

ASA ىلج AnyConnect ةرادال VPN ق فن نيوكت

تاوت حمل

[قم دق م ل ا](#)

[ةيساس أ ل ا تاب ل ط م ل ا](#)

[تاب ل ط م ل ا](#)

[ةمدخت س م ل ا تانوك م ل ا](#)

[ةيساس أ تامول عم](#)

[قرادال ل مع ق فن](#)

[دوي ق ل ا](#)

[نيوكت ل ا](#)

[ASDM/CLI ل ل الخ نم ASA ىلج نيوكت ل ا](#)

[AnyConnect Management VPN في رعت فلم عاش ن ا](#)

[AnyConnect ةراداب ص اخل ل ا VPN في ص وت ل ر ش ن ل ا ب ل ا س ا](#)

[ق فن ل ا ر ب ع ل ل ل ا نيوكت معدل ة ص ص خ م ة م س نيوكت ب م ق \(ى ر ا ب ت خ ل\)](#)

[ةحص ل ا نم ق ق ح ت ل ا](#)

[اه ج ال ص او ع ا ط خ أ ل ا ف اش ك ت س ا](#)

[ةلص ت ا ذ ت ا م و ل ع م](#)

ةمدق م ل ا

AnyConnect Secure نم تالاصت ال ا VPN ة باوب ل بقت شي ح ASA نيوكت دنت س م ل ا اذه فص ي Management VPN ق فن ل ل الخ نم AnyConnect Secure Mobility Client.

ةيساس أ ل ا تاب ل ط م ل ا

تاب ل ط م ل ا


ةيل ل ال عيضاوم ل ا ب ة فرعم ك ي د ل نوكت ن ا ب Cisco ي ص وت:

- (ASDM) في ك ت ل ل ل ا ب ا ق ل ا نام أ ل ا ة ز ه ج أ ر ي د م ل ل ل خ نم VPN نيوكت
- ةيساس أ ل ا ة ل د ع م ل ا نام أ ل ا ة ز ه ج أ ل (CLI) ر م او أ ل ا ر ط س ة ه ج او نيوكت
- X509 ت ا د ا ه ش

ةمدخت س م ل ا تانوك م ل ا

ةيل ل ال ا ة ي د ا م ل ا تانوك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ل ا ل ا دنت س م ل ا اذه في ة د ر او ل ا تامول عم ل ا دنت س ت:

- Cisco نم 9.12(3)9 ر ا د ص ل ا ل ا ASA ج م ا ن ر ب
- Cisco نم 7.12.2 ر ا د ص ل ا ل ا ASDM ج م ا ن ر ب
- Windows 10 ع م Cisco AnyConnect Secure Mobility Client، ر ا د ص ل ا ل ا 4.8.03036

 AnyConnect VPN بيولا ىل ع (anyconnect-win*.pkg or anyconnect-macos*.pkg) رشن ةمزح ليزنت :ةظالم AnyConnect ليمع خسنا .(طقف نيلجسملال عالمعلل) Cisco [جمانرب ليزنت](#) نم (macos*.pkg) رتوي بمك ةزهجأ ىل اهل يزننت متيس يتال ASA ل (ةتقؤملا ةركاذل) Flash ةركاذ ىل VPN [AnyConnect مسق تيبثت](#) عجار .ASA عم SSL VPN لاصلتا عاشنال ةديعبال مدختسملال تامولعملال نم ديزم ىل ع لوصحلل ASA نيوكت ليلدي في [Client](#)

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجال نم دنتسملال اذ في ةدراولال تامولعملال عاشنال مت تناك اذا .(يضارتفا) حوسمم نيوكت ب دنتسملال اذ في ةمدختسملال ةزهجال عيمج تآب رمأ يأل لمحتحملال ريثأتلل كمهف نم دكأتف ،ليغشتال دي قكتك ب شب

ةيساسأ تامولعمل

متاملك ةكرشلال ةكبشبال لاصلتال ةرادلال (VPN) ةيرهاظلال ةصاخلال ةكبشبال قفن نم ضي (VPN) ةيرهاظلال ةصاخلال ةكبشبال لاصلتال سيسي سأت دن ع طقف سي لو ،ليمعلال ماظن ليغشت ب، بكملا چراخ ةياهنلال طاقن ىل ع مزحلال ةرادل ذيفنت كنكمي .يئاهنلال مدختسملال ةطساوب ،VPN ةكبش رب ع ،مدختسملال ةطساوب رركتم لكشبال اهليصوت متي يتال ةزهجال ةصاخو ليغشتال ماظن ىل لوخدلال ليحستل ةيصنلال جماربال ديغتست امك .ببكملا ةكبشبال ةزيملال هذه نم ةكرشلال ةكبشبال لاصلتال بلطت يتال Endpoint OS

نم لخدت نود AnyConnect ب لاصلتالاب ني لوؤسملل "AnyConnect ةرادل قفن" حمسي نارتقالاب AnyConnect ةرادل قفن لمعي نأ نكمي .مدختسملال لوخد ليحست لبق مدختسملال ةطقن نوكت ام دن ع طقف هليغشت متي يلاتلابو ،"اهب قوؤوملا ةكبشبال فاشتك" عم ةرادل قفن نوكي .مدختسملال اهدب VPN ةكبشبال نم اهليصوف متي ولصلال چراخ ةياهنلال مدختسملال موقوي ام دن ع ايئاقلت لاصلتال ع طقوي ويئاهنلال مدختسملال فافش AnyConnect VPN ةئيهت ب

رادصلال تابللطتمل ىندالال دحل	قبيبطتلال/ليغشتال ماظن
9.0.1	ASA
7.10.1	ASDM
4.7.00136	Windows AnyConnect رادصل
4.7.01076	MacOS نم AnyConnect رادصل
دمتعم ريغ	سكنيل

ةرادلال لمع قفن


نأ فشتكي هنإ .ماظنلال ديهمت دن ع ايئاقلت AnyConnect VPN ليمع ةمدخ ليغشت ادب متي نأ قبيبطت نوبز ةرادلال قلطي وه كلذل ،(VPN profile ةرادلال قيرط نع) ةمس تنكم قفن ةرادلال فيرعت فلم نم فيضملال لاخدل ةرادلال ليمع قبيبطت مدختسي .ليصوت قفن ةرادل ادبي ،داتعملال VPN قفن عاشنال متي مث .لاصلتال ادبل ةرادلال (VPN) ةيرهاظلال ةصاخلال ةكبشبال ،نم هنأل ارظن ةرادل قفن لاصلتال ائانثأ جمانربل ثيدحت يأ عارج متي ال :دحاو ائانثتسا عم .مدختسملال فافش ةرادلال قفن نوكي نأ ضررتفلم

ليغشتب موقت يتالو ،AnyConnect مدختسملال ةهجاو رب ع VPN قفن ادبب مدختسملال موقوي .داتعملال مدختسملال قفن عاشنال رمتسي ،ةرادلال قفن اهانل دن ع .ةرادلال قفن اهانل

ةيئاقللتلا عاشنإلا ةداعإ لئغشت ىلإ يءؤي يذلاو، VPN قفن لاصتا عطقب مدختسملا موقى ةرادإلا قفنل.

دويقلا

- موعدم ريغ مدختسملا لعافت
- (Windows في) "يلاآلا تاداهشلا نزخم" لالخنم ةداهشلا ىلإ ةدنتسملا ةقداصملا طقف ةموعدم
- ديقملا مداخل ةداهش صحف صرف متي
- موعدم ريغ صاخلا ليكولا
- ةيساسالا ةمظنالا ىلع ليكولل ةيلصالا ةميقلال معد متي) دم تعم ريغ ماعلا ليكولا (ضرعتسملا نم يلاصالا ليكولا تاداعإ دادرستسا متي ال شيح
- ةموعدم ريغ AnyConnect في صيصختلل ةيصلنلا جماربلا


 [Management VPN قفن لوح](#) ىلإ عجرا، تامولعمل نم ديزم ىلع لوصحلل: ةظحالم

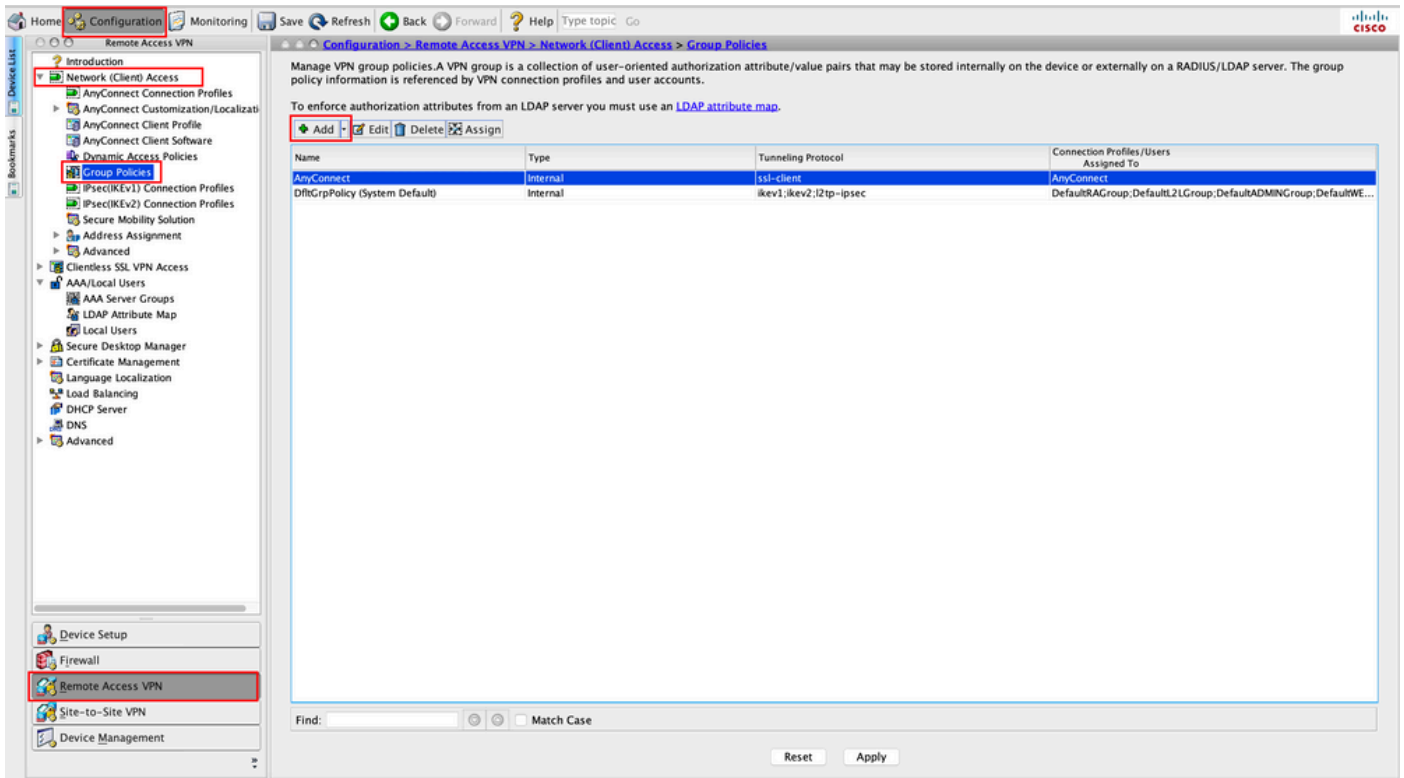
نيوكتلا

عالمع نم تالاصتالا لوبقل VPN ةبوابك Cisco ASA نيوكت ةيفيكم مسقلا اذه فصبي Management VPN قفن لالخنم AnyConnect.

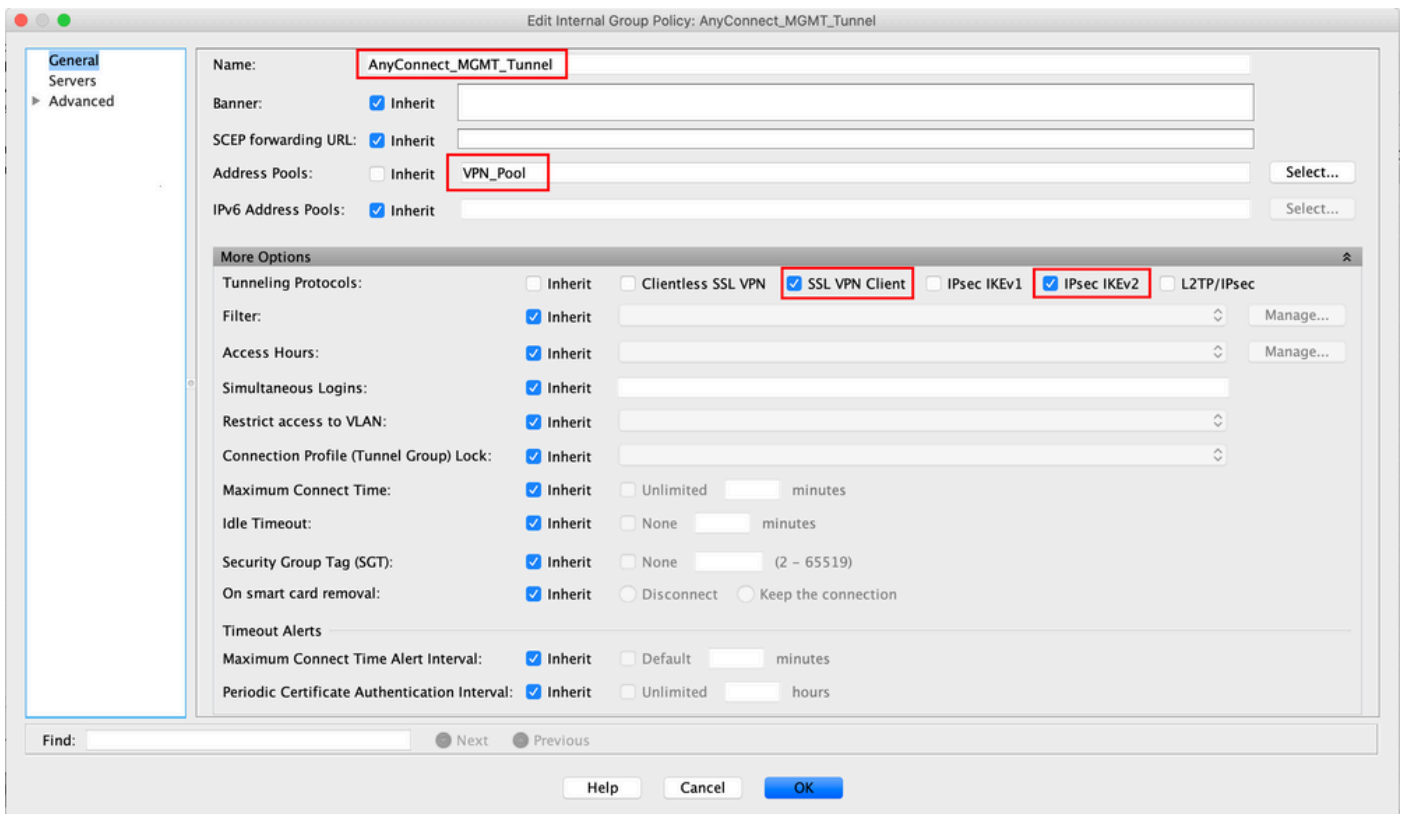
ASDM/CLI لالخنم ASA ىلع نيوكتلا

ىلإ لقتنا. AnyConnect ةومجم جهن عاشنإ. 1. ةوطخلا Configuration > Remote Access VPN > Network (Client) Access > Group Policies. رقنا Add.

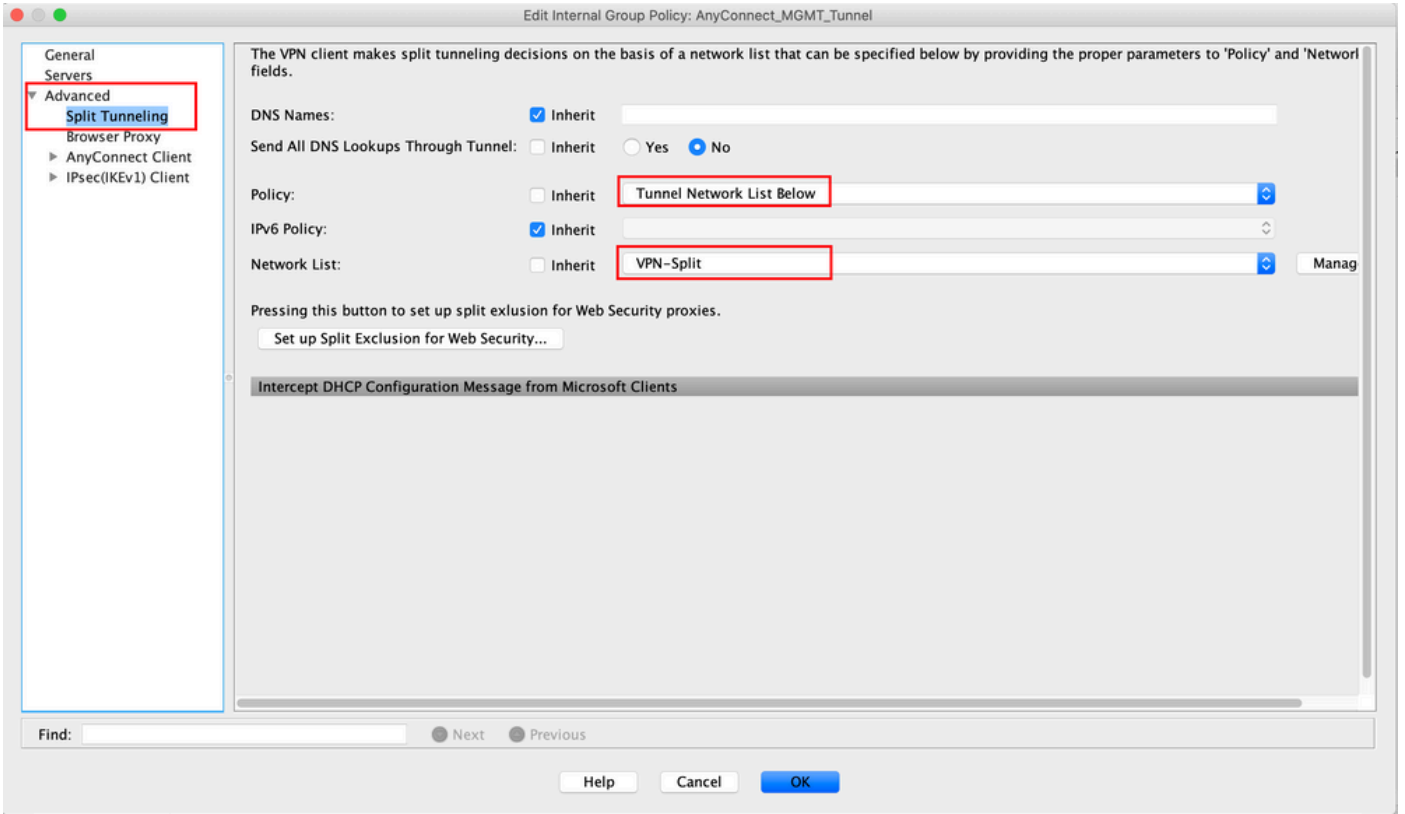
 ةرادإ قفنل همادختسا متي ديذج AnyConnect ةومجم جهن عاشنإ نسحتسملا نم: ةظحالم AnyConnect طقف.



2. ةوطخلال Name ري فوت. ةومحملال جه نل ءاشن/نبي عت. ةومحملال جه نل Name ري فوت. ةوطخلال SSL ء Tunneling Protocols راتخن. Address Pool ءاشن/نبي عت. ةومحملال جه نل Name ري فوت. ةوطخلال VPN Client ء او IPsec IKEv2، ءامك ء ةومحملال جه نل Name ري فوت. ةوطخلال

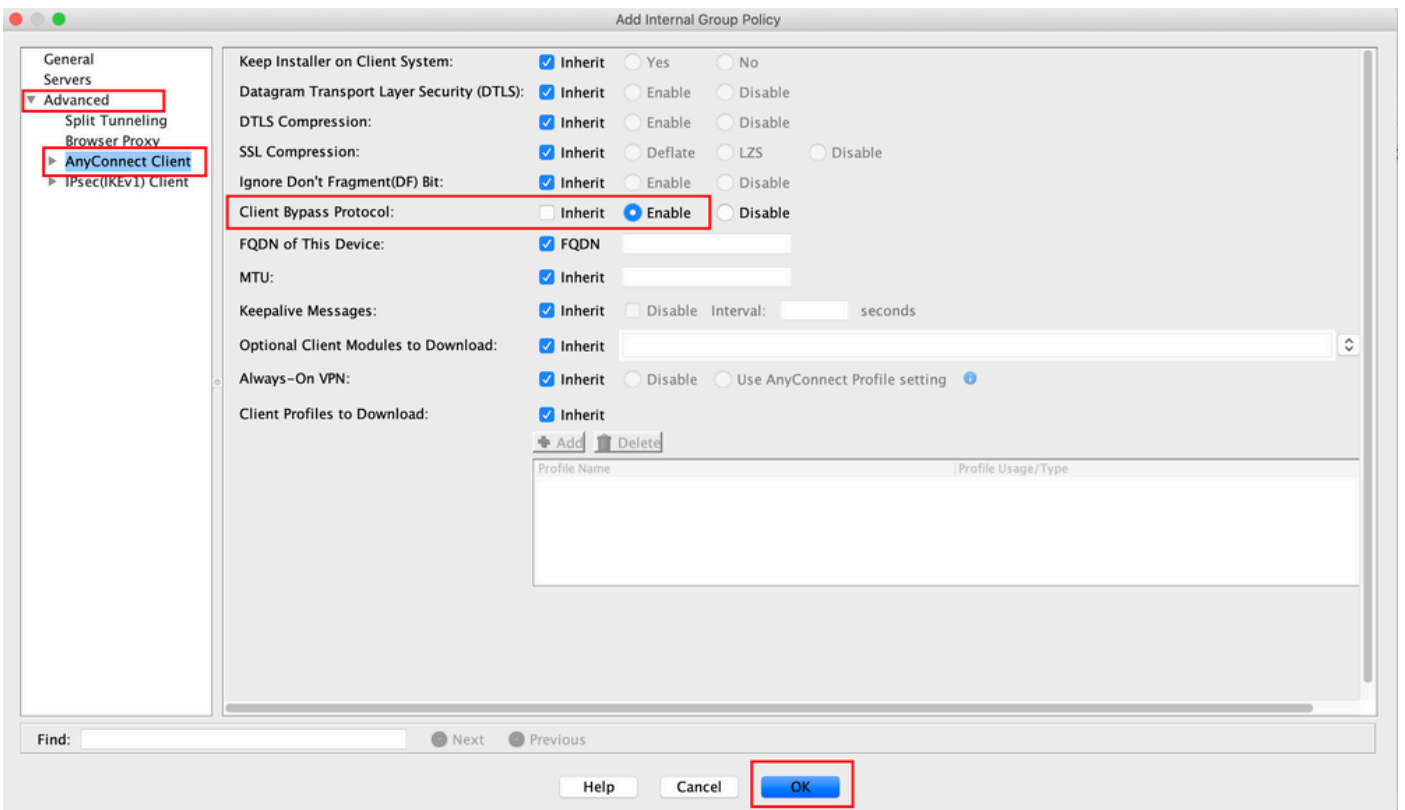


3. ةوطخلال Advanced > Split Tunneling. ءاشن/نبي عت. ةومحملال جه نل Name ري فوت. ةوطخلال Tunnel Network List ء Policy نيوكتب مق. ءاشن/نبي عت. ةومحملال جه نل Name ري فوت. ةوطخلال Network List، راي ء او ءاشن/نبي عت. ةومحملال جه نل Name ري فوت. ةوطخلال

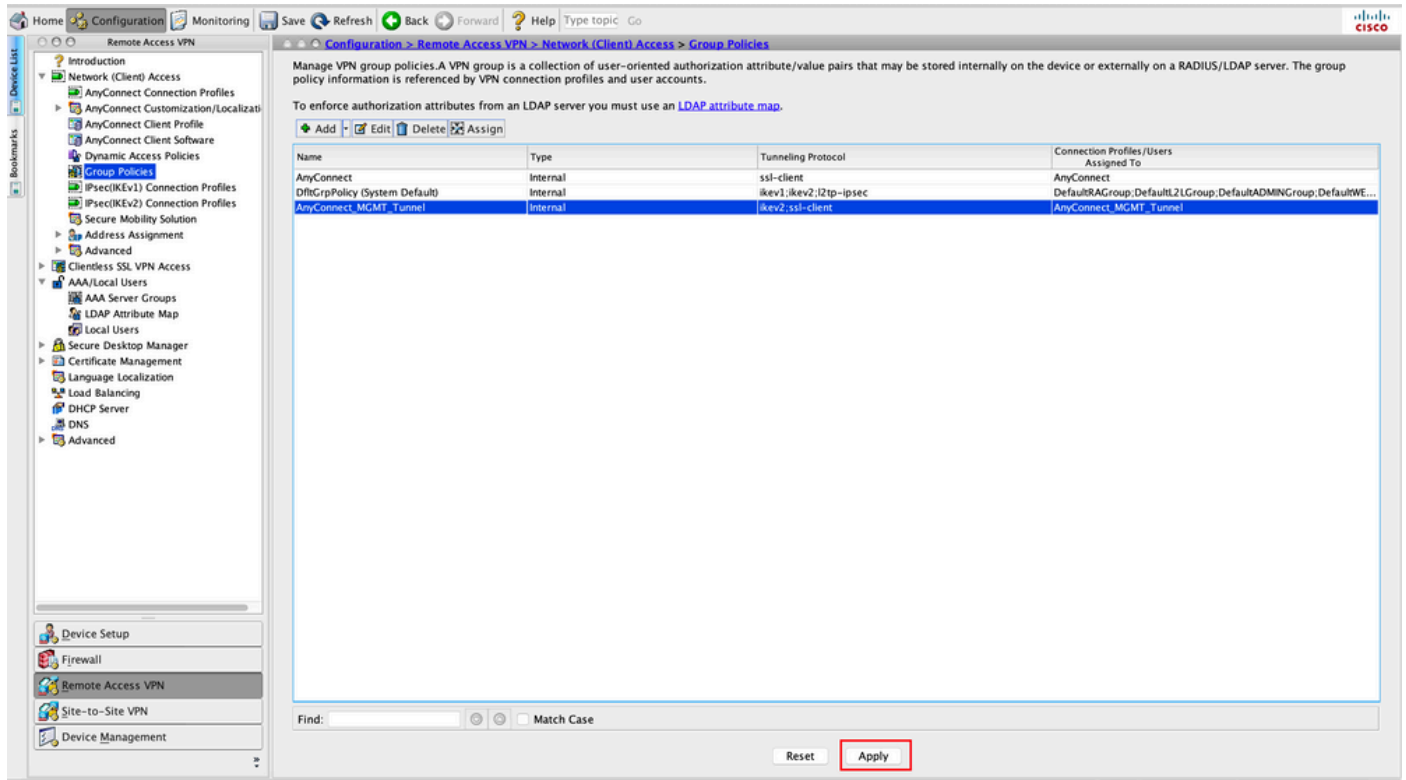


✎ Client Bypass ناف (IPv4 و IPv6) يلو كوتورب نم لكل لي مع اونع ع فد متي مل اذا: عظهارم
 ةطساوب ةقباطملا رورملا ةكرح لي طعت متي ال شيحب enabled دادعالا نوكي نأ ب جي Protocol
 4. ةوطخلإا إلى ع جرا، نيوكتلل. ةرادإل ق فن

ة و ع و م ج م Client Bypass Protocol ة و م ج م Advanced > AnyConnect Client. إلى ل ق ت نا 4. ة و ط خ ل ل
 ة ر و ص ل ل ي ف ح و م و ه امك، ظ ف ل ل OK ر ق نا. إلى Enable.



ASA إلى ليكشنتل ع فدل Apply قوف رونا، ةروصلل هذه يف حضورم وه امك 5. ةوطخلل



ةس ايس ة عوم جم ل ليكشنتل CLI:

```
<#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
```

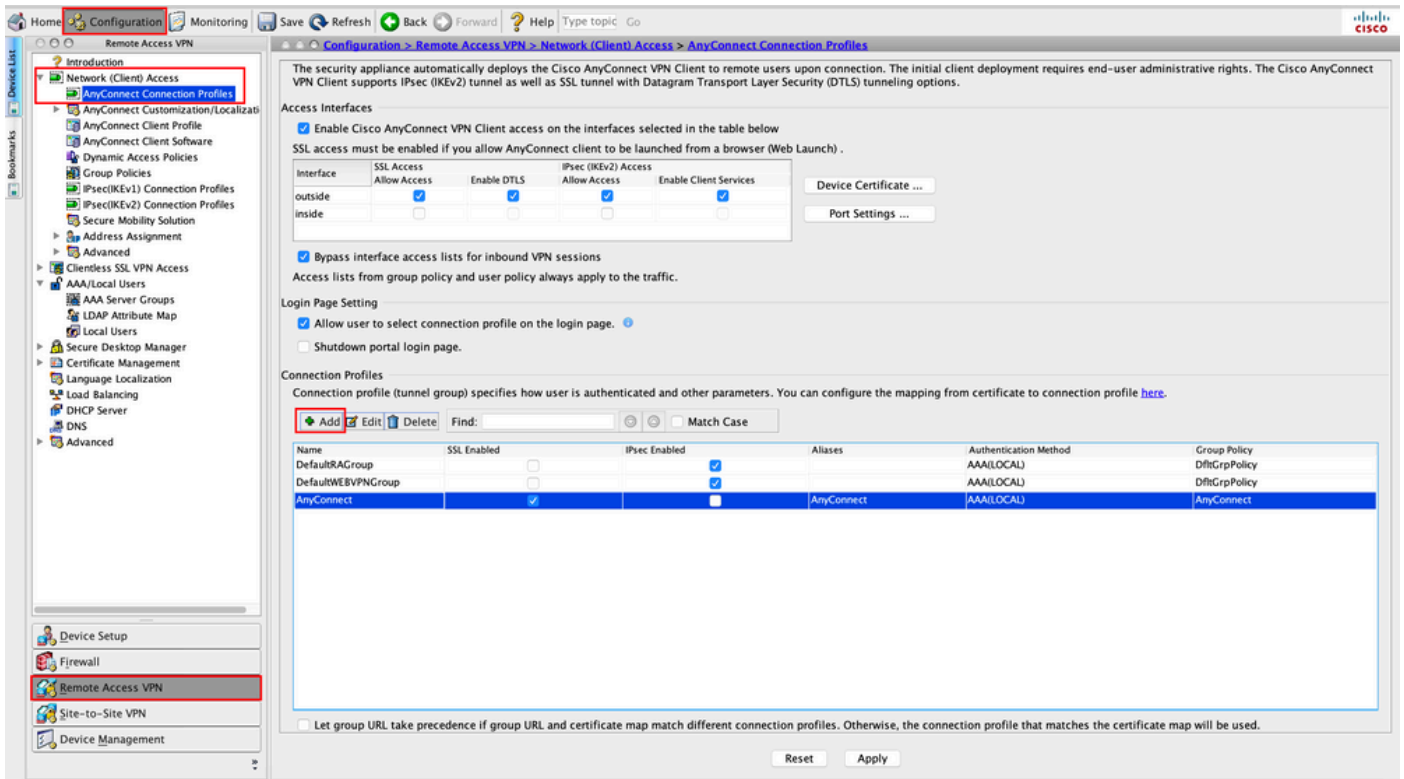
client-bypass-protocol enable

address-pools value

VPN_Pool

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Add.

هم ادخست متي ديدج AnyConnect لاصتا فيرعت فلم عاشن ن سحت رسم ل نم : عطا ل م
طوقف AnyConnect ارا د ق فنل



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	<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"/>

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](#).

Find: Match Case

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

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.

Authentication Method ك Certificate only. لي صوت ل في صوت ل Name ري فوت 7. عطا ل م
1. عطا ل م ي ف هؤاشن م ي ذل ل م لثم Group Policy رتخأ

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:

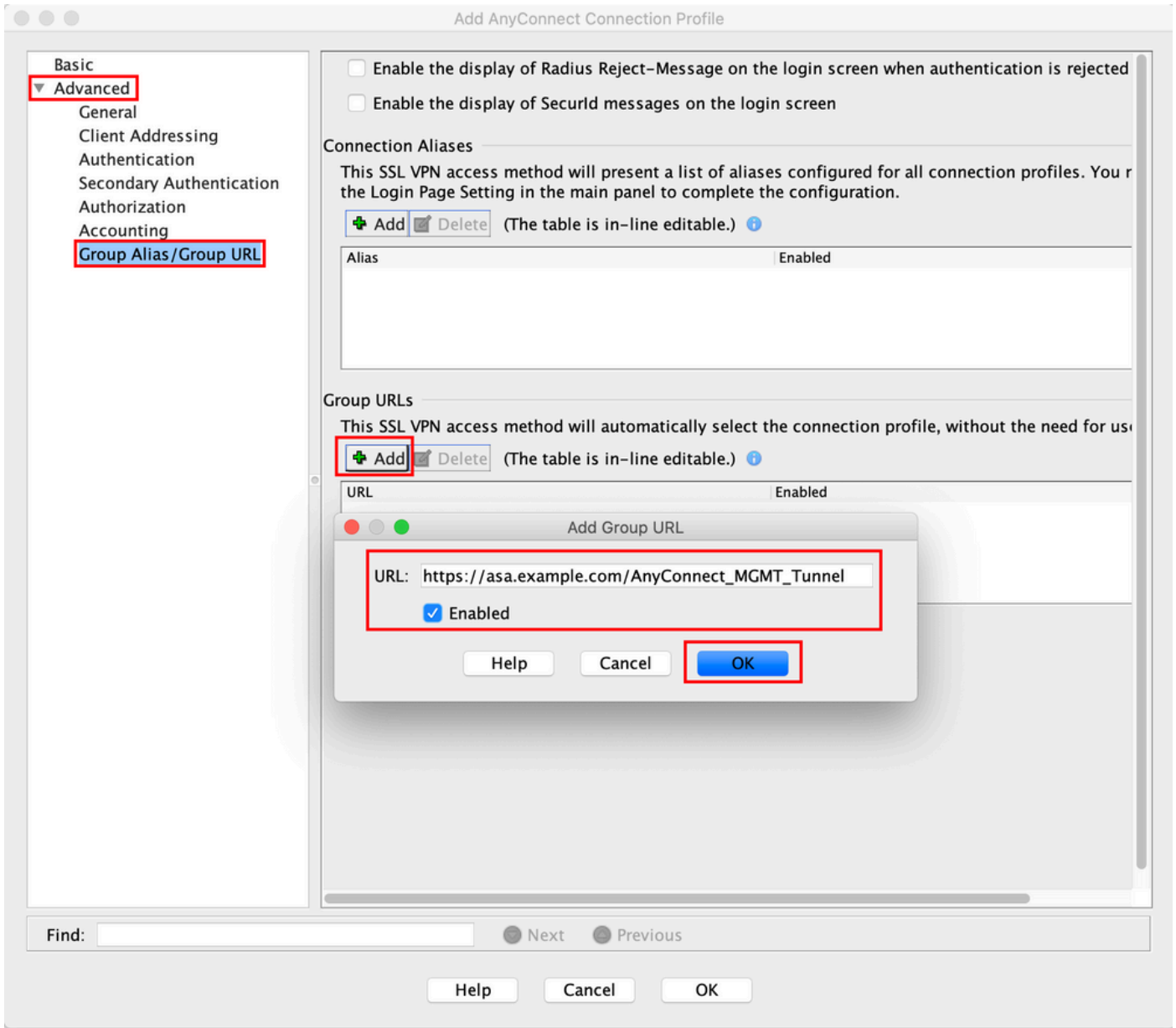
Find: Next Previous

Help Cancel OK

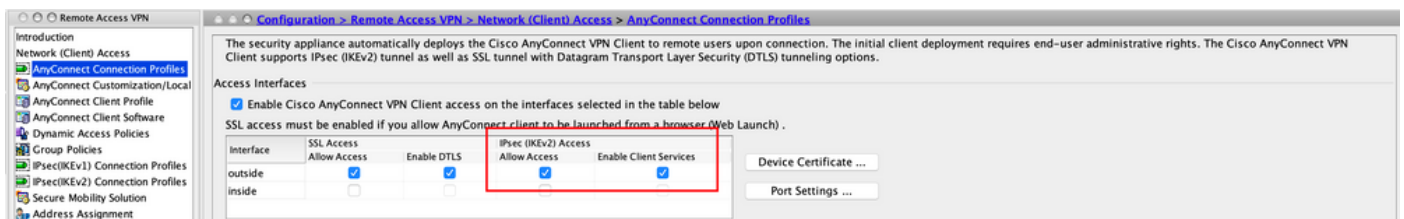
✎ لقتنا ASA ىلع ةدوجوم ىلحملا قدصملا عجرملا نم رذجلا ةداهشلا نأ نم دكأت :ةظحالم ةداهشلا ضرع/ةفاضإل Configuration > Remote Access VPN > Certificate Management > CA Certificates ىل

✎ نمخم ىف ىلحملا قدصملا عجرملا سفن نع ةرداص ةيوه ةداهش دوجو نم دكأت :ةظحالم (ىف MacOS) ماظنلا حيتافم ةلسلس ىف وأو (ىف Windows) زاهجلا تاداهش.

URL ةفاضإو Group URLs تحت Add رقنا Advanced > Group Alias/Group URL. ىل لقتنا 8 ةوطخلا ةروصولا ىف حضورم وه امك ،ظحلل OK رقنا .هديدحت مت Enabled نمضن



AnyConnect ل ةم دختس م ل ةه ج اول ا لى ع IPsec (IKEv2) Access نم دكأت ، IKEv2 مادختس ا ةل ا ح ف



ASA لى لى لكش ت ل ا ع ف دل Apply ر ق ن ا 9 ة و ط خ ل ا

CLI لى صوتل في صوتل لى كشت (tunnel-group):

```
<#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
```

ةمدختسم لاة هاولاب ةطبترم و ASA لى عاهب قووم ةداهش تيبت نم دكأت. 10 ةوطخل
ضرع/ةفاضل Configuration > Remote Access VPN > Advanced > SSL Settings لى لقتنا AnyConnect. تالاصتال
دادعإل اذه

 [ASA في ةوهل اةداهش تيبت](#) عجار: ةطخال م

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

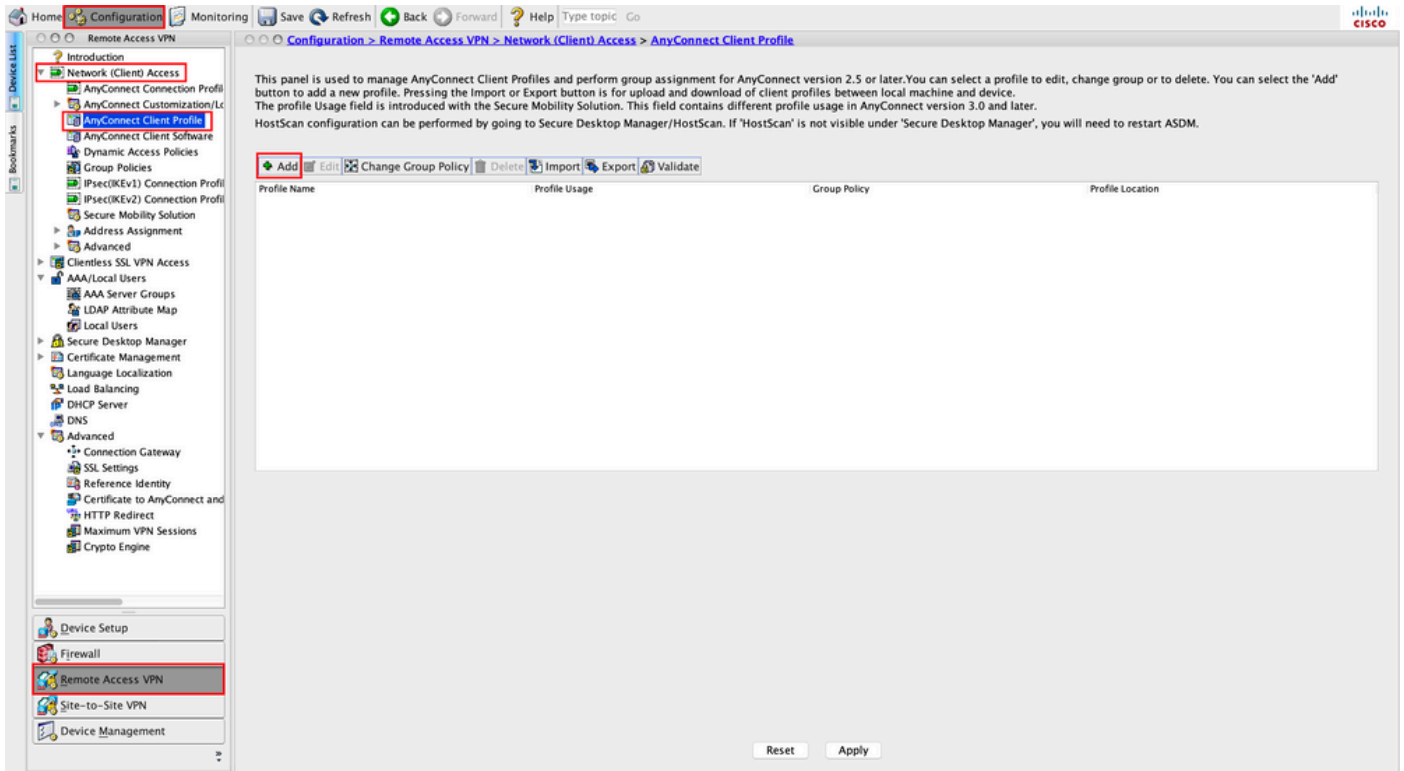
تويوك ل SSL TrustPoint ج CLI ن نيوك

<#root>

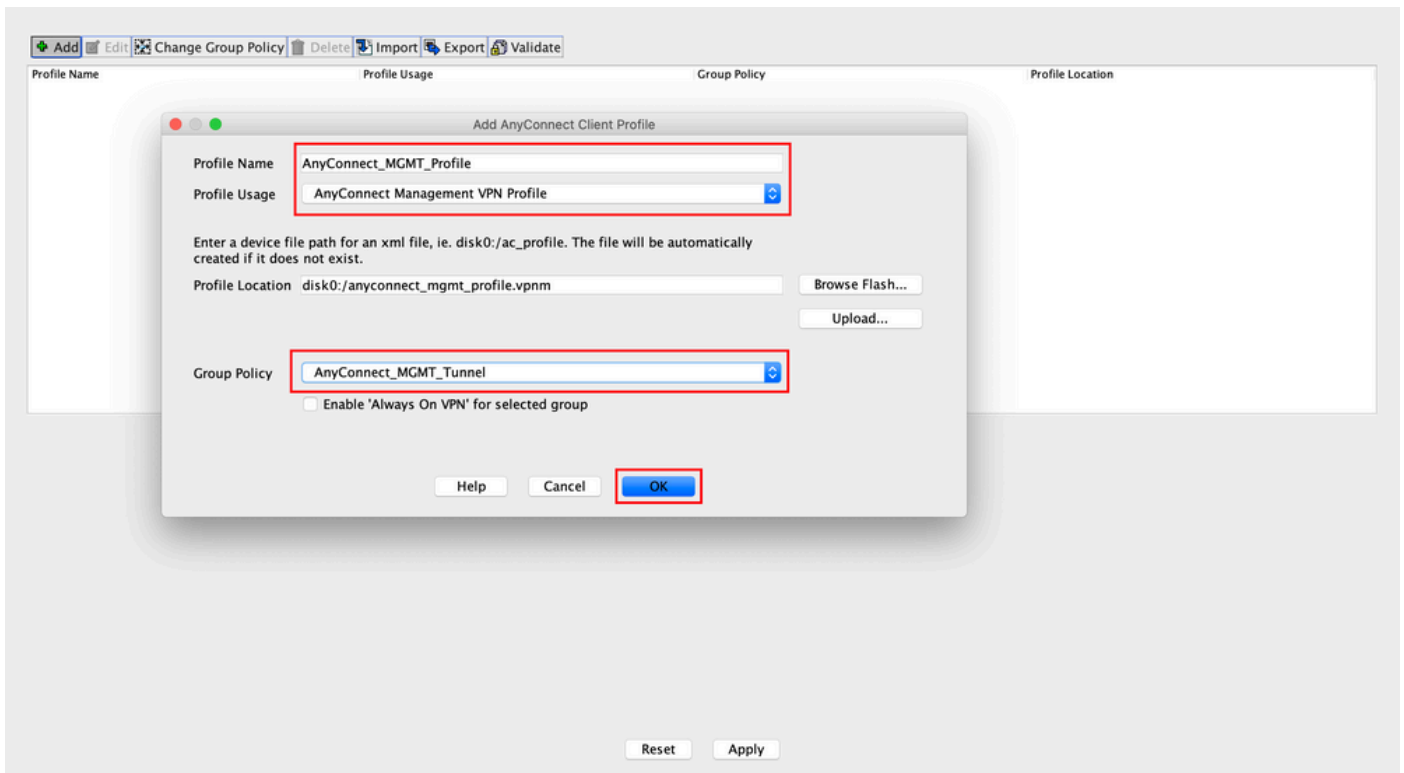
ssl trust-point ROOT-CA outside

AnyConnect Management VPN فيرعت فلم عاشن

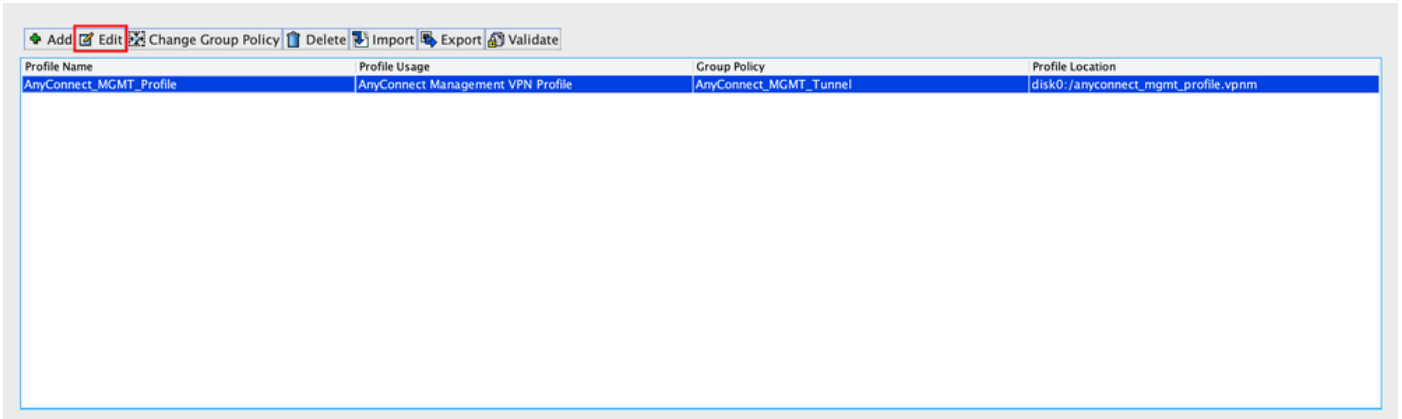
ي ل لقتنا Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. قنا Add، روم وه امك، ةوطخلال



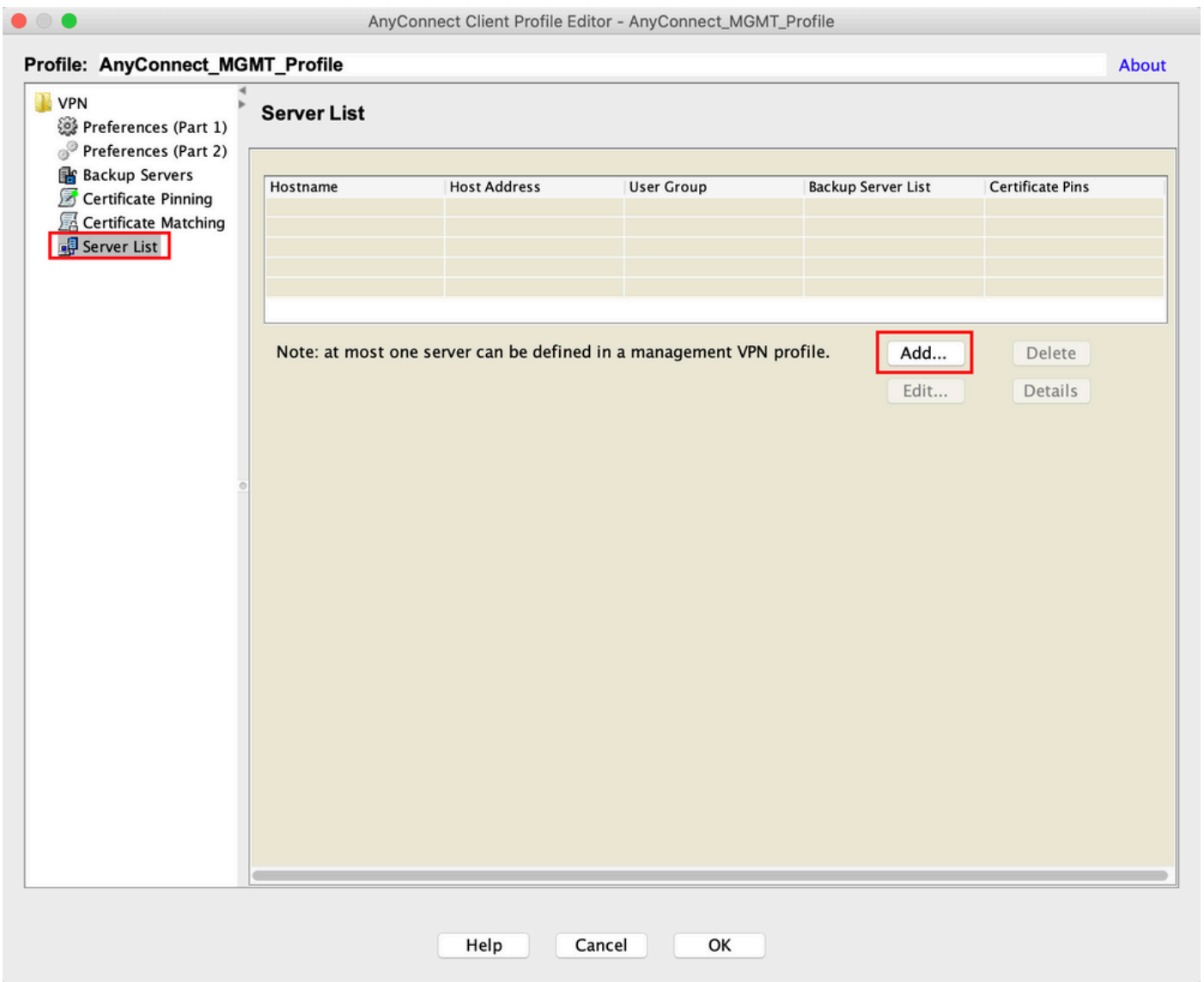
م ت Group Policy رتخأ AnyConnect Management VPN profile. ك Profile Usage رتخأ Profile Name. ريفوت 2. ةوطخلال ةروصلال ي ف حضورم وه امك ، OK رقنا 1. ةوطخلال ي ف هؤاشنإ



ةروصلال ي ف حضورم وه امك ، Edit قوف رقناو هؤاشنإ م ت يذلا فيصوتلال رتخأ 3. ةوطخلال



في حضوره وه امك ،ديج مداوخ ةمئاق لاخدا ةفاضلا Add رقنا Server List. لى لقتنا 4. ةوطخلا ةروصلا.



ةومحمل مساك User Group ريفوت .ASA لى نم FQDN/IP address ةفاضلا Display Name. ريفوت 5. ةوطخلا ةومحمل مساك User Group و FQDN عم ايئاقلت اهؤلم متي Group URL رقنا .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)

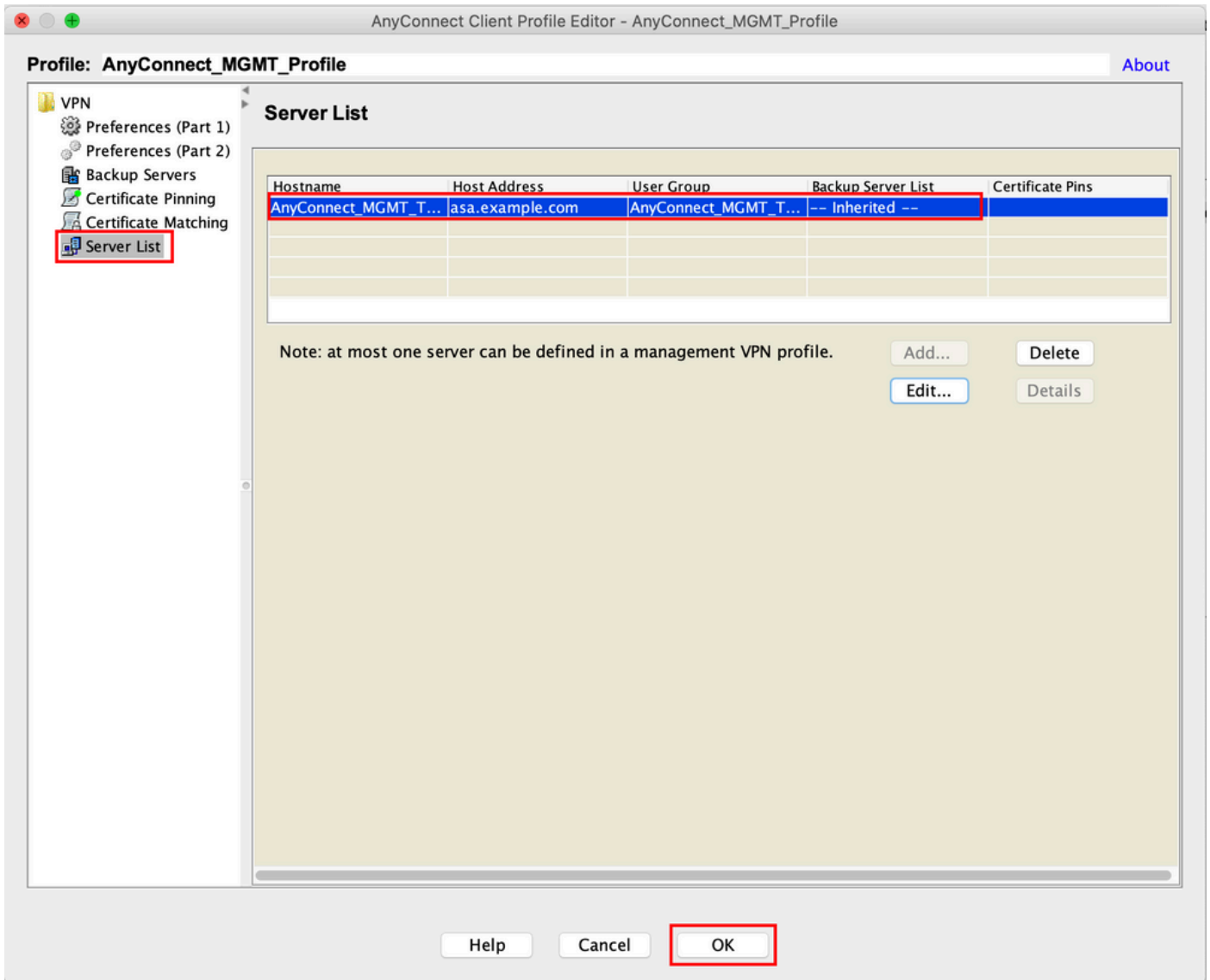
Backup Servers

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

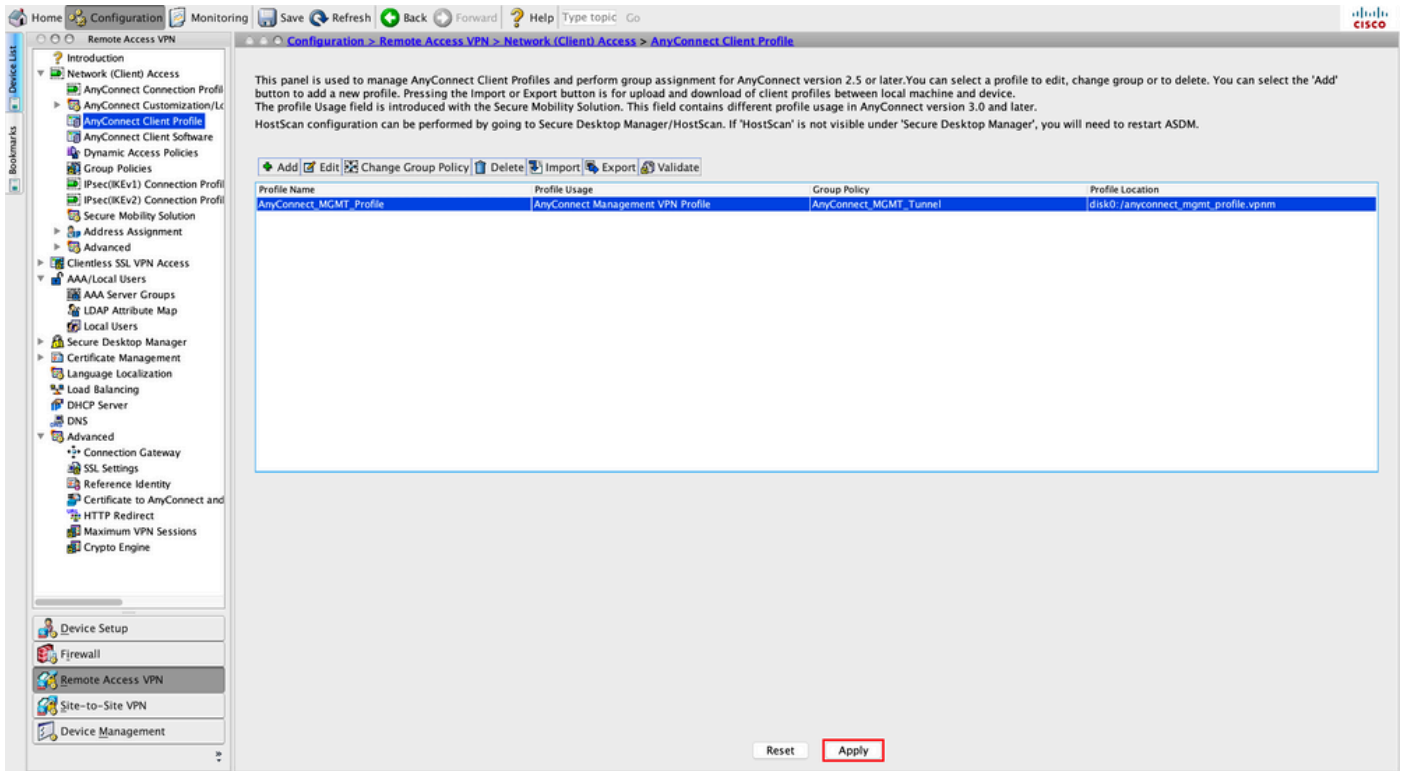
URL ناووع س فن وه نېم دخت س م ل ا ة ة وم جم + FQDN/IP ناووع نو كي ن ا ب جي : ة ظ ح ا ل م [8 ة و ط خ ل ا](#) ي ف AnyConnect ل ا ص ت ا ف ي ر ع ت ف ل م ن ي و ك ت ا ن ث ا ر و ك ذ م ل ا ة ة وم جم ل ا ب ص ا خ ل ا

VPN ة ك ب ش ا ا ش ن ا ل ل و ك و ت و ر ب ك IKEv2 ع م AnyConnect م ا د خ ت س ا ا ض ي ا ن ك م ي : ة ظ ح ا ل م [5 ة و ط خ ل ا](#) ي ف IPsec ل ا ع ه ن ي ي ع ت م ت Primary Protocol ن م ض ن . ASA ل ا ل ا ة ي ر ا د ا ل ا

ظ ف ح ل ل OK ر ق ن ا ، ة ر و ص ل ا ي ف ح ض و م وه ا م ك . 6 ة و ط خ ل ا



ةروصلال ي ف حضوم وه امك ،ASA ىلإ نيوكتلل ع ف د Apply to ر قنا . 7 ةوطخلال



AnyConnect Management VPN. فیرعت فلم ةفاض! دع ب لیكشت CLI

<#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 لڀم ع زاھج ىل ع AnyConnect Management VPN فيرعت فلم

<#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 UserControlable="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>

 فيرعت فلم في (TND) اهب قو ووملا ةكبشلا فاشتك ا مادختسا ةلاح في: ةظالم فلم في تادادع ا ل س فن ةقباطم نسحتسم ل نم ف ،مدختسم ل ل AnyConnect VPN ةراد ا ق فن ليغشت متي . ةقسا نتم مدختسم ةبرجت ل Management VPN فيرعت ةفاض ا ل ا ب و .مدختسم ل ل VPN ق فن فيرعت فلم يل ع ةقبطم ل ل TND تادادع ا يل ع ا ن ب ا م د ن ع ط ق ف ه ض ر ف م ت ي) VPN ةراد ا فيرعت فلم في TND ل اص ت ا ا ر ج ا ق ب ط ي ، ك ل ذ ي ل ا ةراد ا ق فن ا ن ا م ض ل ،مدختسم ل ل VPN ق فن يل ع ا م ئ ا د (اطشن VPN ةراد ا ق فن نو كي ي . يئاهن ل ا مدختسم ل ل ف افش VPN

 VPN ةراد ا فيرعت فلم ن ا ك ا ذ ا ، يئاهن ل ا مدختسم ل ل ي ص خ ش ر ت و ي ب م ك ي ا في: ةظالم ذ خ ا ي ه ن ا ف ، د و ق ف م م د خ ت س م ل ا ب ص ا خ ل ا VPN فيرعت فلم ن ا ك ا ذ ا و ة ن ك م م TND تادادع ا ب ي ف ا ه ل ي ط ع ت م ت ي) TND ل ة ي ض ا ر ت ف ا ل ا ت ا ل ي ض ف ت ل ا تادادع ا ر ا ب ت ع ا ل ا ي ف VPN فيرعت فلم ن م ا ل د ب (AC ل ي م ع ق ي ب ط ت ي ف ة ي ض ا ر ت ف ا ل ا ت ا ل ي ض ف ت ل ا د د ح م ر ي غ / ع ق و ت م ر ي غ ك و ل س ي ل ا ا ذ ه ق ب ا ط ت ل ا م د ع ي د و ي د ق . د و ق ف م ل ا م د خ ت س م ل ل ة ي ض ا ر ت ف ا ل ا ت ا ل ي ض ف ت ل ا ي ف TND تادادع ا ل ي ط ع ت م ت ي ، ي ض ا ر ت ف ا ل ك ش ب ي ف ا ت ب ا ث ا ر ي ف ش ت ة ر ف ش م ل ا ت ا ل ي ض ف ت ل ل ة ي ض ا ر ت ف ا ل ا تادادع ا ل ا يل ع ب ل غ ت ل ل يل ع يئاهن ل ا م د خ ت س م ل ا ر ت و ي ب م ك ي و ت ح ي ن ا ب ج ي ، AnyConnect Client ق ي ب ط ت ر ا ي ت ل ا ةراد ا ل VPN فيرعت فلم و م د خ ت س م ل ل VPN فيرعت فلم و ، VPN ي في صوت TND تادادع ا س فن يل ع ا م ه ن م ا ل ك ي و ت ح ي ن ا ب ج ي و ، د د ر ت م ل ا VPN ق فن ا ش ن ا ل ه ن ا ي ف ا ه ل ص ف و ةراد ا ل ل VPN ق فن ل اص ت ا ا ر و ق ط ن م ل ا ل ث م ت ي م د خ ت س م ل ل VPN فيرعت فلم ل TND تادادع ا د د ر ت م ل ا ر ا ي ت ل ا ل م ا ع م د خ ت س ي ، ةراد ا ل ل فيرعت فلم ل TND تادادع ا ن م ق ق ح ت ي ه ن ا ف ، Management VPN ق فن ل اص ت ا ع ط ق ل و ةراد ا ل ل VPN .

AnyConnect ةراد ا ب ص ا خ ل ا VPN في صوت ل ر ش ن ل ا ب ي ل ا س ا

- فلم ل ي ز ن ت ل ASA ل اص ت ا فيرعت فلم ب م د خ ت س م ل ل ح ج ا ن VPN ل اص ت ا ل ا م ك ا م ت ي VPN ة ب ا و ب ن م AnyConnect Management VPN فيرعت

 ا ش ن ا م ز ل ي ، IKEv2 و ه Management VPN ق فن ل م د خ ت س م ل ا ل و ك و ت و ر ب ل ا ن ا ك ا ذ ا : ةظالم (ASA ن م AnyConnect Management VPN فيرعت فلم ل ي ز ن ت ل) SSL ل ا ل خ ن م ل اص ت ا ل و ا

- نم اما ليمعلا ةزهجأ ىلإ ايودي AnyConnect ةرادب صاخلا VPN فيرعت فلم ليمحت نكمي فلم مسانم دكأت) ايودي لتيبثتال قيرط نع وأ (GPO) ةومجملا جهن نئاك عفدلال (VpnMgmtTunProfile.xml) فيرعتال.

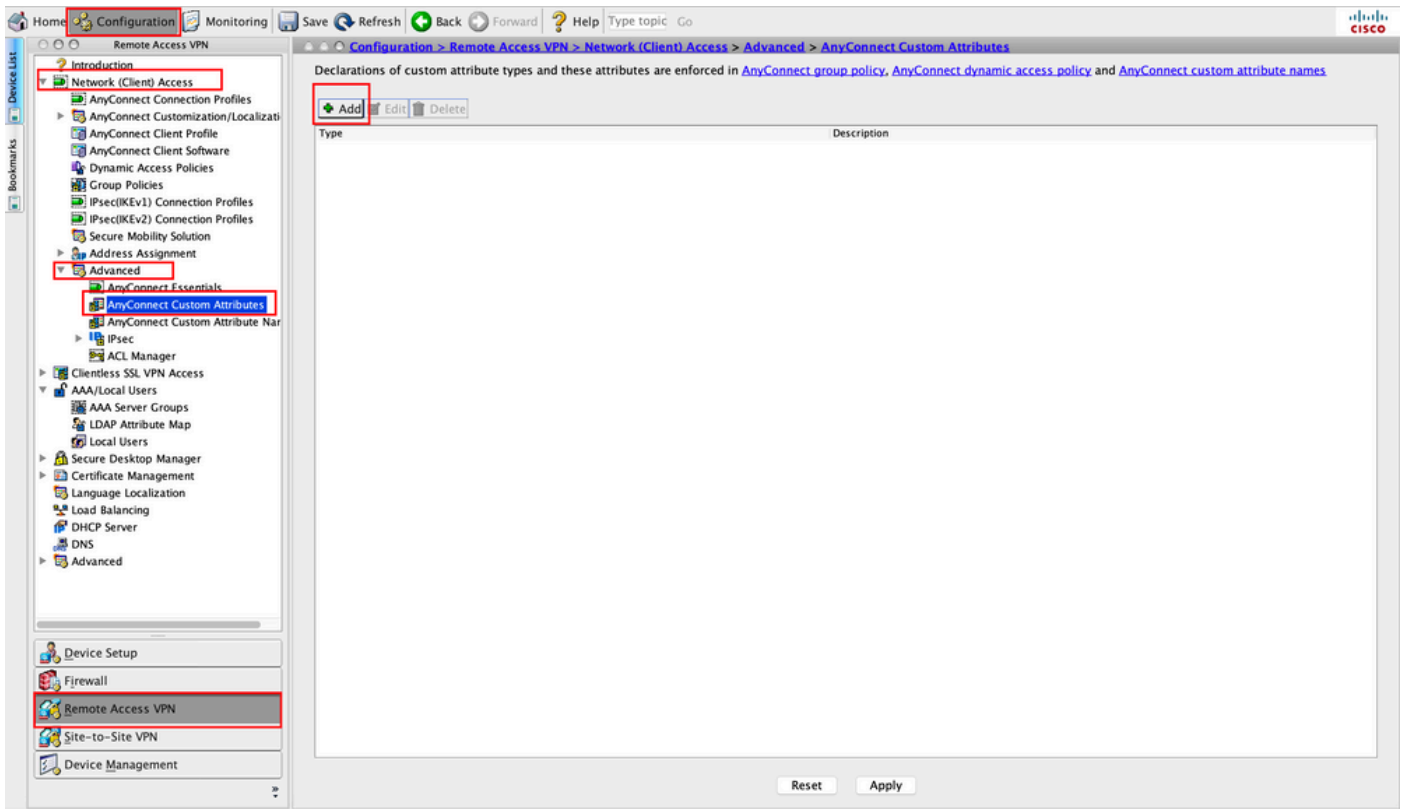
هيلي فيرعتال فلم ةفاضل بجي يذلا دلجملا عقوم:

Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun
 س: /opt/cisco/anyconnect/profile/mgmttun/ وأ كام

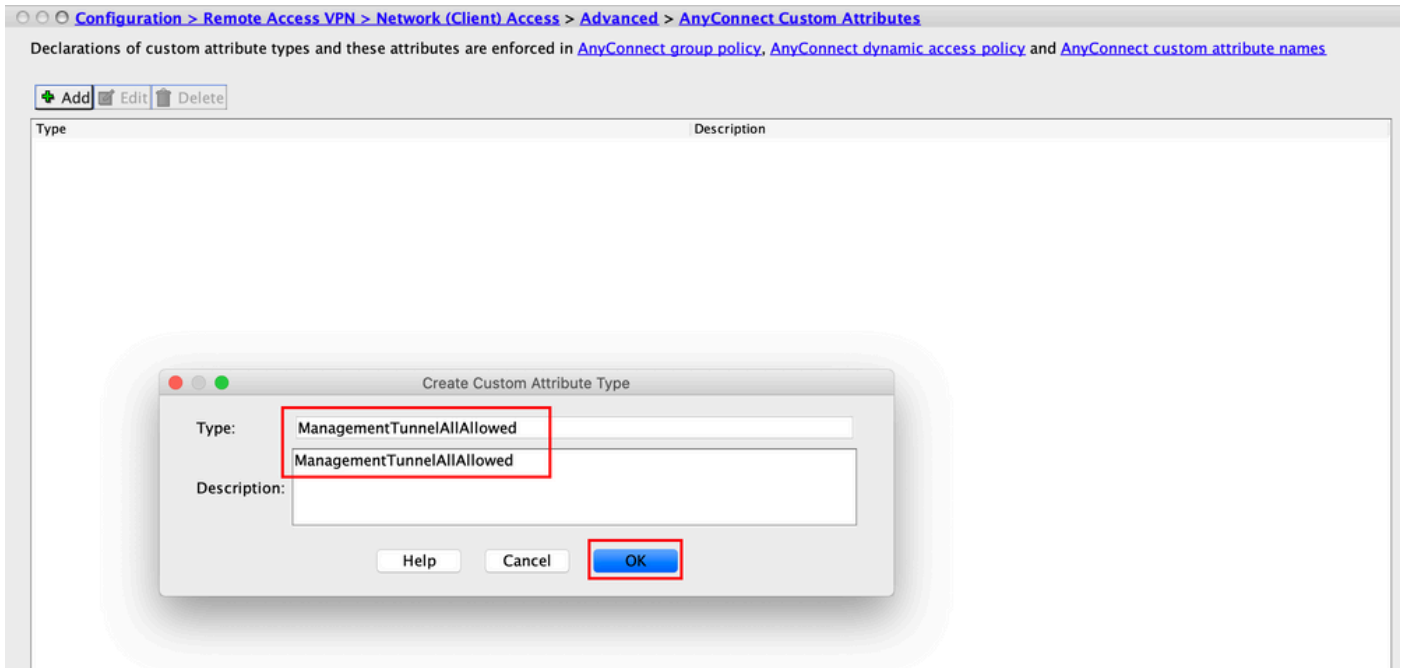
قفنل ربع لكلكل نيوكت معدلة صصخم ةمس نيوكت ب مق (يرايخا)

بنجتل، ايضارتفا، tunneling ليكشت نمضتي اماسقن Management VPN قفن بلطتي ةمسلا نيوكت دنع ءارجلا اذه زواجت نكمي. مدختسملا هأب يذلا ةكبشلا لاصتا ىلع ريثأت ةرادال قفن لاصتا لبق نم مدختسملا ةومجملا جهن في ةصصخملا.

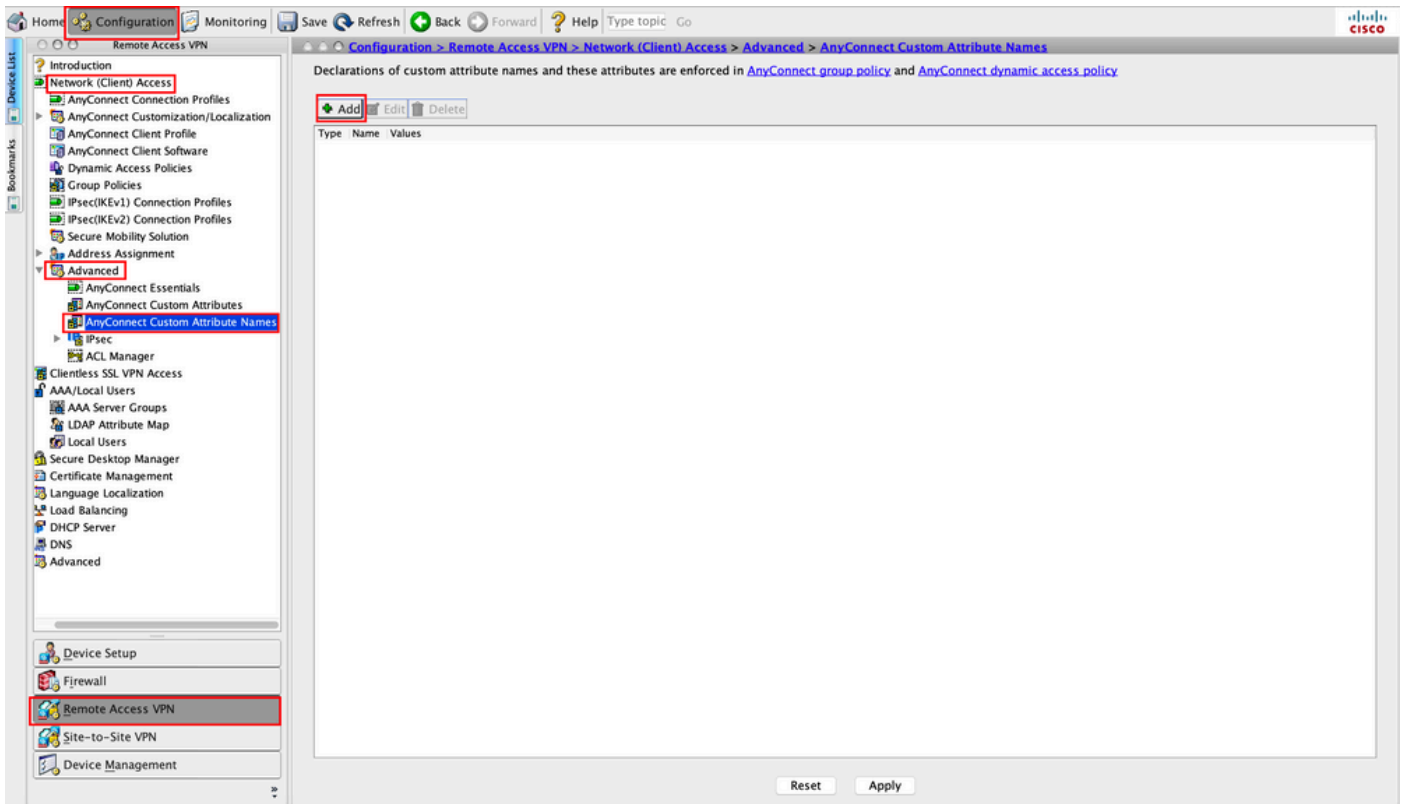
ةوطخلل 1. Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. رونا Add، وه امك.



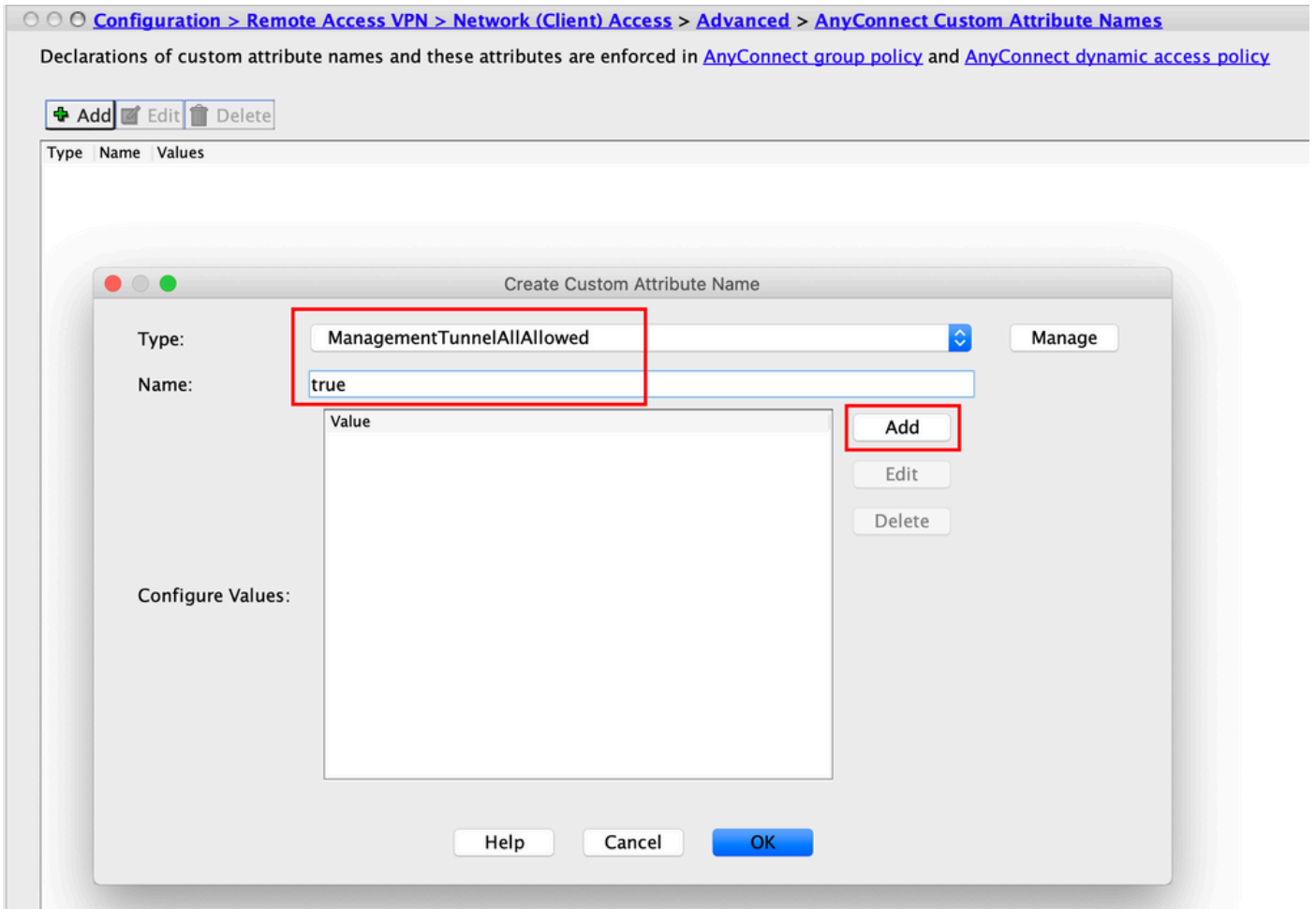
ميديقتو Description ManagementTunnelAllAllowed ىلإ ةصصخملا ةمسلا عون نييغت 2. ةوطخلل ةروصلال في حضورم وه امك، OK رونا.



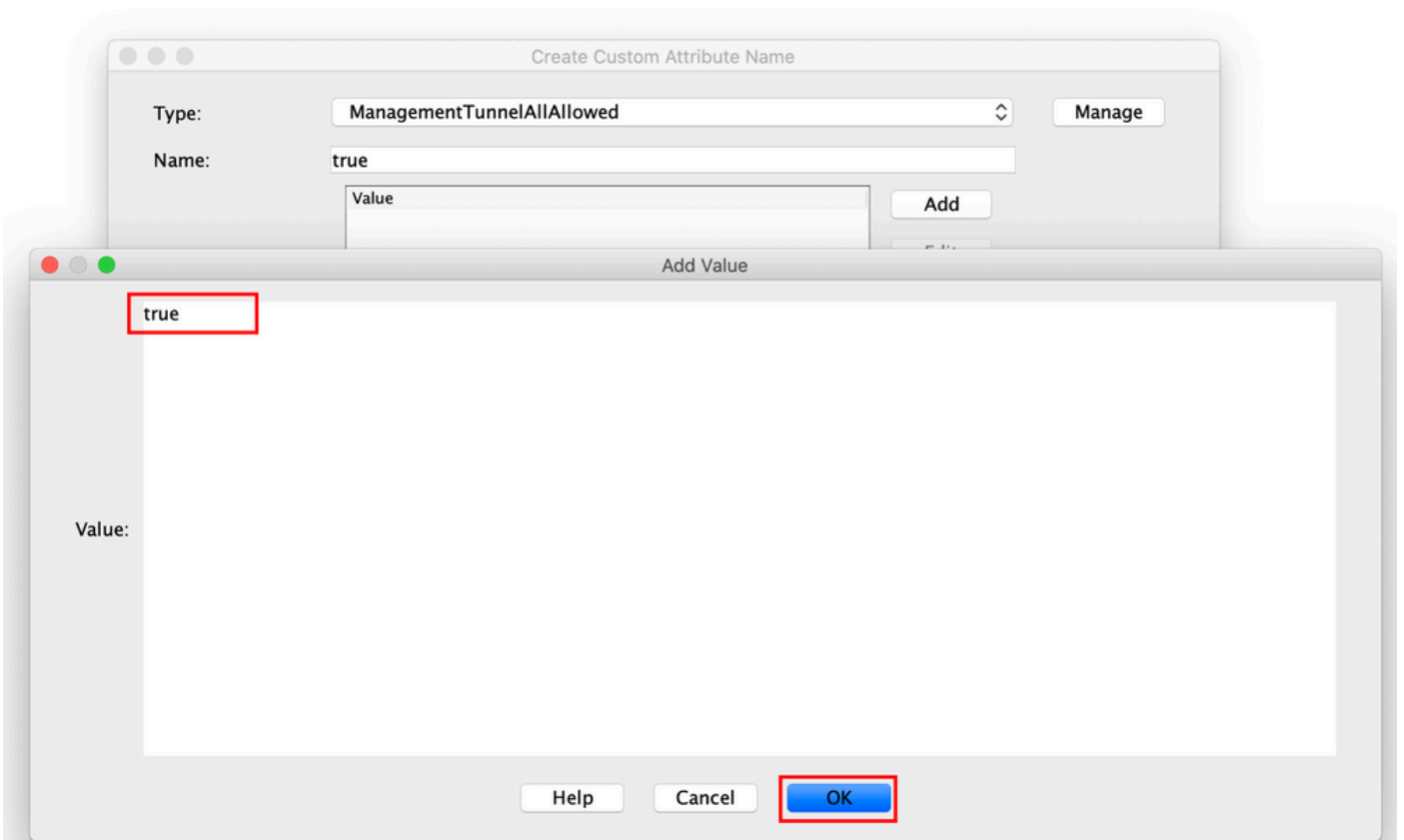
3. لإلقتنا Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. ةروصلال يف حضورم وه امك، رقنا Add،



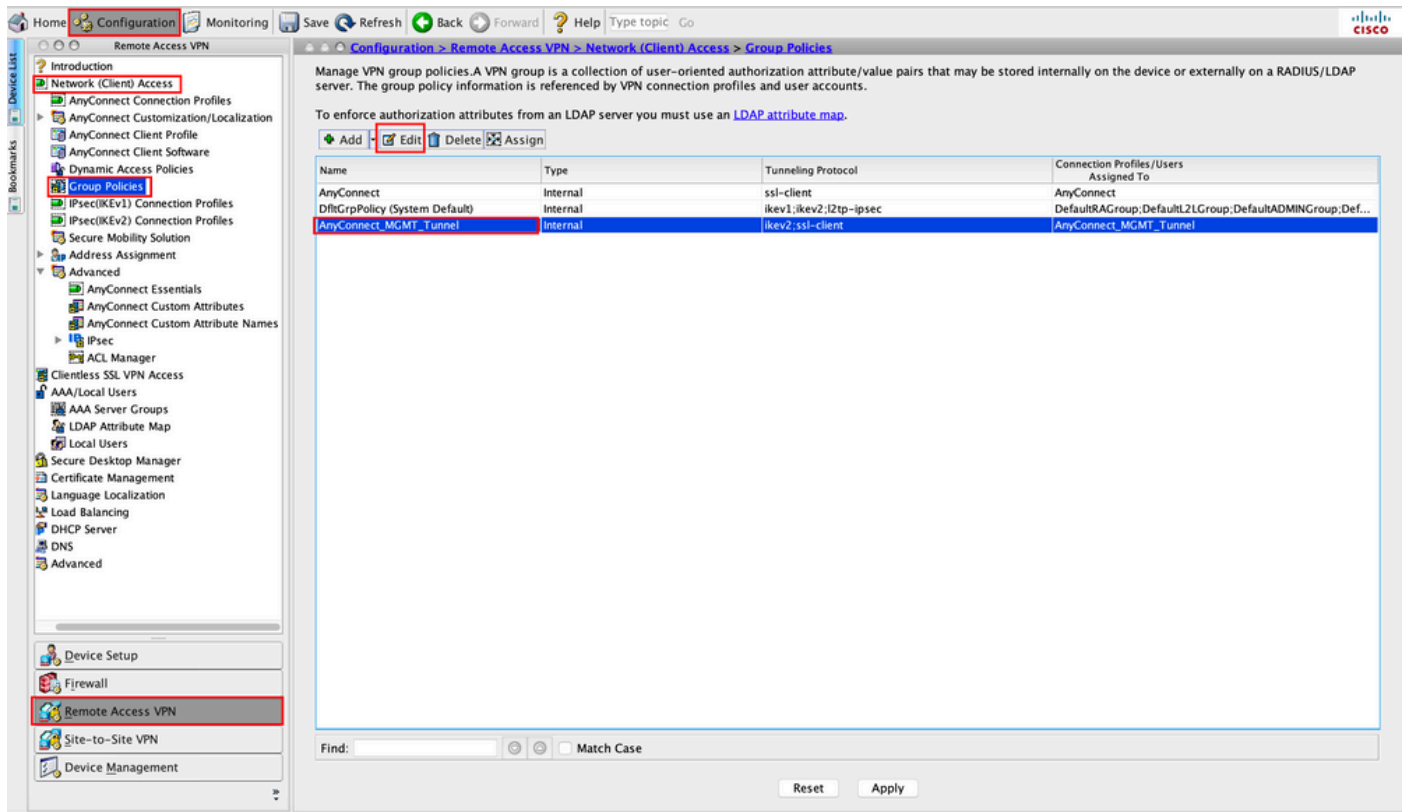
4. ةوطخلال ريفوتل Add رقنا true. ك مسالال نييغت . ManagementTunnelAllAllowed مساب عونلار تخأ. ةوطخلال ةروصلال يف حضورم وه امك، ةصصخم ةمس ةميقي



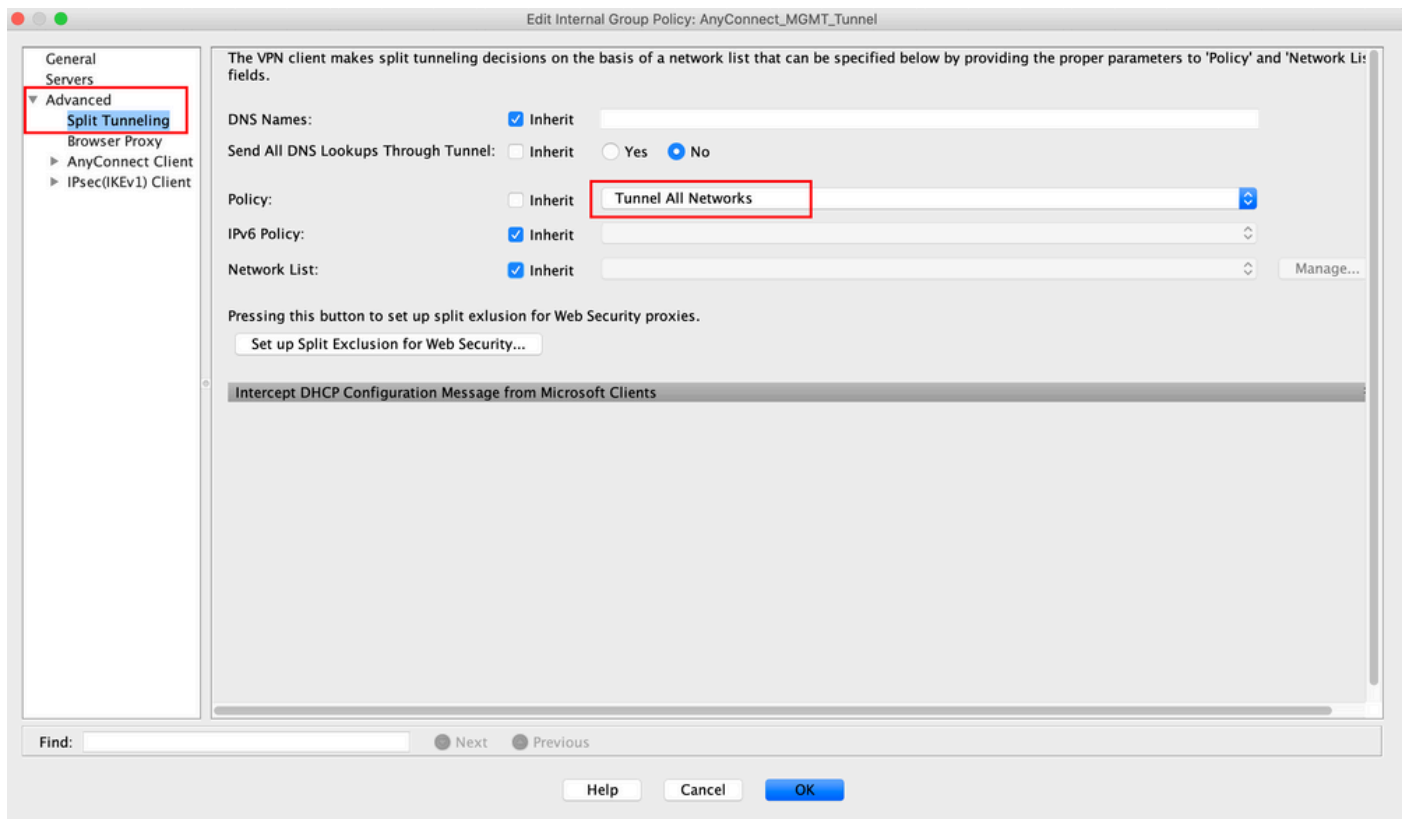
ةروضلا يف حضوم وه امك ، OK رقنا true. ك ةميقلا نبيعت 5. ةوطخلا



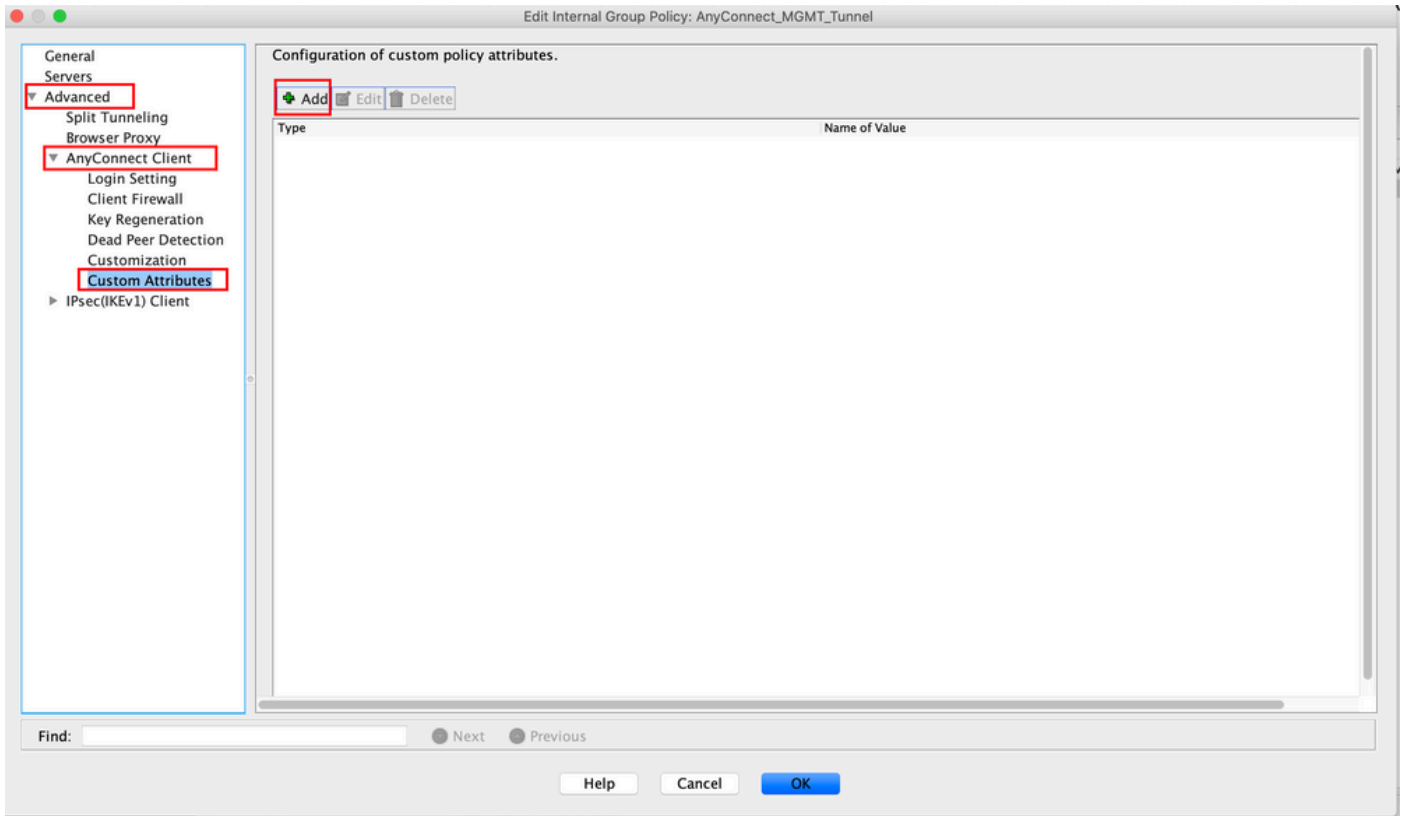
جهن رتخأ Configuration > Remote Access VPN > Network (Client) Access > Group Policies. إلالق تنا 6. ةوطخلال ةروصلال يف حضوم وه امك ، Edit رقنا .ةومجمل



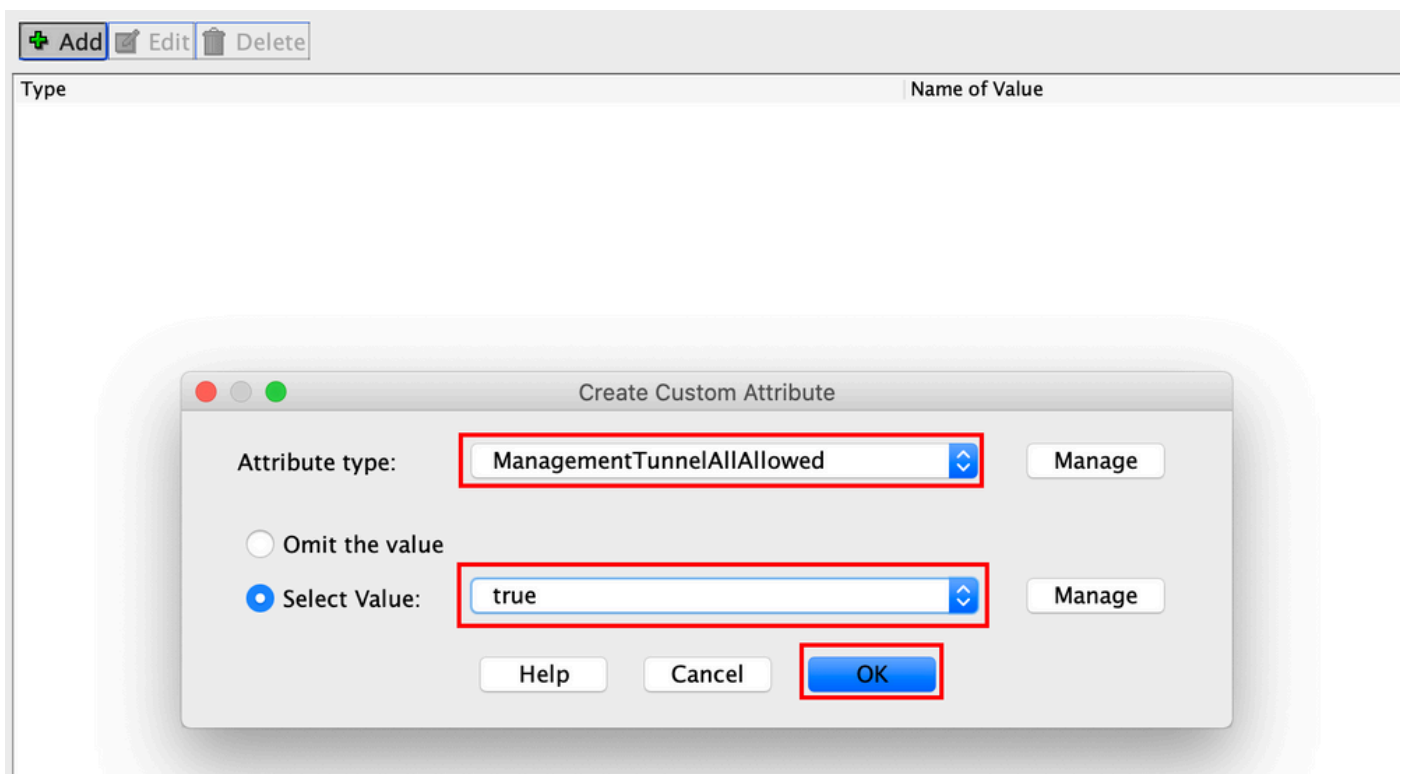
Tunnel ك جهنلال نيوكت Advanced > Split Tunneling. إلالق تنا ،ةروصلال هذه يف حضوم وه امك 7. ةوطخلال All Networks.



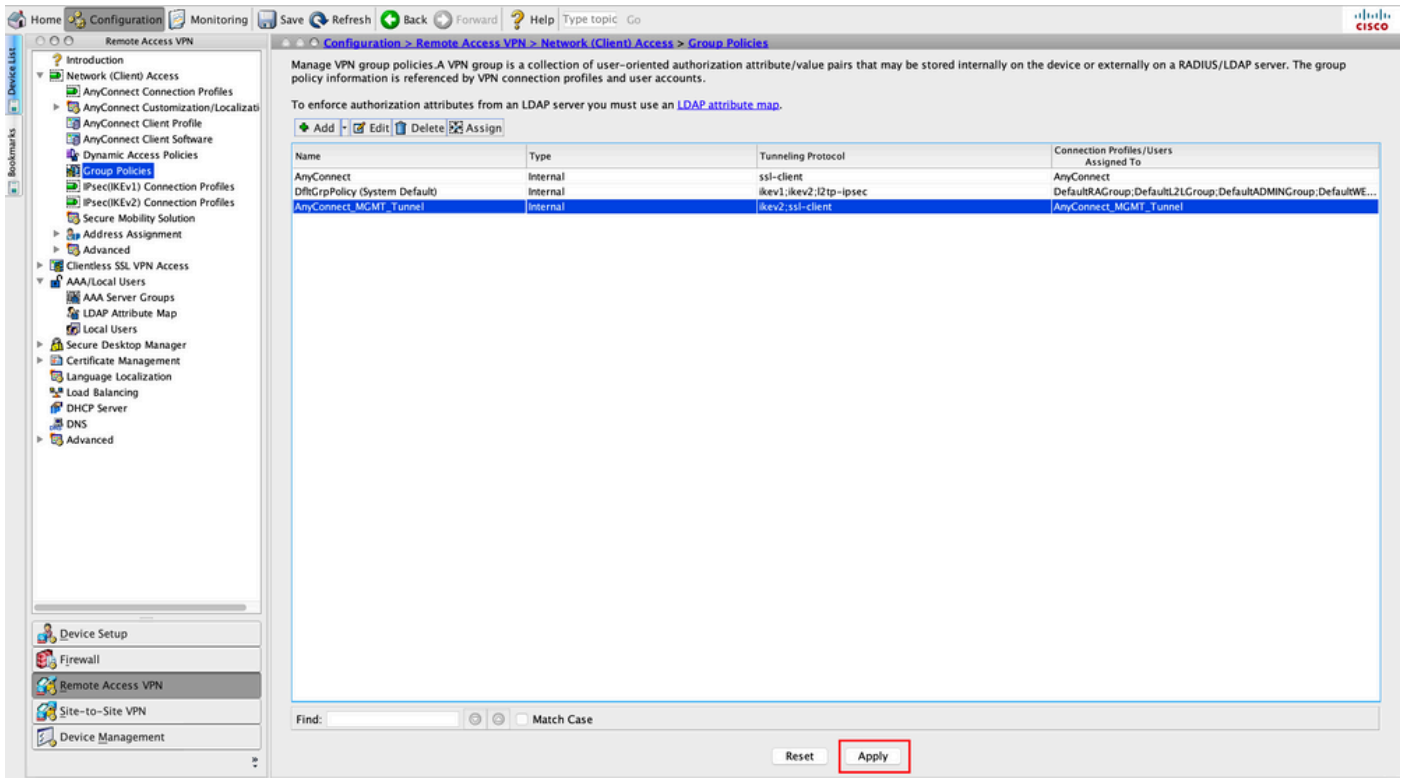
ةروصلال يف حضوم وه امك ، Add رقنا Advanced > Anyconnect Client > Custom Attributes. إلالق تنا 8. ةوطخلال



حضوره وه امك، OK رقنا true كة ميقول ارتخاو ManagementTunnelAllAllowed كة مسلال عون رتخأ. 9 ةوطخلا ةروصللا يف.



ةروصللا يف حضوره وه امك، ASA إىل نيوكتلا عفدل Apply رقنا. 10 ةوطخلا



عصصخملا ةمسلا ةفاضإ تمت ManagementTunnelAllAllowed ل دعب ليكشت CLI:

```
<#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
```

ةحصل لآ نم ققحت لآ

show vpn-sessiondb detail Management VPN قفن لآصتا نم ققحت
anyconnect erasecat4000_flash:.

<#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:

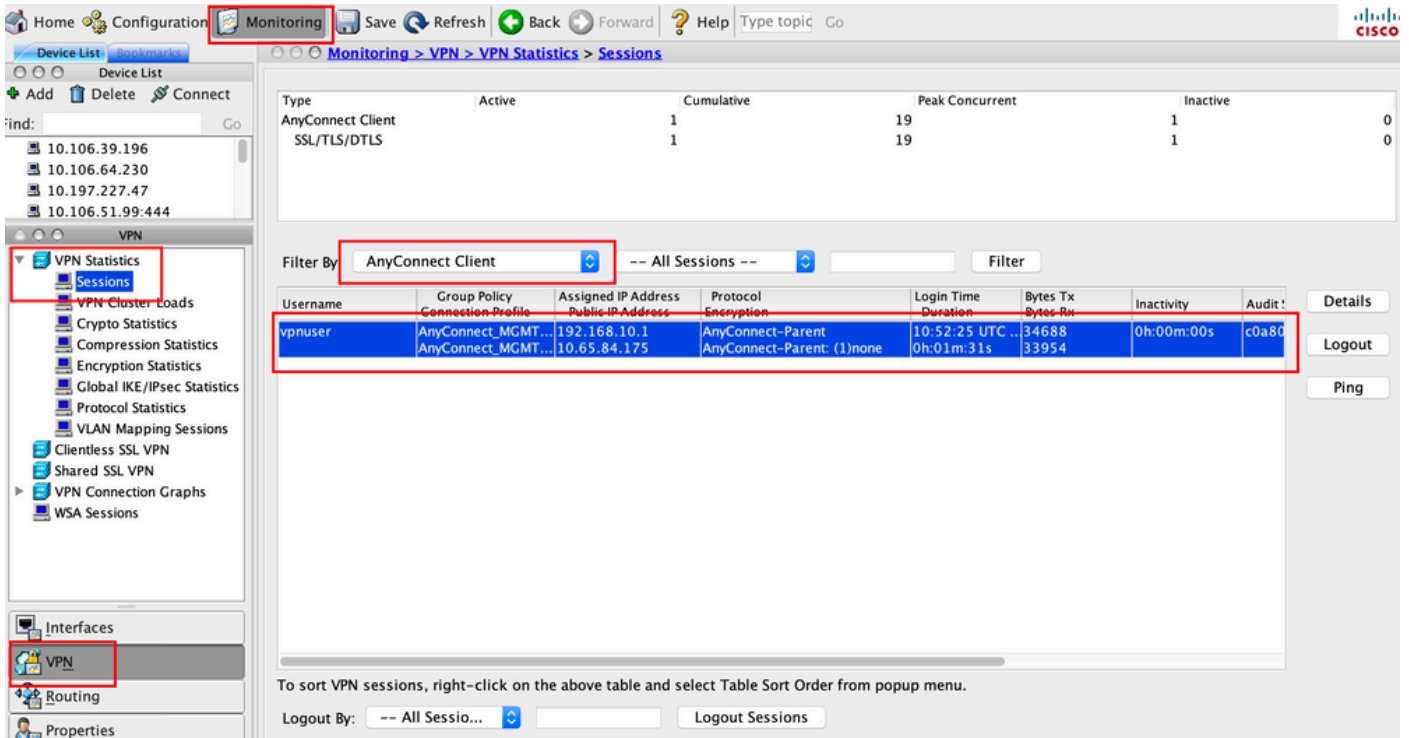
Tunnel ID : 10.3
Assigned IP : 192.168.10.1 Public IP : 10.65.84.175
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 57053
UDP Dst Port : 443

Auth Mode : Certificate

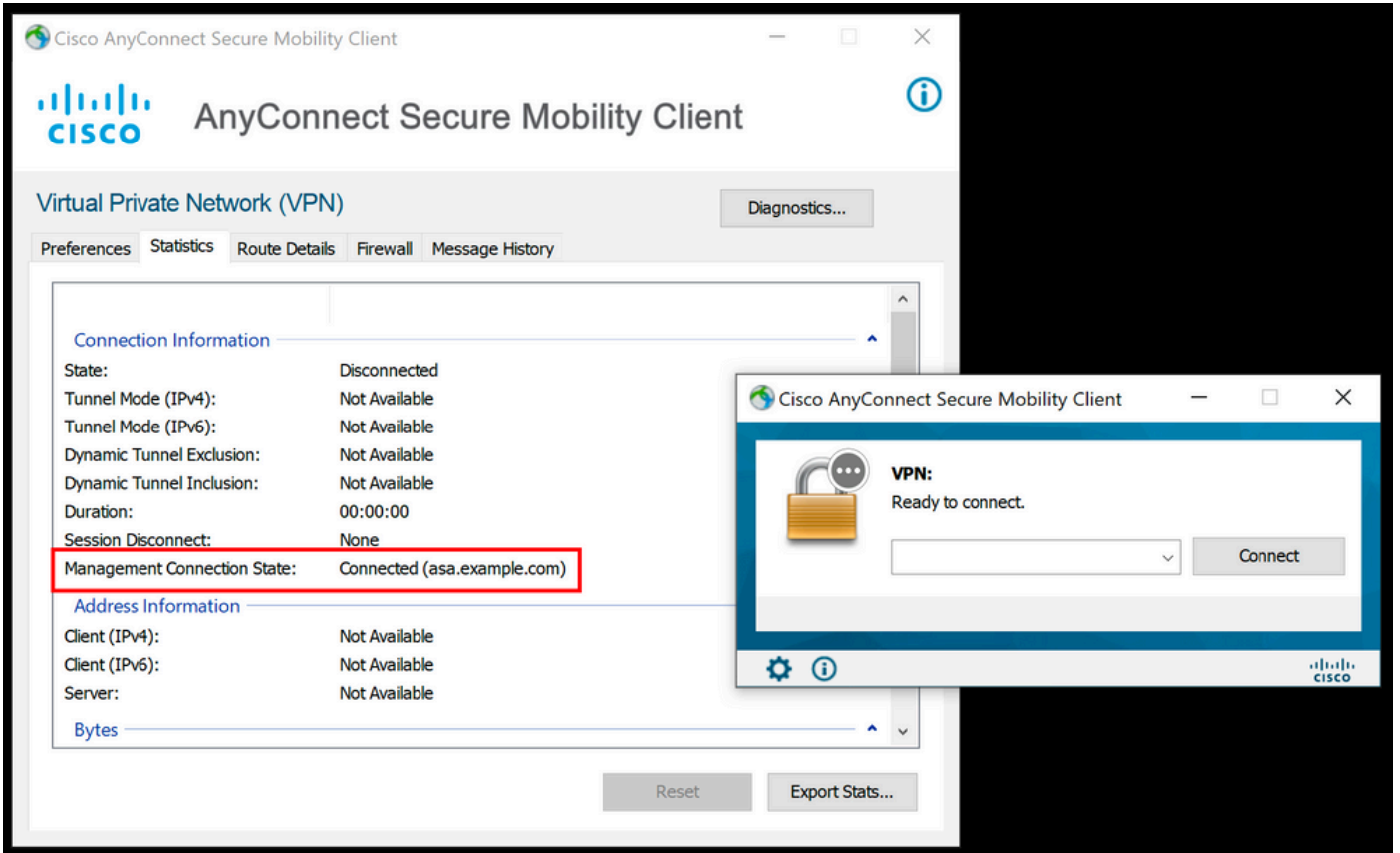
Idle Time Out: 30 Minutes Idle TO Left : 18 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03036
Bytes Tx : 17238 Bytes Rx : 1988
Pkts Tx : 12 Pkts Rx : 13
Pkts Tx Drop : 0 Pkts Rx Drop : 0

ليعمل على ASDM VPN Management قفنا لاصتا نم ققحت

ليعمل على طساوب ةي فصت ال . لمعمل ال اسلج > VPN > تايئ اصح | > VPN > ةبقارم ال لقتنا
ليعمل ال لمعمل ال اسلج ضرعل AnyConnect



ليعمل ال زاهاج ال قفنا لاصتا نم ققحت ال:



اه حال صا و عا ط خا ل فاش ك ت سا

فاش ك ت سا ل (ة را دا ل ل اص تا ة ل ا ح) ة دي د ج ل م د خ ت س م ل ا ه ج ا و ت ا ي ئ ا ص ح ا ر ط س م ا د خ ت س ا ن ك م ي ل و ق ت ا م و م ع د ه ا ش ت ي ت ل ا ع ا ط خ ا ل ي ه ه ذ ه و . ا ه ح ا ل ص ا و ة را دا ل ل ق ف ن ل اص تا ع ا ط خ ا

(ل ط ع م) ل اص تا ل ا ع ط ق م ت :

- ة ل ط ع م ة ز ي م ل ا .
- ر ب ع ، ل ي م ع ل ا ل ل ة را دا ل ل (VPN) ة ي ر ه ا ظ ل ا ة ص ا خ ل ا ة ك ب ش ل ا ف ي ر ع ت ف ل م ر ش ن ن م د ك ا ت ة ي ر ه ا ظ ل ا ة ص ا خ ل ا ة ك ب ش ل ا ف ي ر ع ت ف ل م ة ف ا ص ا ك ن م ب ل ط ت ي) م د خ ت س م ل ا ق ف ن ل اص تا ل ي م ح ت ل ل ا ل خ ن م ق ا ط ن ل ا ج ر ا خ و ا (م د خ ت س م ل ا ق ف ن ة ع و م ج م ة س ا ي س ل ل ة را دا ل ل (VPN) ف ي ر ع ت ل ل ف ل م ل ي و د ي ل ا .
- ق ف ن ن م ص ت ي ن ا ل خ د م د ي ح و ف ي ض م ع م ص ي ص خ ت ب و ل س ا VPN ة را دا ل ل ت ل ك ش ن ا ت ن م ص ة ع و م ج م .

(ا ه ب ق و ث و م ة ك ب ش) ل ص ت م ر ي غ :

- ة را دا ل ل ق ف ن ء ا ش ن ا م ت ي م ل ك ل ذ ل ا ه ب ق و ث و م ة ك ب ش TND ف ش ت ك ا .

(ط ا ش ن م د خ ت س م ل ا ق ف ن) ل اص تا ل ا ع ط ق م ت :

- ا ي ل ا ح ط ا ش ن م د خ ت س م ل ل VPN ق ف ن .

(ةي لمعلا ليغشت لشف) لاصتال عطق مت

- ةرادال قفن لاصتال ةلواحم دنع ةي لمعلا ءدب لشف ةفداصم تمت

(ل لاصتال لشف) لصتم ريغ

- ةرادال قفن ءاشنإ دنع لاصتال لشف ةفداصم تمت
- ةومجملا هن يف راعش دجوي الو، قفنل ةومجم يف ةداهشلا ةقداصم نيوكت نم دكأت، اهب قووثوم مداخل ةداهش نوكت نأ بجيو

(حل لاص ريغ VPN نيوكت) لصتم ريغ

- VPN مداخل نم حل لاص ريغ يف قفن ميسقت نيوكت يقلت مت
- ةرادال قفن ةومجم هن يف قفنل لاصتال ميسقت نيوكت نم ققحت

(قلعم جم انربل لثي دحت) لاصتال عطق مت

- اي للاح قلعم AnyConnect جم انرب لثي دحت

ل لاصتال عطق مت

- رخآ ببسل هؤاشنإ رذعت وأ ةرادال قفن ءاشنإ كشوأ دقل

اهحلص او ءاطخال فاشكتسأ نم ديزمل [DART](#) عي مجت ب مق

ةلص تاذا تامولعم

- [Management VPN قفن نيوكت](#)
- [اهحلص او ءاطخال فاشكتسأ ةرادال VPN قفن](#)
- [Cisco Systems - تادنتس مل او ينقتل لمعدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومجم مادختساب دن تسمل اذ Cisco تمچرت
ملاعلاء ان اعيمچ يف نيمدختسمل معدى وتحم مي دقتل ليرشبل او
امك ةقيد نوك تن ل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco ي لخت. فرتم مچرت مامدقي يتل ل ةيفارتهال ةمچرتل عم لال او
ىل إأمئاد ةوجلابل يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزيلچنل دن تسمل