTunnelAllAllowed Benutzerdefiniertes Attribut wird hinzugefügt:

```
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
```

Überprüfung

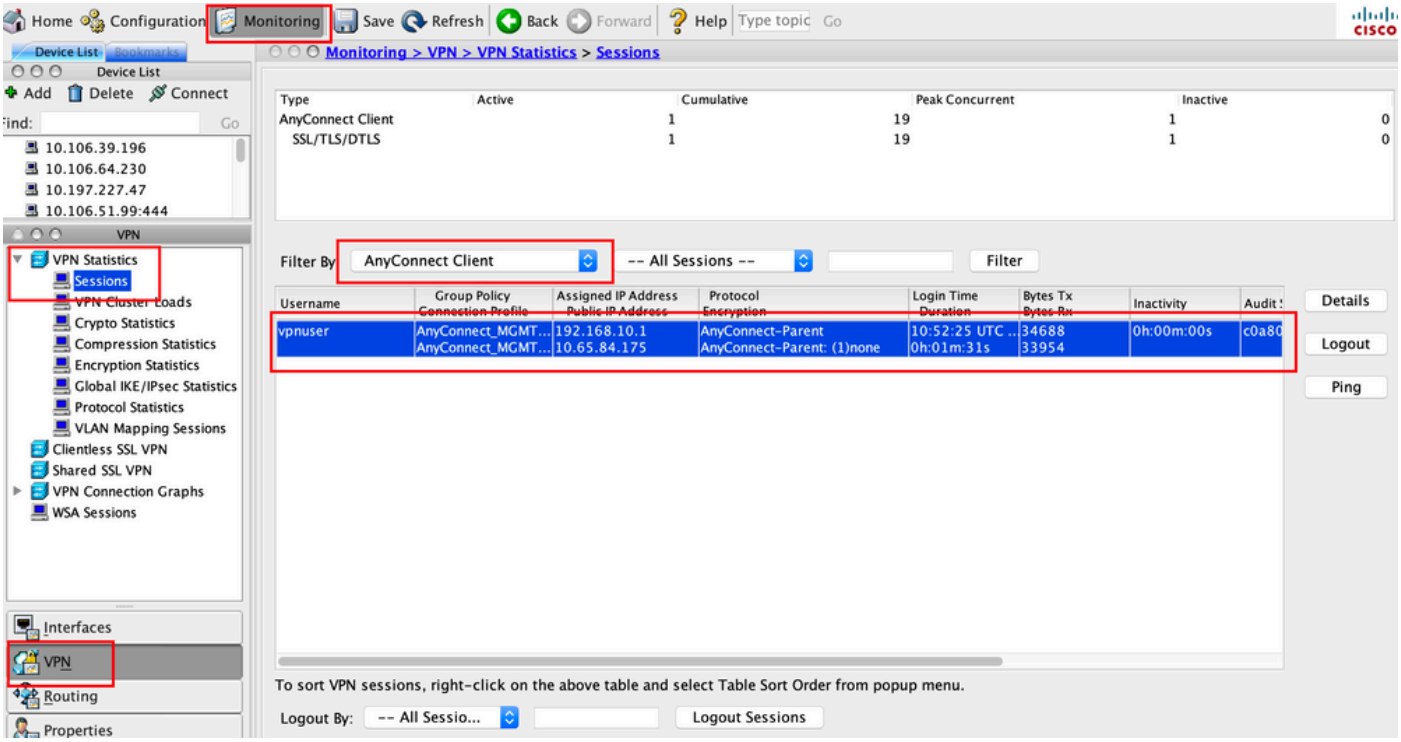
Überprüfen Sie die Management-VPN-Tunnelverbindung auf der ASA CLI mit dem show vpn-sessiondb detail anyconnect aus.

```
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
```

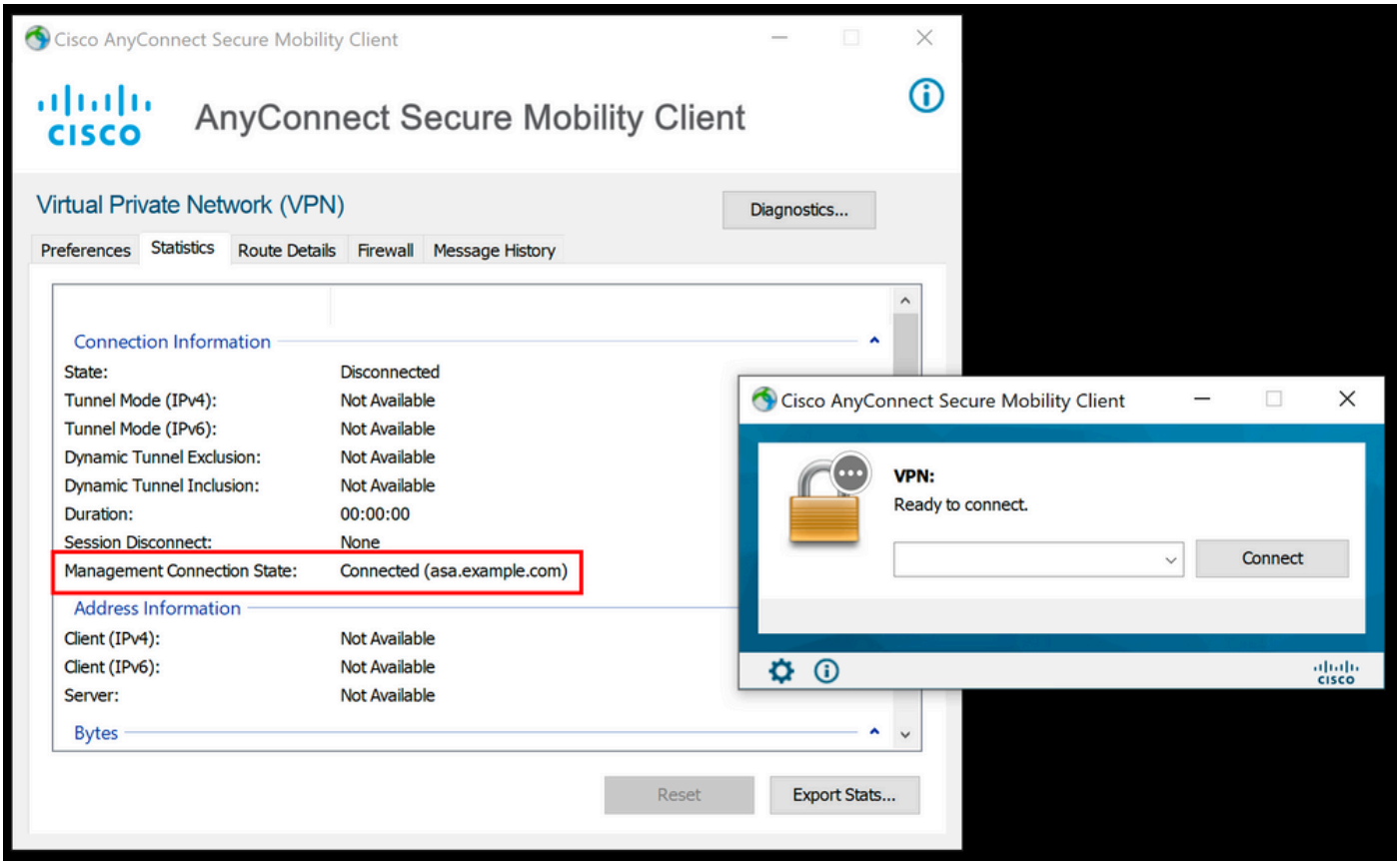
```
Encapsulation: DTLSv1.2              UDP Src Port : 57053
UDP Dst Port : 443                   Auth Mode    : Certificate
Idle Time Out: 30 Minutes            Idle TO Left : 18 Minutes
Client OS    : Windows
Client Type  : DTLS VPN Client
Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03036
Bytes Tx     : 17238                 Bytes Rx     : 1988
Pkts Tx      : 12                    Pkts Rx      : 13
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

Überprüfen Sie die Management-VPN-Tunnelverbindung in ASDM.

Navigieren Sie zu Monitoring > VPN > VPN Statistics > Sessions (Überwachung > VPN > VPN-Statistik > Sitzungen). Filtern Sie nach AnyConnect-Client, um die Client-Sitzung anzuzeigen.



Überprüfen der Management-VPN-Tunnelverbindung auf dem Client-Computer:



Fehlerbehebung

Die neue Statistikzeile Management Connection State (Management-Verbindungsstatus) in der Benutzeroberfläche kann verwendet werden, um Probleme mit der Management-Tunnelverbindung zu beheben. Die häufigsten Fehlerzustände sind:

Disconnected (disabled) (Verbindung getrennt (deaktiviert)):

- Die Funktion ist deaktiviert.
- Stellen Sie sicher, dass das Management-VPN-Profil auf dem Client über eine Benutzer-Tunnel-Verbindung (Sie müssen das Management-VPN-Profil der Benutzer-Tunnel-Gruppenrichtlinie hinzufügen) oder Out-of-Band über den manuellen Upload des Profils bereitgestellt wurde.
- Stellen Sie sicher, dass das Management-VPN-Profil mit einem einzelnen Hosteintrag konfiguriert ist, der eine Tunnelgruppe enthält.

Disconnected (trusted network) (Verbindung getrennt (vertrauenswürdiges Netzwerk)):

- TND hat ein vertrauenswürdiges Netzwerk erkannt, sodass der Management-Tunnel nicht eingerichtet wird.

Disconnected (user tunnel active) (Verbindung getrennt (Benutzertunnel aktiv)):

- Ein Benutzer-VPN-Tunnel ist derzeit aktiv.

Disconnected (process launch failed) (Verbindung getrennt (Prozess konnte nicht gestartet werden)):

- Fehler beim Starten des Prozesses beim Versuch, eine Management-Tunnelverbindung herzustellen.

Disconnected (connect failed) (Verbindung getrennt (Verbindung fehlgeschlagen)):

- Beim Herstellen des Verwaltungstunnels ist ein Verbindungsfehler aufgetreten.
- Stellen Sie sicher, dass die Zertifikatauthentifizierung in der Tunnelgruppe konfiguriert ist, kein Banner in der Gruppenrichtlinie vorhanden ist und das Serverzertifikat vertrauenswürdig sein muss.

Disconnected (invalid VPN configuration) (Verbindung getrennt (ungültige VPN-Konfiguration)):

- Eine ungültige Split-Tunneling-Konfiguration wurde vom VPN-Server empfangen.
- Überprüfen Sie die Split-Tunneling-Konfiguration in der Management-Tunnelgruppenrichtlinie.

Disconnected (software update pending) (Verbindung getrennt (Software-Updates ausstehend)):

- Ein AnyConnect-Software-Update steht derzeit aus.

Disconnected (Verbindung getrennt):

- Der Verwaltungstunnel steht kurz vor der Einrichtung oder kann aus anderen Gründen nicht eingerichtet werden.

Sammeln Sie DART zur weiteren Fehlerbehebung.

Zugehörige Informationen

- Konfiguration des Management-VPN-Tunnels
- Fehlerbehebung beim Management-VPN-Tunnel
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.