使用 ASA 上的分割通道設定 AnyConnect Secure Mobility 用戶端

目錄

簡介

本文檔介紹如何在運行軟體版本9.3(2)的思科自適應安全裝置(ASA)上通過思科自適應安全裝置管理器(ASDM)配置Cisco AnyConnect安全移動客戶端。

必要條件

需求

Cisco AnyConnect安全移動客戶端Web部署包應下載到本地案頭，ASDM可從該案頭訪問ASA。要下載客戶端軟體包，請參閱Cisco AnyConnect安全移動客戶端網頁。可以將各種作業系統(OS)的Web部署包同時上傳到ASA。

以下是各種作業系統的Web部署檔名：

- Microsoft Windows OS - *AnyConnect-win-<version>-k9.pkg*
- Macintosh(MAC)OSs - *AnyConnect-macosx-i386-<version>-k9.pkg*

- **Linux操作**系統- *AnyConnect-linux-<version>-k9.pkg*

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA版本9.3(2)
- ASDM版本7.3(1)101
- AnyConnect版本3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

本文詳細介紹如何通過ASDM使用Cisco AnyConnect配置嚮導來配置AnyConnect客戶端並啟用分割隧道。

分割隧道用於只有特定流量必須進行隧道傳輸的情況，而不是所有客戶端電腦生成的流量在連線時通過VPN的情況。預設情況下，使用AnyConnect配置嚮導將在ASA上生成*全通*道配置。必須單獨配置拆分隧道，本文檔部分對此有進一步的詳細說明。

在此配置示例中，目的是通過VPN隧道傳送用於10.10.10.0/24子網（ASA後面的LAN子網）的流量，並且來自客戶端電腦的所有其他流量都通過自己的網際網路電路轉發。

AnyConnect許可證資訊

以下連結指向有關Cisco AnyConnect安全移動客戶端許可證的有用資訊：

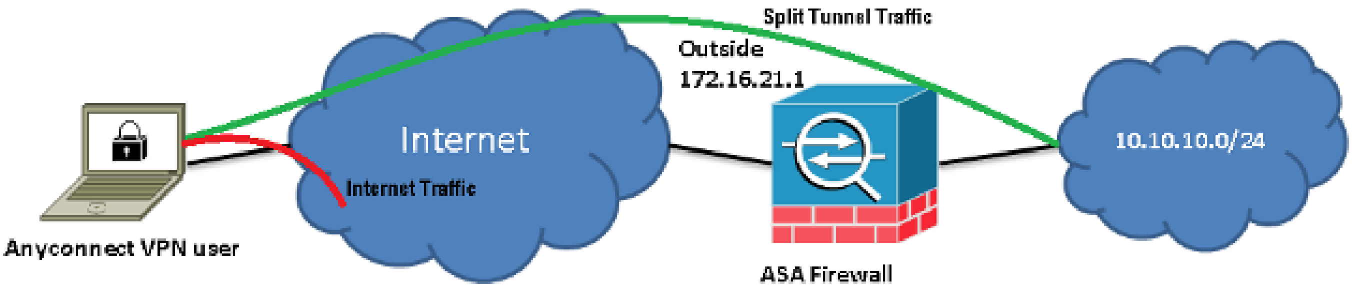
- 請參閱AnyConnect安全移動客戶端功能、許可證和作業系統3.1版文檔，以確定AnyConnect安全移動客戶端所需的許可證和相關功能。
- 有關AnyConnect Apex和Plus許可證的資訊，請參閱Cisco AnyConnect訂購指南。
- 請參閱IP電話和移動VPN連線需要哪種ASA許可證？有關IP電話和移動連線的附加許可證要求的資訊，請參閱。

設定

本節介紹如何在ASA上配置Cisco AnyConnect安全移動客戶端。

網路圖表

以下是本文範例中使用的拓撲：

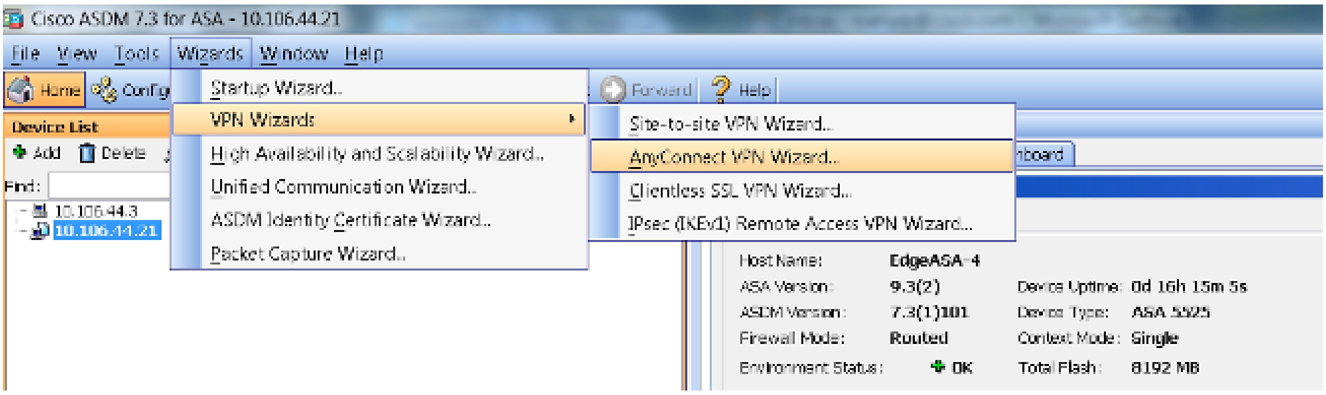


ASDM AnyConnect配置嚮導

AnyConnect配置嚮導可用於配置AnyConnect安全移動客戶端。繼續進行之前，請確保AnyConnect客戶端軟體包已上載到ASA防火牆的快閃記憶體/磁碟。

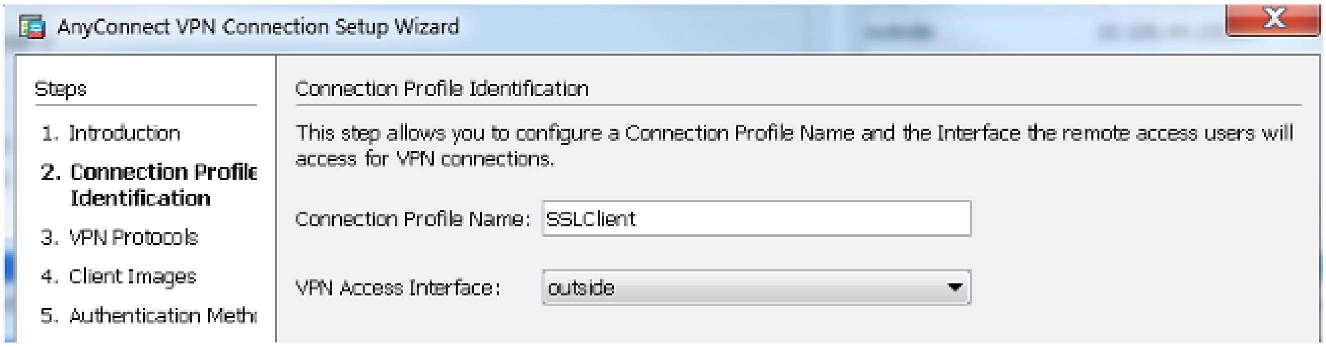
完成以下步驟，以便通過配置嚮導配置AnyConnect安全移動客戶端：

1. 登入到ASDM，啟動**配置嚮導**，然後按一下**下一步**:


Cisco ASDM 7.3 for ASA - 10.106.44.21
File View Tools Wizards Window Help
Home Config
Forward Help
Device List
Add Delete
Find:
10.106.44.3
10.106.44.21
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
ASDM Identity Certificate Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
AnyConnect VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
board

Host Name: EdgeASA-4
ASA Version: 9.3(2)
ASDM Version: 7.3(1)101
Firewall Mode: Routed
Environment Status: OK
Device Uptime: 0d 16h 15m 5s
Device Type: ASA 5525
Context Mode: Single
Total Flash: 8192 MB

2. 輸入*Connection Profile Name*，從*VPN Access Interface*下拉選單中選擇將終止VPN的介面，然後按一下**Next**:


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Meth

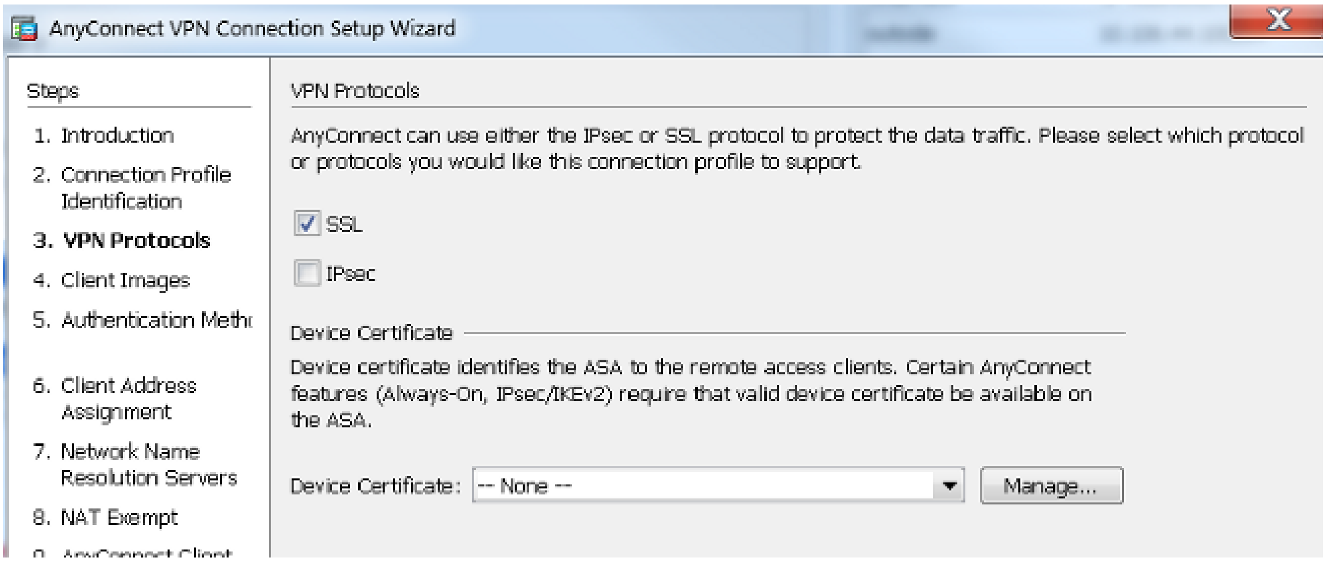
Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

Connection Profile Name: SSLClient

VPN Access Interface: outside

3. 勾選「**SSL**」覈取方塊以啟用安全套接字層(SSL)。 *Device Certificate*可以是受信任的第三方證書頒發機構(CA)頒發的證書（例如Verisign或Entrust）或自簽名證書。如果證書已安裝在ASA上，則可以通過下拉選單選擇證書。 **附註**：此證書是要提供的伺服器端證書。如果ASA上當前沒有安裝任何證書，並且必須生成自簽名證書，則按一下**Manage**。要安裝第三方證書，請完成ASA 8.x手動安裝第三方供應商證書以與WebVPN配置示例Cisco文檔配合使用中所述的步驟。



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. **VPN Protocols**
4. Client Images
5. Authentication Meth
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt

VPN Protocols

AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

☑ SSL

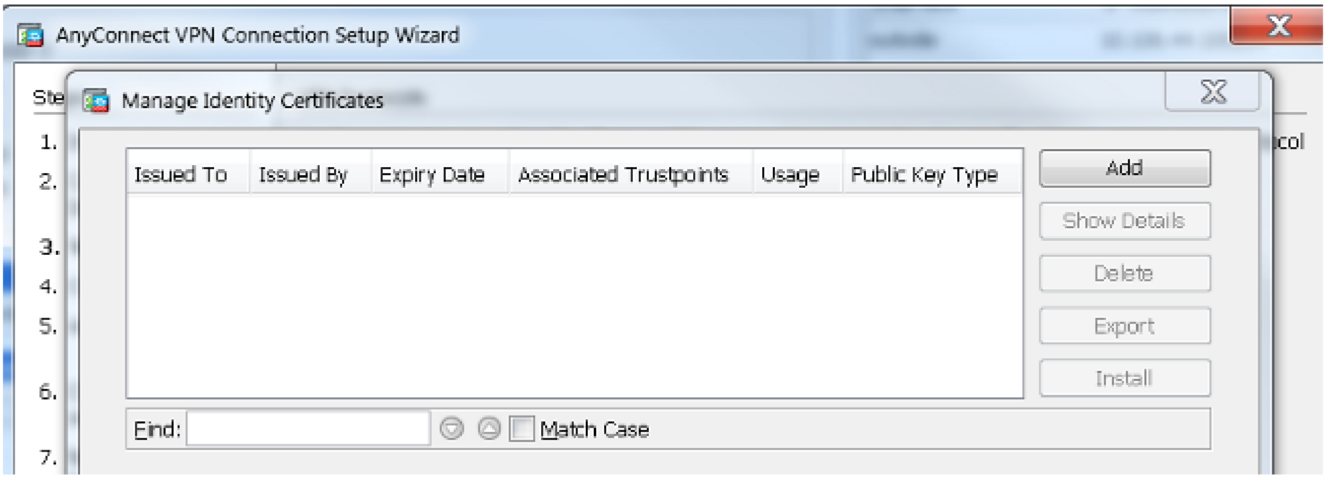
□ IPsec

Device Certificate

Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

Device Certificate: -- None --

4. 按一下「**Add**」：

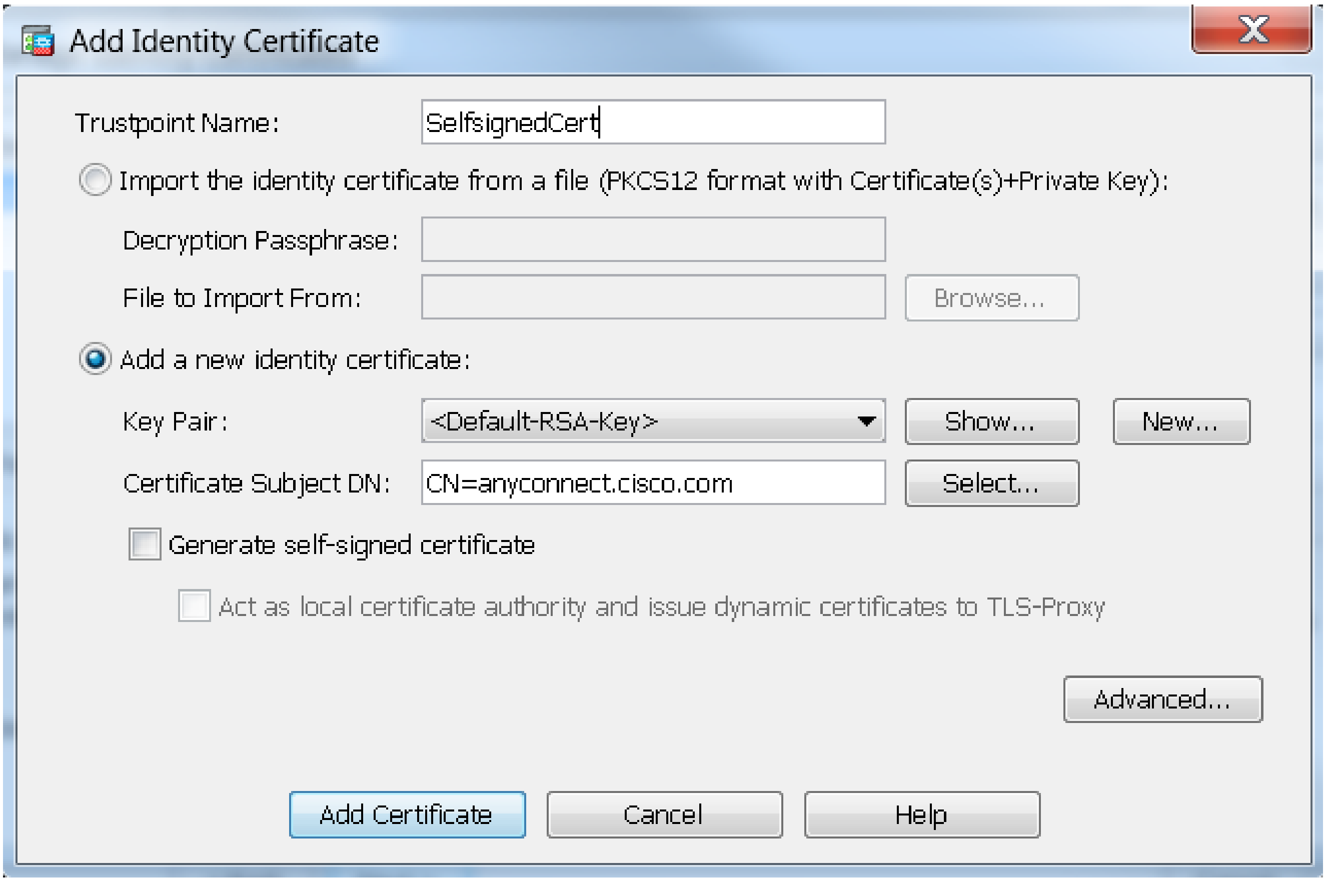


AnyConnect VPN Connection Setup Wizard

Manage Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

5. 在*Trustpoint Name*欄位中鍵入適當的名稱，然後按一下**Add a new identity certificate**單選按鈕。如果裝置上沒有Rivest-Shamir-Addleman(RSA)金鑰對，請按一下**New**以生成一個：



Add Identity Certificate

Trustpoint Name: SelfsignedCert

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

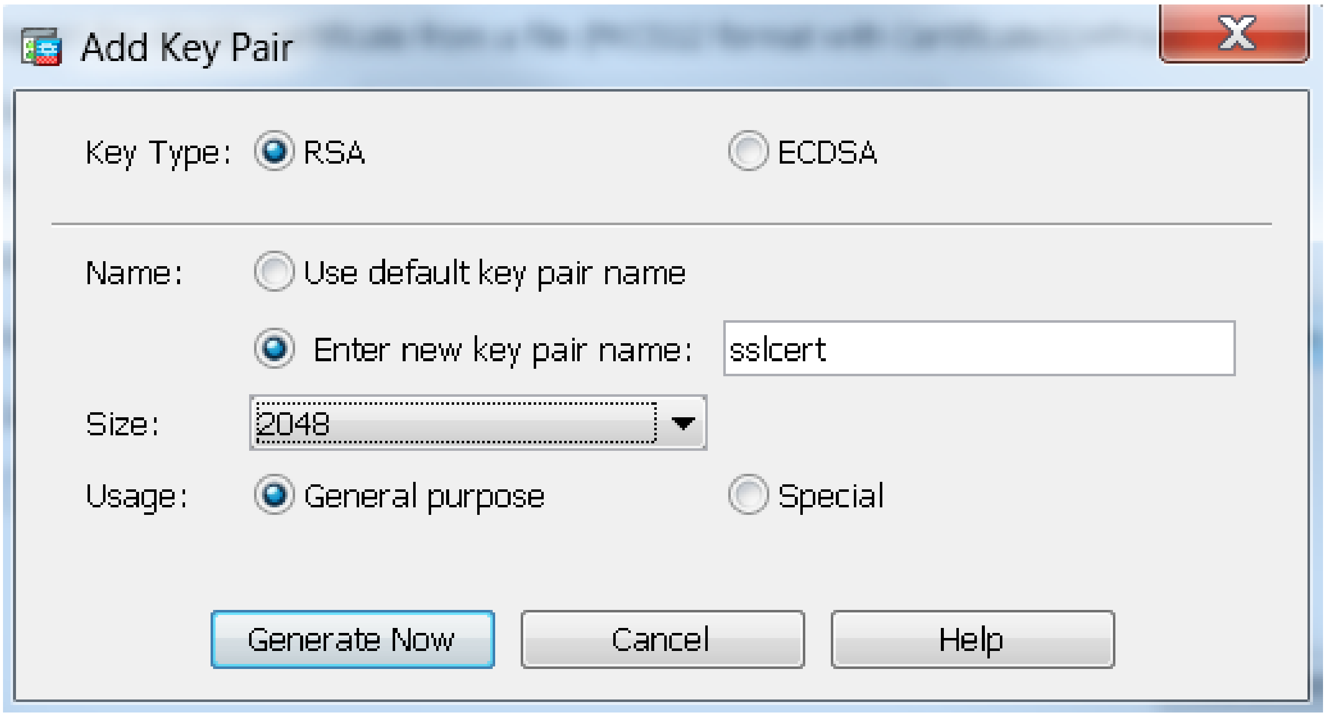
Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=anyconnect.cisco.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

6. 按一下**Use default key pair name** 單選按鈕，或按一下**Enter new key pair name**單選按鈕並輸入新名稱。選擇金鑰的大小，然後按一下**Generate** Now:



Add Key Pair

Key Type: ● RSA ○ ECDSA

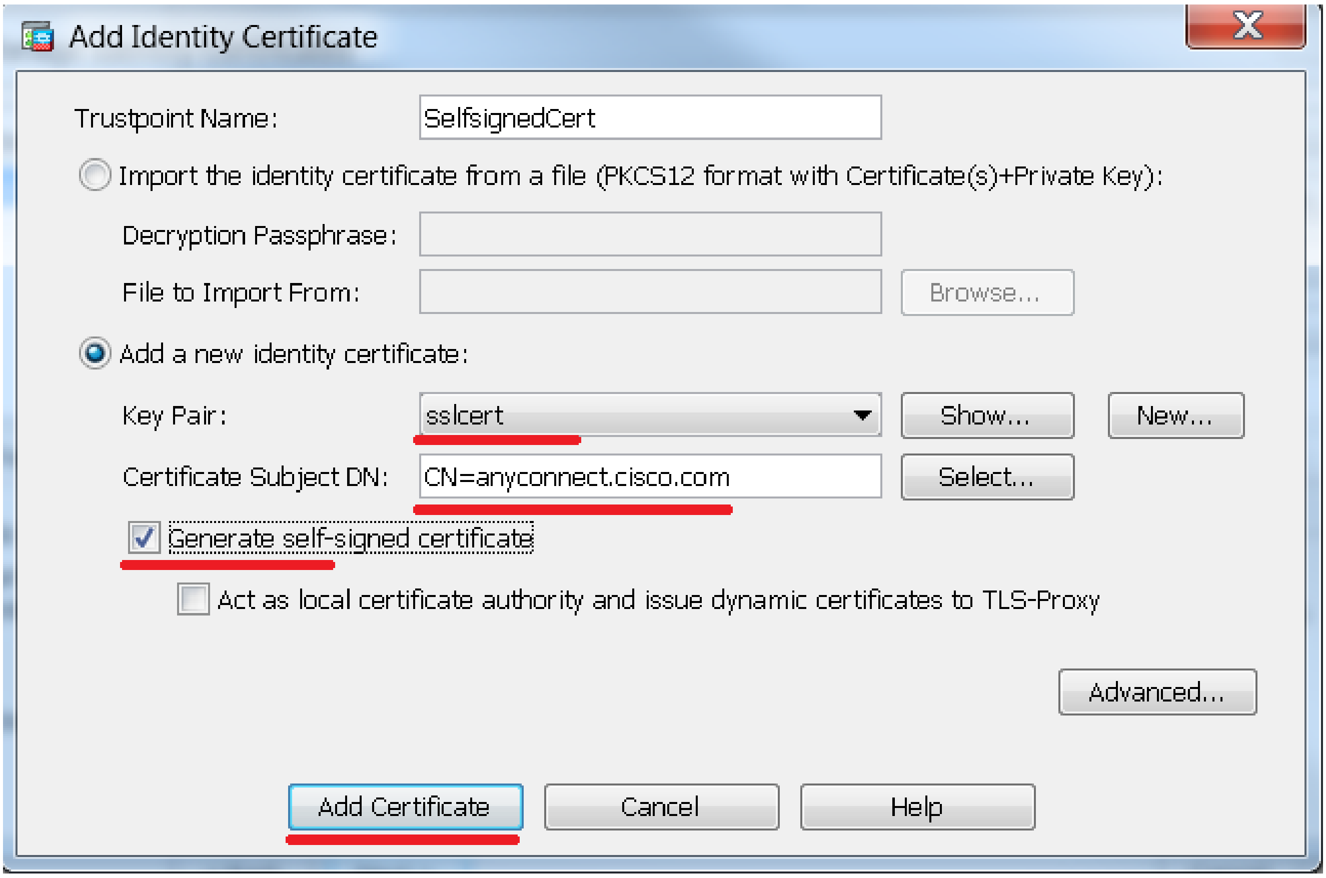
Name: ○ Use default key pair name

● Enter new key pair name: sslcert

Size: 2048

Usage: ● General purpose ○ Special

7. 生成RSA金鑰對後，選擇金鑰並選中**Generate self-signed certificate**覈取方塊。在*Certificate Subject DN*欄位中輸入所需的使用者域名(DN)，然後按一下**Add Certificate**:



Add Identity Certificate

Trustpoint Name: SelfsignedCert

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

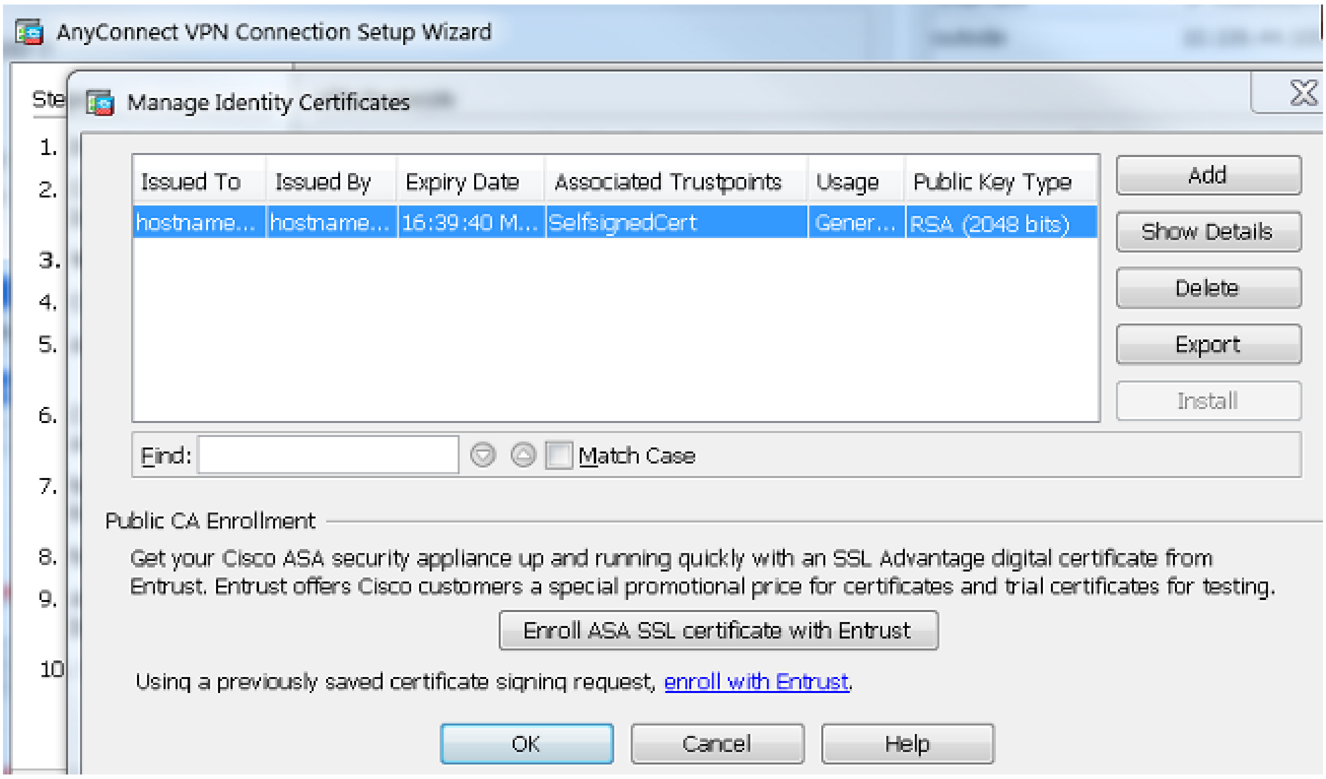
Key Pair: sslcert

Certificate Subject DN: CN=anyconnect.cisco.com

☑ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

8. 註冊完成後，依次按一下**OK**、**OK**和**Next**:



AnyConnect VPN Connection Setup Wizard

Manage Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname...	hostname...	16:39:40 M...	SelfsignedCert	Gener...	RSA (2048 bits)

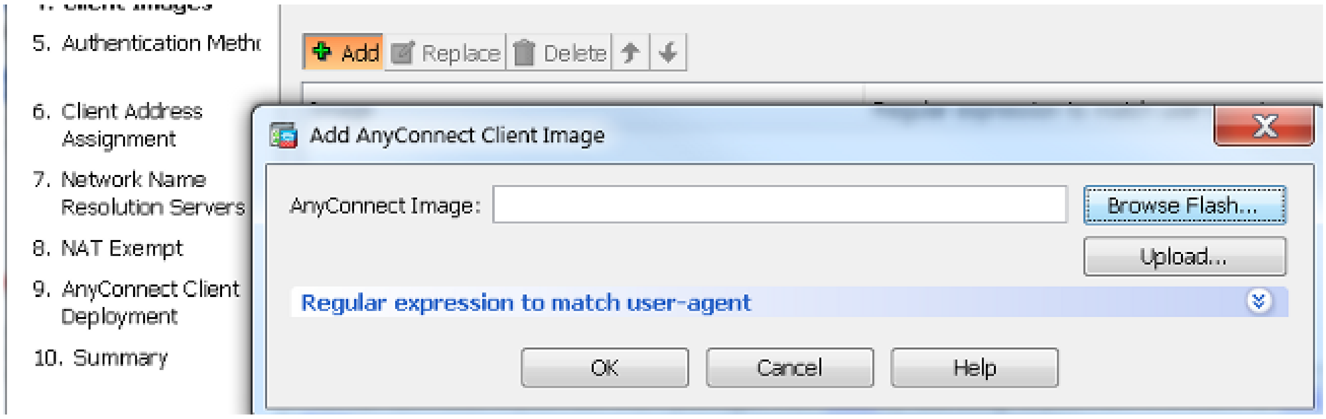
Find: □ Match Case

Public CA Enrollment

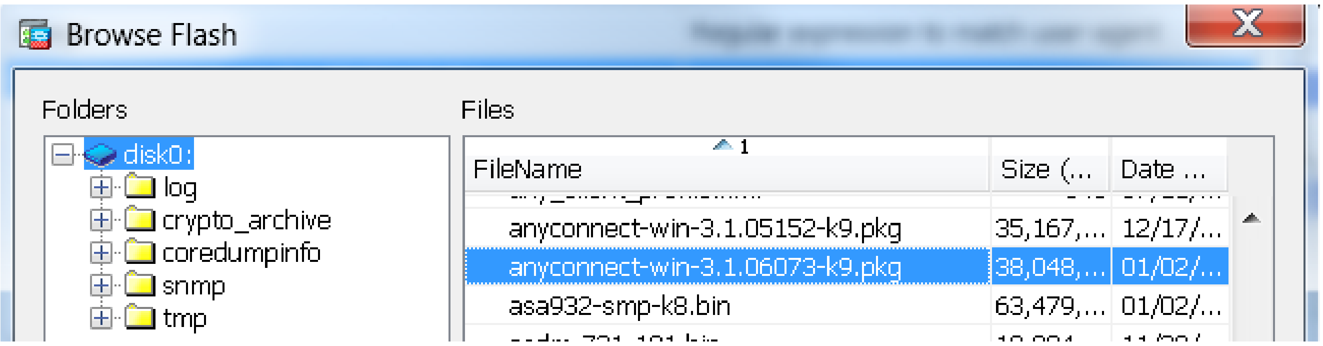
Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

Using a previously saved certificate signing request, enroll with Entrust.

9. 按一下「**Add**」以從PC或快閃記憶體中新增AnyConnect客戶端映像(.*pkg*檔案)。按一下「**Browse Flash**」以從快閃磁碟機新增映像，或按一下「**Upload**」以直接從主機新增映像：


5. Authentication Meth
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
Add
Replace
Delete
Add AnyConnect Client Image
Browse Flash...
Upload...
Regular expression to match user-agent
OK
Cancel
Help

AnyConnect Image:



FileName	Size (...	Date ...
anyconnect-win-3.1.05152-k9.pkg	35,167,...	12/17/...
anyconnect-win-3.1.06073-k9.pkg	38,048,...	01/02/...
asa932-smp-k8.bin	63,479,...	01/02/...

10. 新增映像後，按一下**Next**:

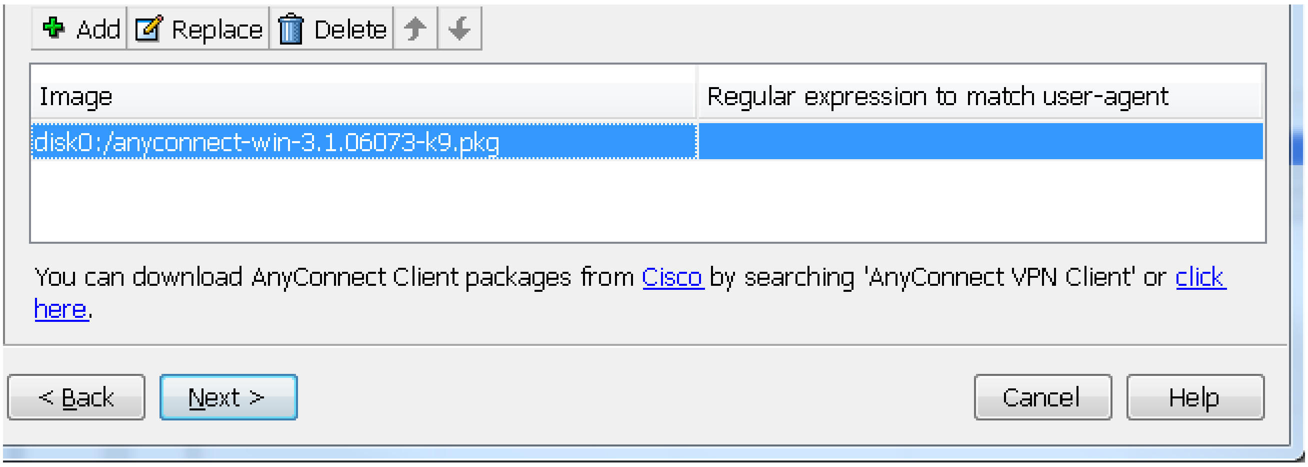
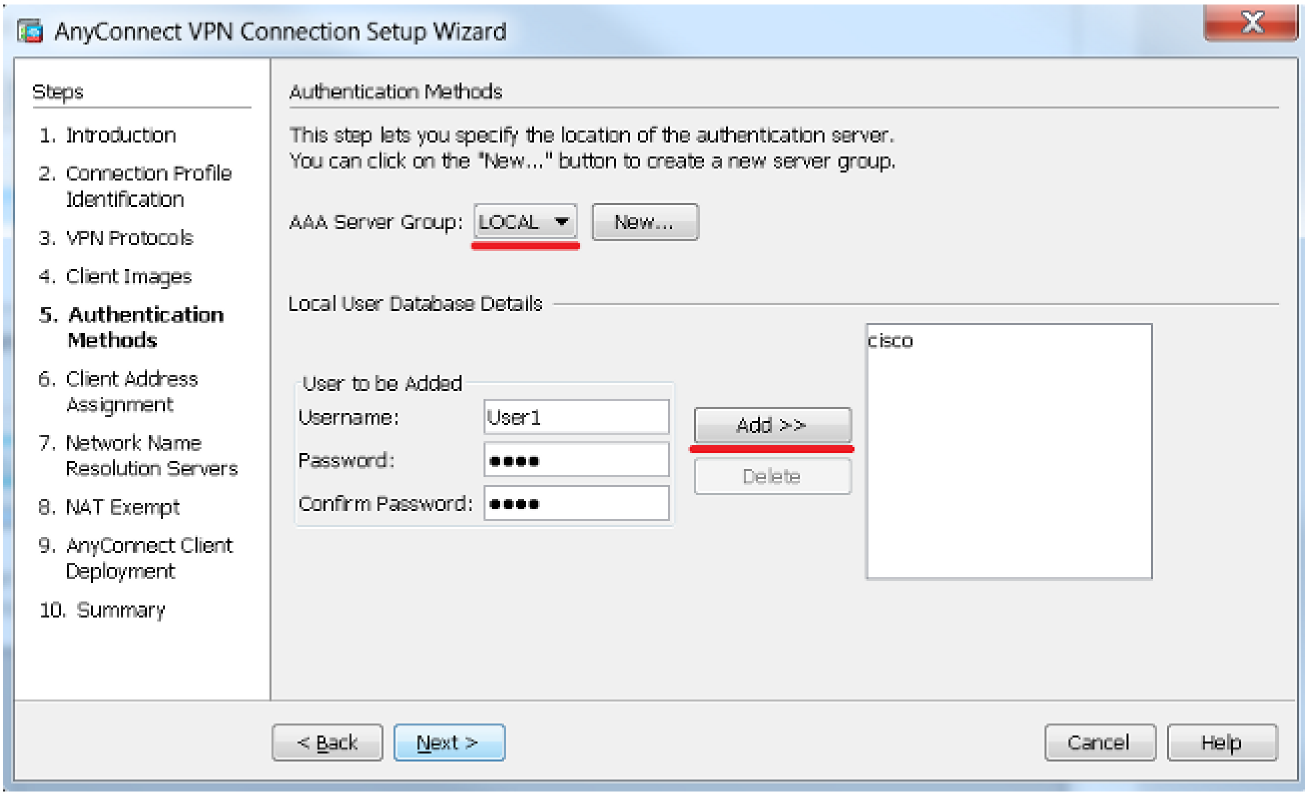


Image	Regular expression to match user-agent
disk0:/anyconnect-win-3.1.06073-k9.pkg	

You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.

11. 使用者身份驗證可通過身份驗證、授權和記帳(AAA)伺服器組完成。如果使用者已設定，則選擇**LOCA**，然後按一下**Next**。 **附註**：在本示例中，配置了**LOCAL**身份驗證，這意味著將使用ASA上的本地使用者資料庫進行身份驗證。


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
New...
Add >>
Delete
< Back
Next >
Cancel
Help

Authentication Methods

This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.

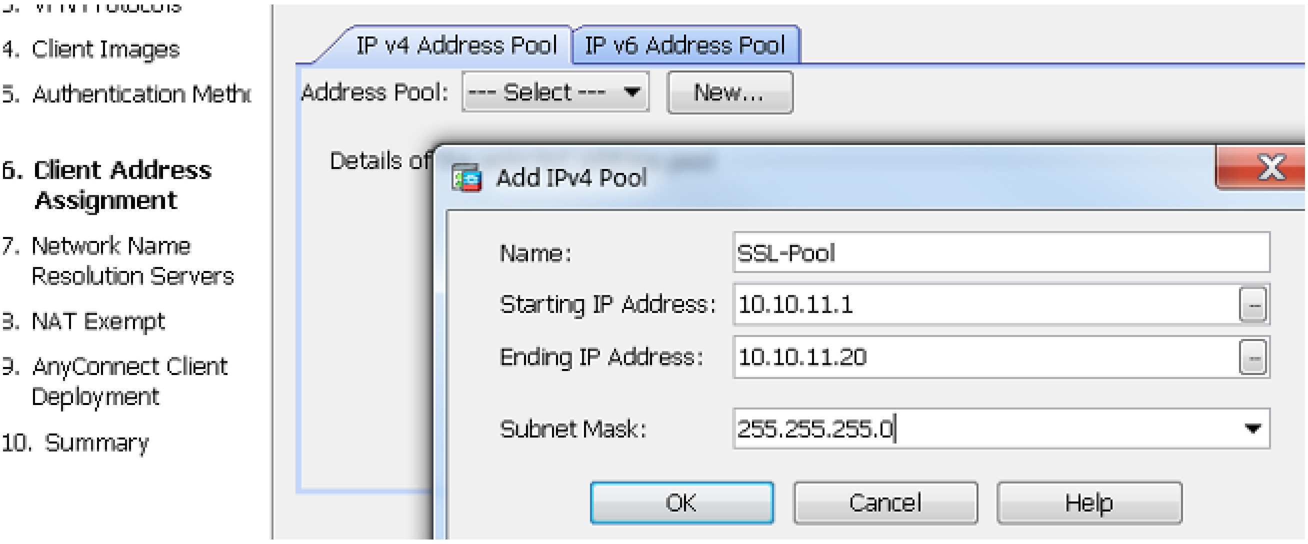
AAA Server Group: LOCAL

Local User Database Details

cisco

User to be Added
Username: User1
Password: ●●●●
Confirm Password: ●●●●

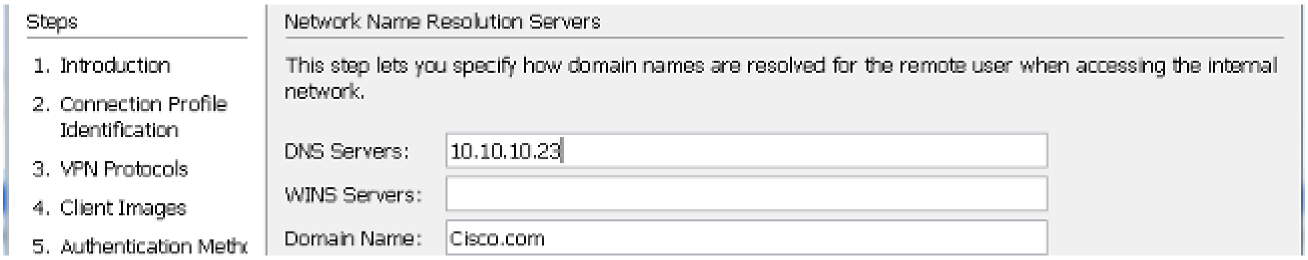
12. 必須配置VPN客戶端的地址池。如果已經配置了一個，則從下拉選單中選擇它。如果不是，請按一下**New**以配置一個新設定。完成後，按一下**Next**:



Address Pool: --- Select ---

Name: SSL-Pool
Starting IP Address: 10.10.11.1
Ending IP Address: 10.10.11.20
Subnet Mask: 255.255.255.0

13. 將域名系統(DNS)伺服器和DN適當地輸入到*DNS*和*域名*欄位，然後按一下**下一步**:



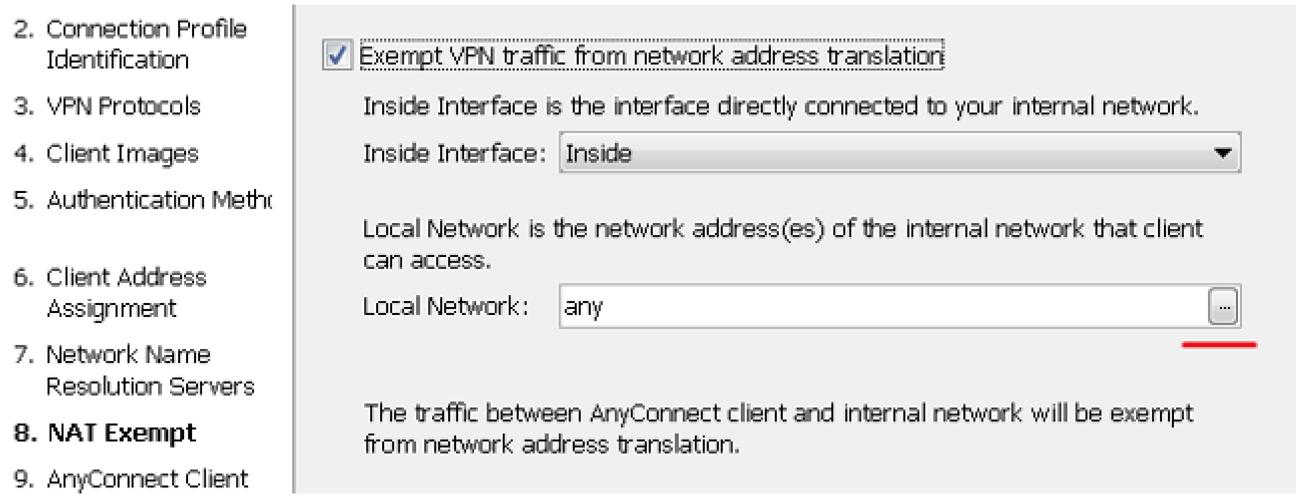
Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 10.10.10.23
WINS Servers:
Domain Name: Cisco.com

14. 在此案例中，目標是限制通過VPN訪問配置為ASA後*Inside*（或LAN）子網的**10.10.10.0/24**網路。客戶端與內部子網之間的流量必須免除任何動態網路地址轉換(NAT)。

選中Exempt VPN traffic from network address translation覈取方塊，並配置用於免除的LAN和WAN介面：



2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Meth
6. Client Address Assignment
7. Network Name Resolution Servers
8. **NAT Exempt**
9. AnyConnect Client

☑ Exempt VPN traffic from network address translation

Inside Interface is the interface directly connected to your internal network.

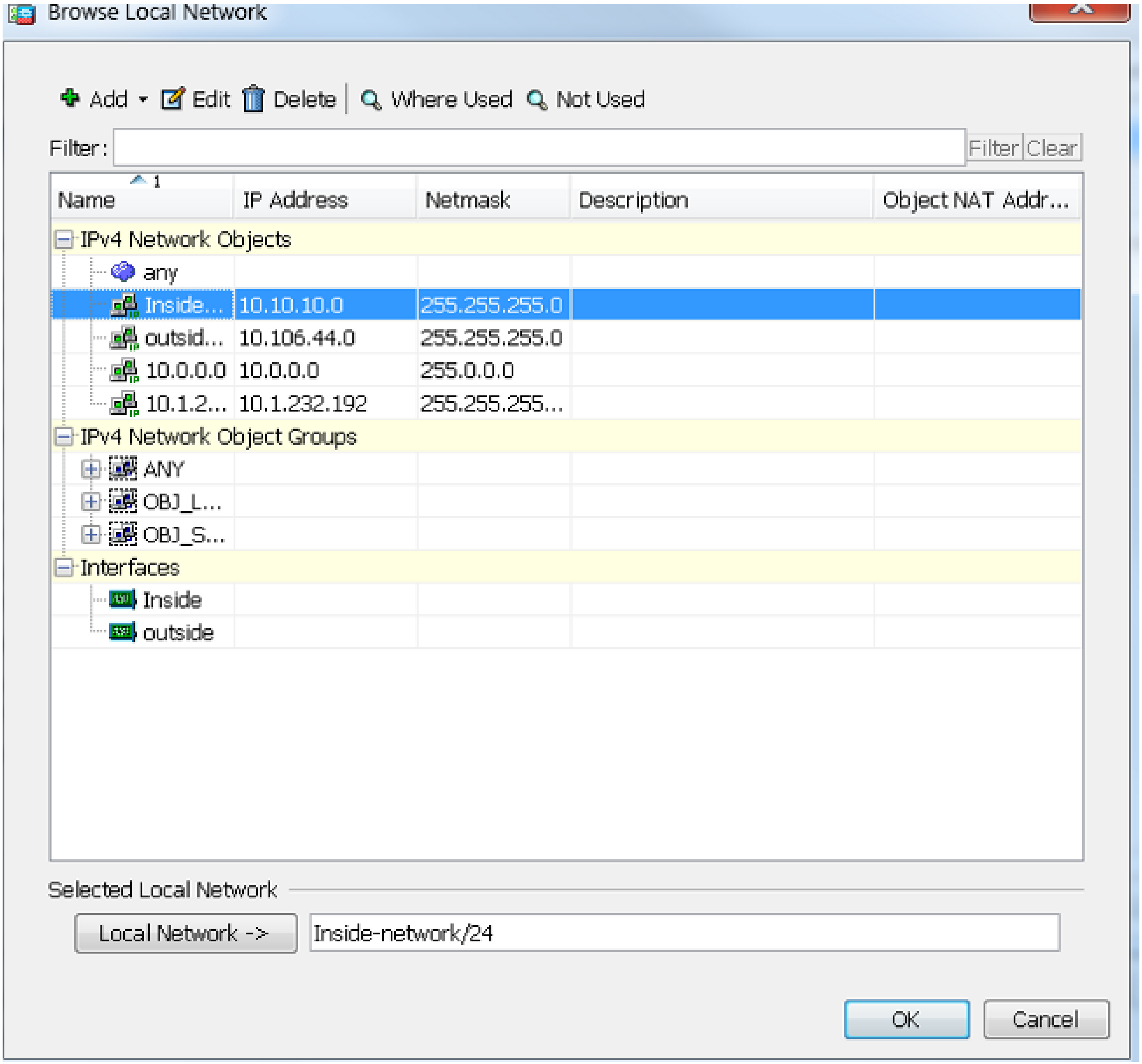
Inside Interface: Inside

Local Network is the network address(es) of the internal network that client can access.

Local Network: any

The traffic between AnyConnect client and internal network will be exempt from network address translation.

15. 選擇必須免除的本地網路：

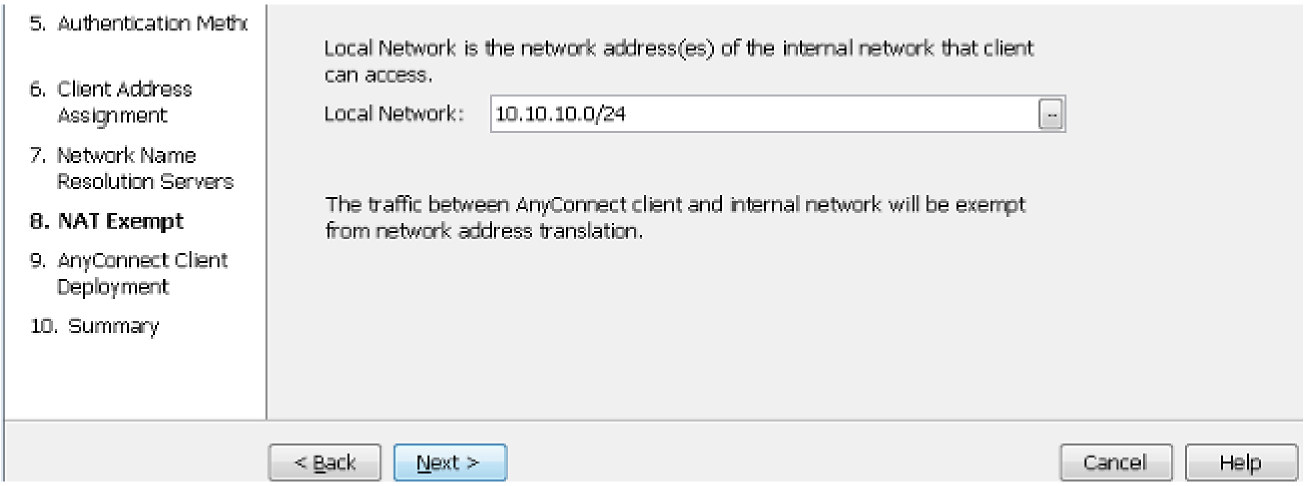


Browse Local Network

Name	IP Address	Netmask	Description	Object NAT Addr...
IPv4 Network Objects				
any				
Inside...	10.10.10.0	255.255.255.0		
outsid...	10.106.44.0	255.255.255.0		
10.0.0.0	10.0.0.0	255.0.0.0		
10.1.2...	10.1.232.192	255.255.255...		
IPv4 Network Object Groups				
ANY				
OBJ_L...				
OBJ_S...				
Interfaces				
Inside				
outside				

Selected Local Network

Local Network -> Inside-network/24


5. Authentication Meth
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

Local Network is the network address(es) of the internal network that client can access.

Local Network: 10.10.10.0/24

The traffic between AnyConnect client and internal network will be exempt from network address translation.

16. 按一下「**Next**」、「**Next**」，然後「**Finish**」。

AnyConnect客戶端配置現在已完成。但是，當您通過配置嚮導配置AnyConnect時，它預設將*拆分隧道*策略配置為**Tunnelall**。為了僅對特定流量進行通道傳輸，*必須實*施分割通道。

> **附註**：如果未配置拆分隧道，則拆分隧道策略將從預設組策略(DfltGrpPolicy)繼承，預設設定為**Tunnelall。**這意味著一旦客戶端通過VPN連線，所有流量（包括到Web的流量）將通過隧道傳送。

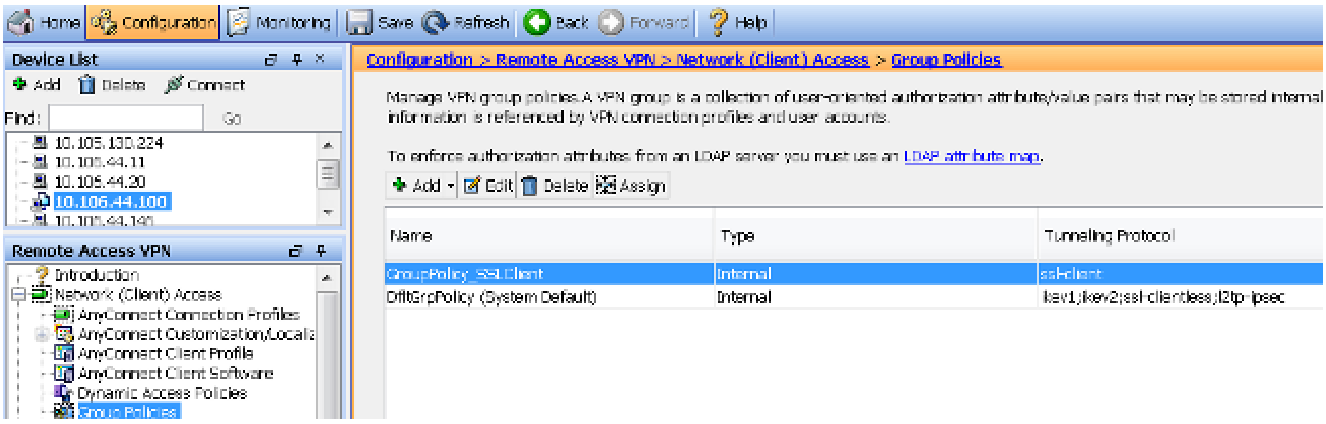
只有目的地為ASA WAN(或*Outside*)IP地址的流量才會繞過客戶端電腦上的隧道。可從Microsoft Windows電腦上**route print**命令的輸出中看到這種情況。

分割隧道配置

分割隧道是一種功能，可用於定義必須加密的子網或主機的流量。其中涉及將與此功能相關聯的存取控制清單(ACL)的組態。此ACL上定義的子網或主機的流量將通過隧道從客戶端進行加密，這些子網的路由將安裝在PC路由表中。

完成以下步驟，以便從*Tunnel-all*組態移至*Split-tunnel*組態：

1. 導航到**Configuration > Remote Access VPN > Group Policies**:



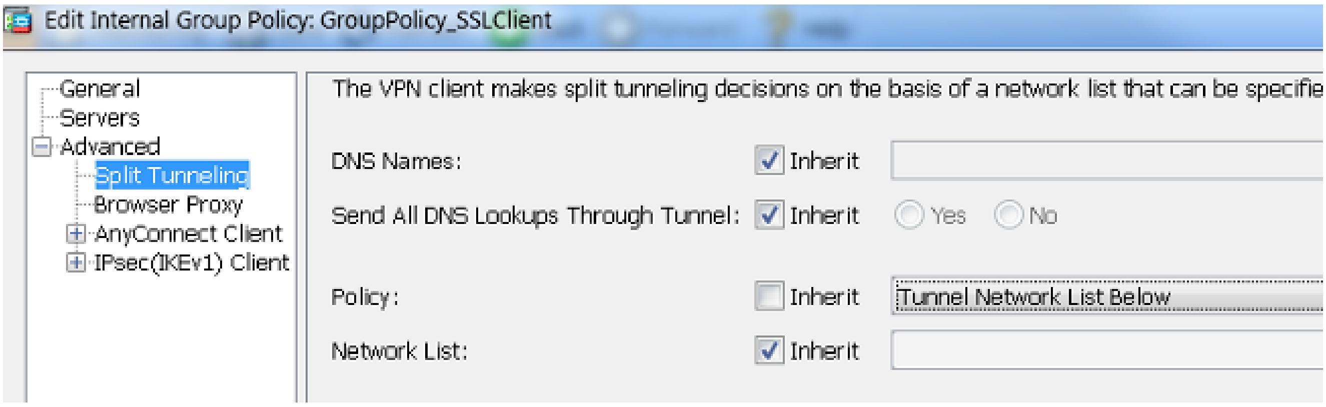
Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internal 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
GroupPolicy_SSLClient	Internal	ssl-client
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec

2. 按一下**Edit**，使用導航樹導航到**Advanced > Split Tunneling**。取消選中*Policy*部分中的**Inherit**覈取方塊，然後從下拉選單中選擇*Tunnel Network List Below*.



The VPN client makes split tunneling decisions on the basis of a network list that can be specifie

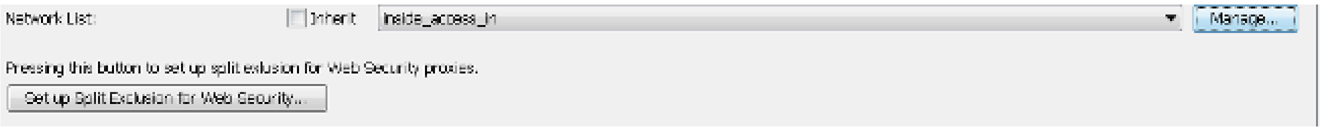
DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: ☑ Inherit ○ Yes ○ No

Policy: □ Inherit Tunnel Network List Below

Network List: ☑ Inherit

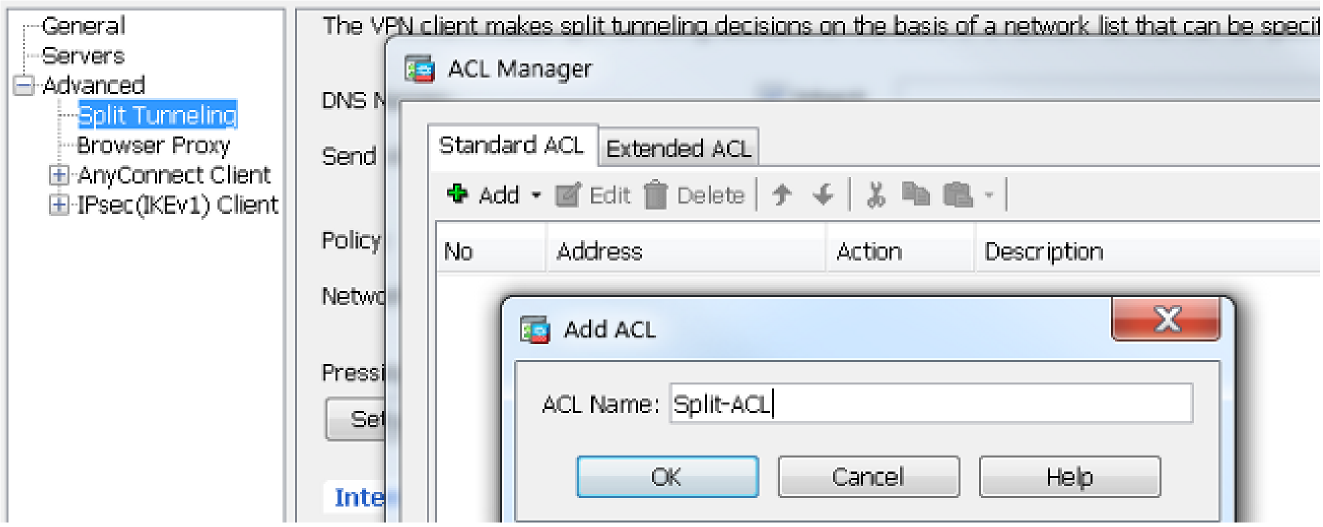
3. 取消選中*Network List*部分中的**Inherit**覈取方塊，然後按一下**Manage**以選擇指定客戶端需要訪問的LAN網路的ACL:



Network List: □ Inherit inside_access_in

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

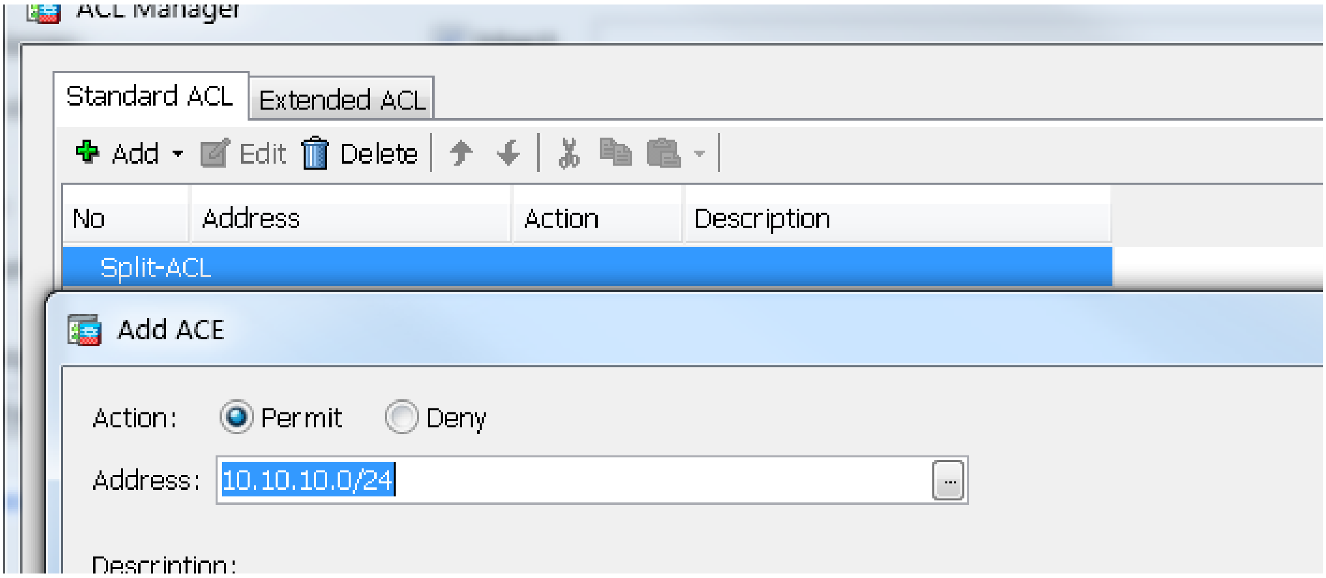
4. 按一下「Standard **ACL**」、「**Add**」、「**Add ACL**」，然後「ACL**name**:



The VPN client makes split tunneling decisions on the basis of a network list that can be specit

ACL Name: Split-ACL

5. 按一下**Add ACE**以新增規則：



ACL Manager

Standard ACL | Extended ACL

No	Address	Action	Description
Split-ACL			

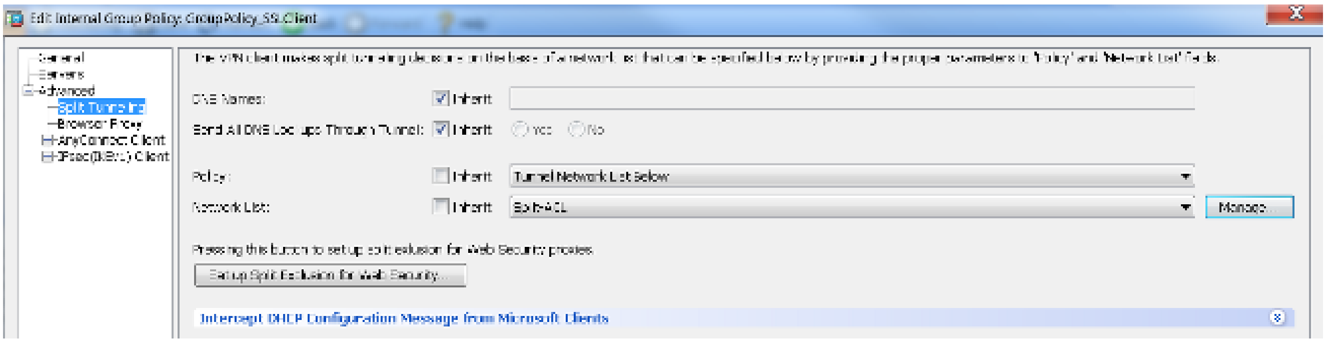
Add ACE

Action: ● Permit ○ Deny

Address: 10.10.10.0/24

Description:

6. 按一下「**OK**」（確定）。



Edit Internal Group Policy: GroupPolicy_SSLClient

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 List' fields.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: ☑ Inherit ○ Yes ○ No

Policy: □ Inherit Tunnel Network List Below

Network List: □ Inherit Split-ACL

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

7. 按一下「**Apply**」。

連線後，拆分ACL上的子網或主機的路由將新增到客戶端電腦的路由表中。在Microsoft Windows電腦上，可以在**route print**命令的輸出中檢視此問題。這些路由的下一跳將是來自客戶端IP池子網的IP地址（通常是子網的第一個IP地址）：

```
C:\Users\admin>route print
IPv4 Route Table
======================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261
10.10.10.0       255.255.255.0    10.10.11.2   10.10.11.1     2

!! This is the split tunnel route.

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261
172.16.21.1     255.255.255.255      On-link     10.106.44.243   6

!! This is the route for the ASA Public IP Address.
```

在MAC OS電腦上，輸入**netstat -r**命令以檢視PC路由表：

```
$ netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Netif Expire
default hsrp-64-103-236-1. UGSc 34 0 en1
```

```
10.10.10/24        10.10.11.2         UGSc    0   44   utun1

!! This is the split tunnel route.

10.10.11.2/32 localhost UGSc 1 0 lo0
172.16.21.1/32     hsrp-64-103-236-1. UGSc    1   0    en1

!! This is the route for the ASA Public IP Address.
```

下載並安裝AnyConnect客戶端

在使用者電腦上部署Cisco AnyConnect安全移動客戶端可以使用兩種方法：

- Web部署

- 獨立部署

這兩種方法將在後面的章節中詳細介紹。

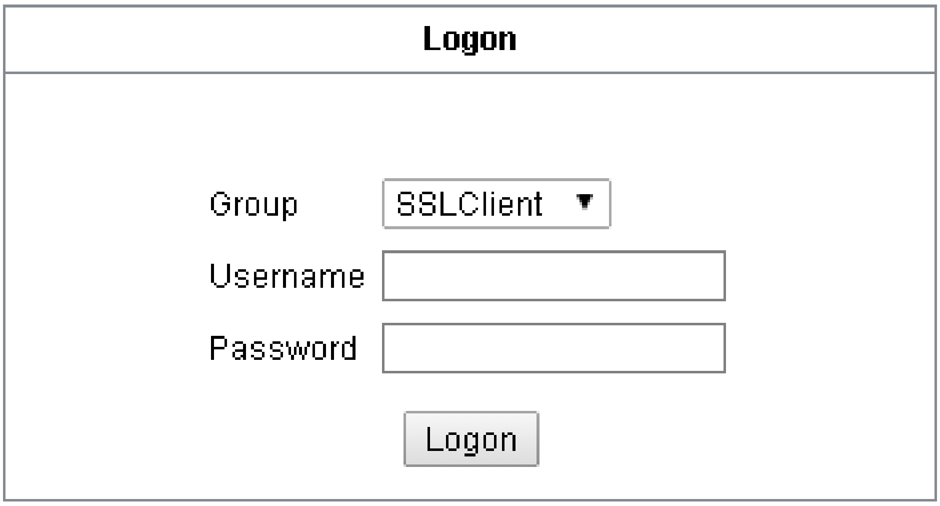
Web部署

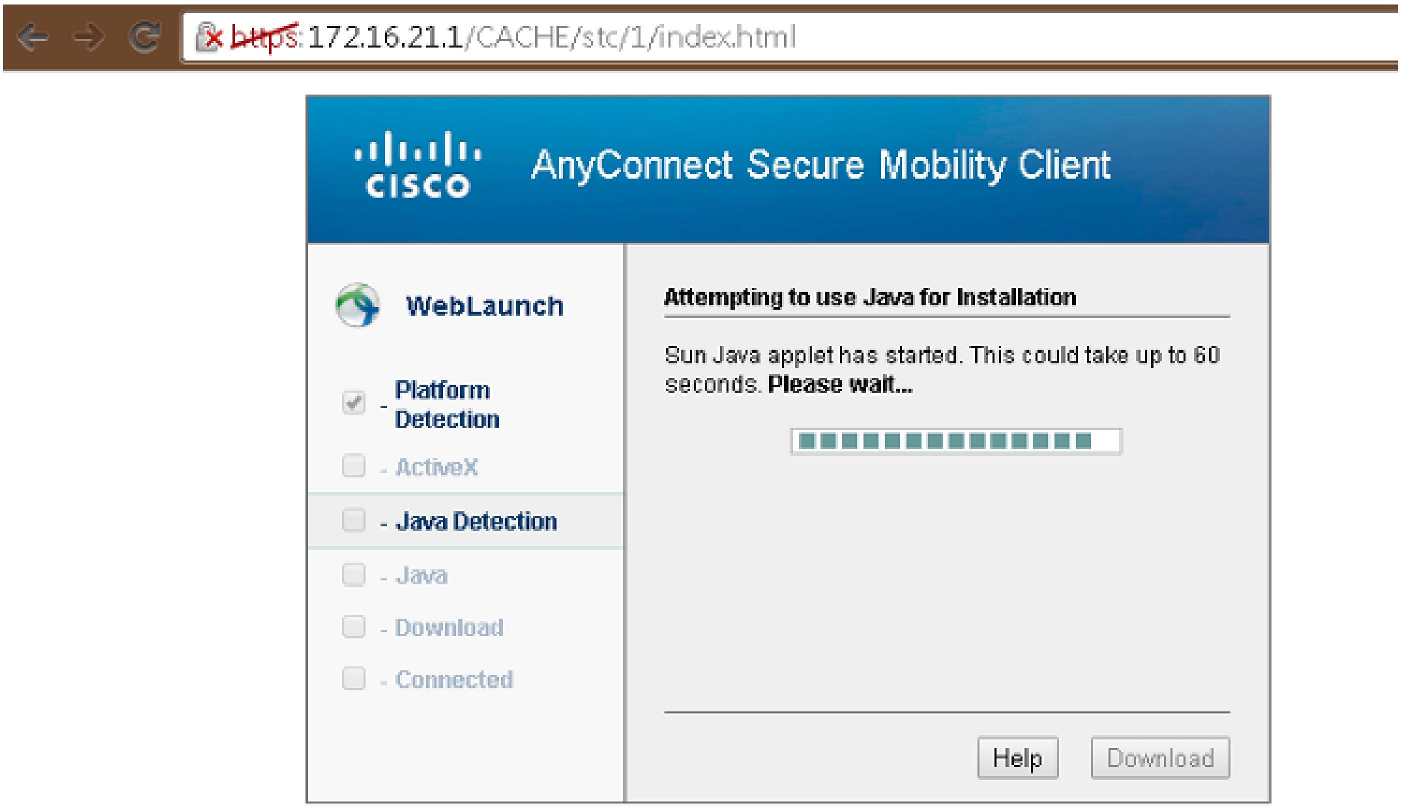
若要使用Web部署方法，請將**https://<ASA的FQDN>或<ASA的IP>**URL輸入客戶端電腦上的瀏覽器，這會將您帶到*WebVPN門戶*頁面。

> **附註**：如果使用Internet Explorer(IE)，則安裝主要通過ActiveX完成，除非強制使用Java。所有其他瀏覽器都使用Java。

登入到頁面後，安裝應在客戶端電腦上開始，並且客戶端應在安裝完成後連線到ASA。

> **附註**：系統可能會提示您輸入運行ActiveX或Java的許可權。若要繼續安裝，必須允許此操作。





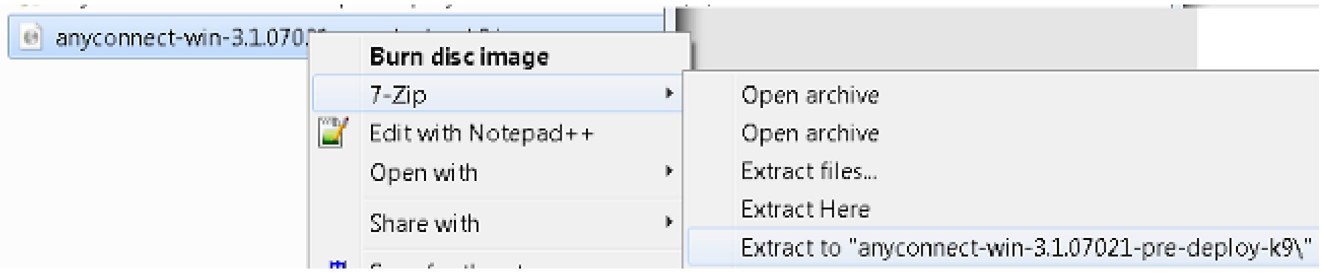
Attempting to use Java for Installation

Sun Java applet has started. This could take up to 60 seconds. **Please wait...**

獨立部署

完成以下步驟即可使用獨立部署方法：

1. 從思科網站下載AnyConnect客戶端映像。若要選擇要下載的正確映像，請參閱Cisco AnyConnect安全行動化使用者端網頁。此頁面上提供了下載連結。導航到下載頁面並選擇適當的版本。搜尋「**Full installation package - Window / Standalone installer(ISO)**」。 **附註**：然後下載ISO安裝程式映像(如*anyconnect-win-3.1.06073-pre-deploy-k9.iso*)。
2. 使用*WinRar*或*7-Zip*擷取ISO封裝的內容：



3. 提取內容後，運行**Setup.exe**檔案並選擇必須與Cisco AnyConnect安全移動客戶端一起安裝的模組。

提示：要配置VPN的其他設定，請參閱*使用CLI 8.4和8.6的Cisco ASA 5500系列配置指南的*配置AnyConnect VPN客戶端連線部分。

CLI組態

本節提供Cisco AnyConnect安全移動客戶端的CLI配置以供參考。

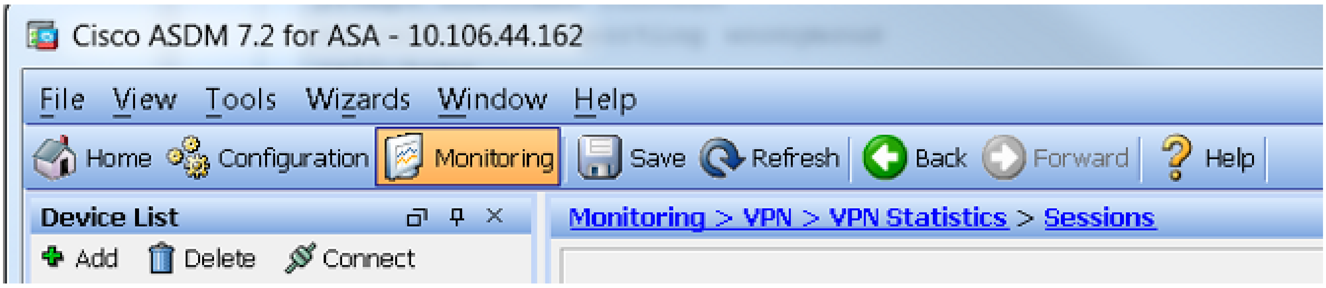
```
ASA Version 9.3(2)
!
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224

access-list all extended permit ip any any

!***********Split ACL configuration***********

access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
no pager
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-721.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

!************** NAT exemption Configuration *****************
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.

nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp
route-lookup
access-group all in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact

!********** Trustpoint for Selfsigned certificate***********
!Genarate the key pair and then configure the trustpoint
!Enroll the trustpoint genarate the self-signed certificate

crypto ca trustpoint SelfsignedCert
enrollment self
subject-name CN=anyconnect.cisco.com
keypair sslcert
crl configure
crypto ca trustpool policy
crypto ca certificate chain SelfsignedCert
certificate 4748e654
308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105
0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e
636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e
170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a
311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31
19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d
06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0
55a975ec a1f2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4
ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0
7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7
53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34
03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8
quit
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1-only
ssl encryption des-sha1 3des-sha1 aes128-sha1 aes256-sha1

!******** Bind the certificate to the outside interface********
ssl trust-point SelfsignedCert outside

!********Configure the Anyconnect Image and enable Anyconnect***
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!*******Group Policy configuration*********
!Tunnel protocol, Spit tunnel policy, Split
```

```
!ACL, etc. can be configured.

group-policy GroupPolicy_SSLClient internal
group-policy GroupPolicy_SSLClient attributes
wins-server none
dns-server value 10.10.10.23
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
default-domain value Cisco.com

username User1 password PfeNk7qp9b4LbLV5 encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

!*******Tunnel-Group (Connection Profile) Configuraiton*****
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

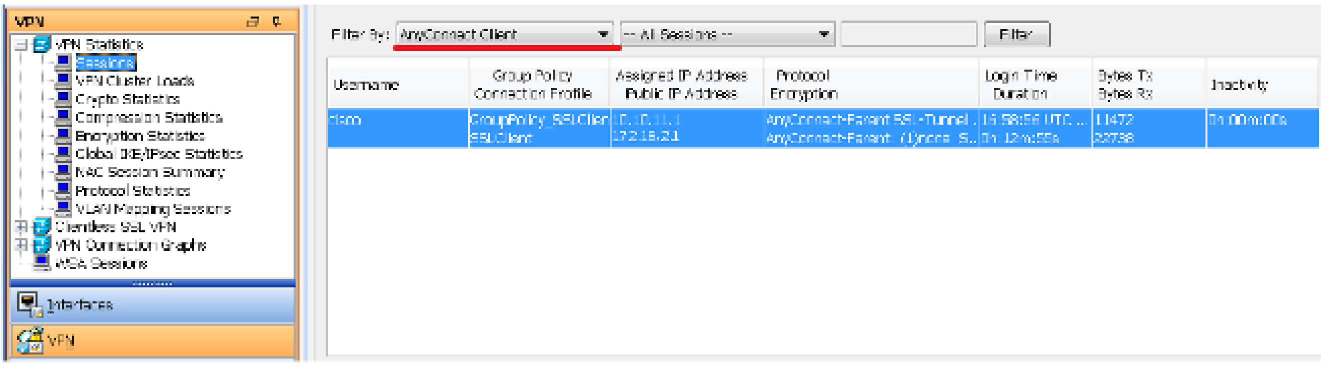
驗證

完成以下步驟，驗證使用者端連線以及與該連線相關的各種引數：

1. 在ASDM上導航到**Monitoring > VPN**:



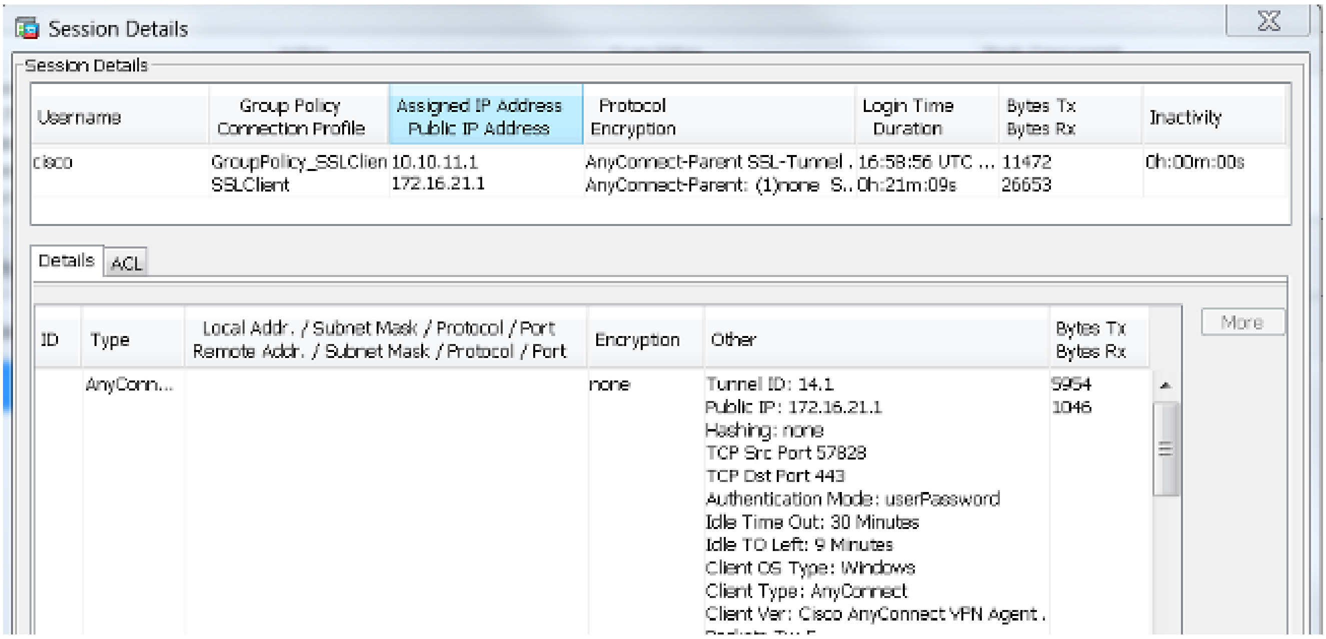
2. 您可以使用**Filter By**選項過濾VPN的型別。從下拉選單中選擇**AnyConnect Client**和所有AnyConnect Client會話。 **提示：**可以使用其他條件（例如使用者名稱和IP位址）進*一步篩選作業階段*。



Filter By: AnyConnect Client -- All Sessions --

Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Inactivity
cisco	GroupPolicy_SSLClien SSLClient	10.10.11.1 172.16.21.1	AnyConnect-Parent SSL-Tunnel ... AnyConnect-Parent: (1)none S...	16:58:56 UTC ... 0h:12m:55s	11472 22738	0h:00m:00s

3. 按兩下一個作業階段，取得該特定作業階段的詳細資訊：



Session Details

Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Inactivity
cisco	GroupPolicy_SSLClien SSLClient	10.10.11.1 172.16.21.1	AnyConnect-Parent SSL-Tunnel ... AnyConnect-Parent: (1)none S...	16:58:56 UTC ... 0h:21m:09s	11472 26653	0h:00m:00s

ID	Type	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Encryption	Other	Bytes Tx Bytes Rx
	AnyConn...		none	Tunnel ID: 14.1 Public IP: 172.16.21.1 Hashing: none TCP Src Port 57828 TCP Dst Port 443 Authentication Mode: userPassword Idle Time Out: 30 Minutes Idle TO Left: 9 Minutes Client OS Type: Windows Client Type: AnyConnect Client Ver: Cisco AnyConnect VPN Agent ...	5954 1046

4. 在CLI中輸入**show vpn-sessiondb anyconnect**命令以獲取會話詳細資訊：

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1    Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient   Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. 您可以使用其他篩選選項來縮小結果範圍：

```
# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed
```

```
Username : cisco Index : 19
Assigned IP : 10.10.11.1    Public IP : 10.106.44.243
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11036 Bytes Rx : 4977
Pkts Tx : 8 Pkts Rx : 60
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSLClient  Tunnel Group : SSLClient
Login Time   : 20:33:34 UTC Mon Apr 6 2015
Duration : 0h:01m:19s

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 19.1
Public IP : 10.106.44.243
Encryption : none Hashing : none
TCP Src Port : 58311 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 772
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 19.2
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : 3DES Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 58315
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 190
Pkts Tx : 4 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 19.3
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : DES Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 58269
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 0 Bytes Rx : 4150
Pkts Tx : 0 Pkts Rx : 59
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

疑難排解

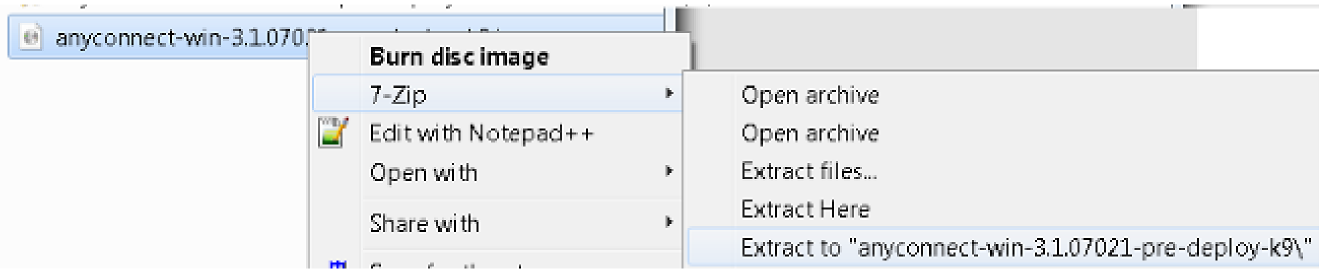
您可以使用AnyConnect診斷和報告工具(DART)來收集有助於排除AnyConnect安裝和連線問題的資

料。DART嚮導用於運行AnyConnect的電腦。DART彙編了思科技術支援中心(TAC)分析的日誌、狀態和診斷資訊，不需要管理員許可權即可在客戶端電腦上運行。

安裝DART

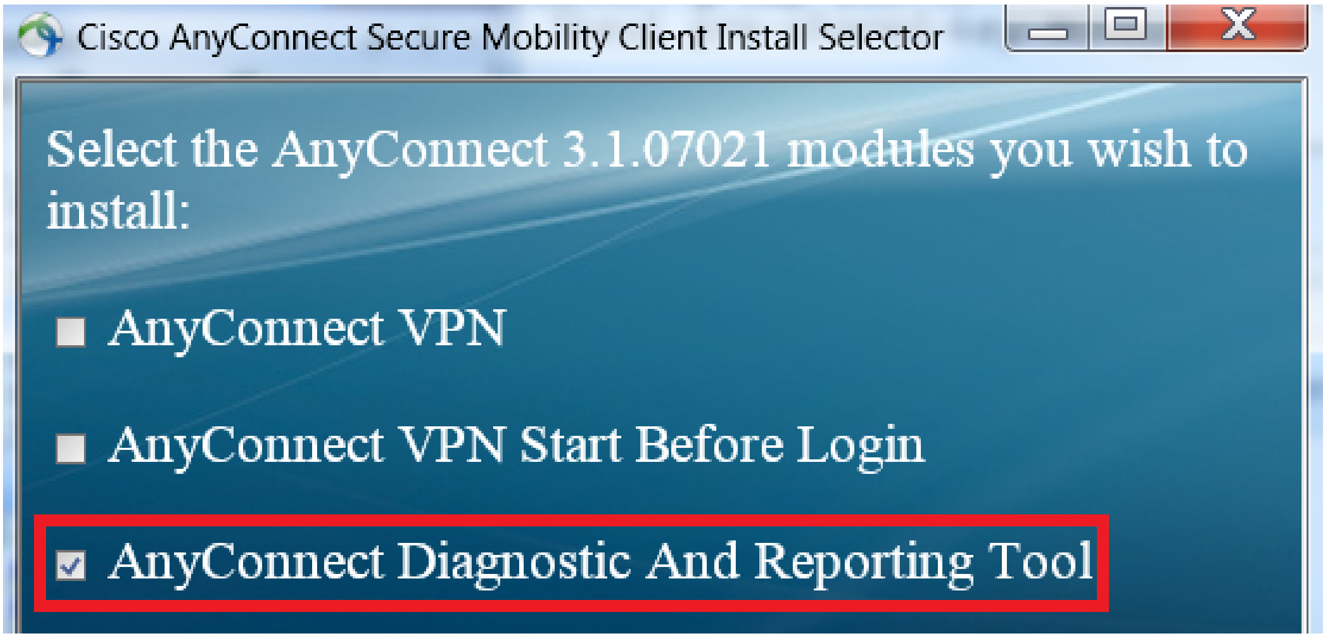
完成以下步驟即可安裝DART:

1. 從思科網站下載AnyConnect客戶端映像。若要選擇要下載的正確映像，請參閱Cisco AnyConnect安全行動化使用者端網頁。此頁面上提供了下載連結。導航到下載頁面並選擇適當的版本。搜尋「**Full installation package - Window / Standalone installer(ISO)**」。 **附註**：然後下載ISO安裝程式映像(如*anyconnect-win-3.1.06073-pre-deploy-k9.iso*)。
2. 使用*WinRar*或*7-Zip*擷取ISO封裝的內容：



3. 瀏覽到內容提取到的資料夾。

4. 運行**Setup.exe**檔案並僅選擇**Anyconnect診斷和報告工具**:


Cisco AnyConnect Secure Mobility Client Install Selector

Select the AnyConnect 3.1.07021 modules you wish to install:

□ AnyConnect VPN

□ AnyConnect VPN Start Before Login

☑ AnyConnect Diagnostic And Reporting Tool

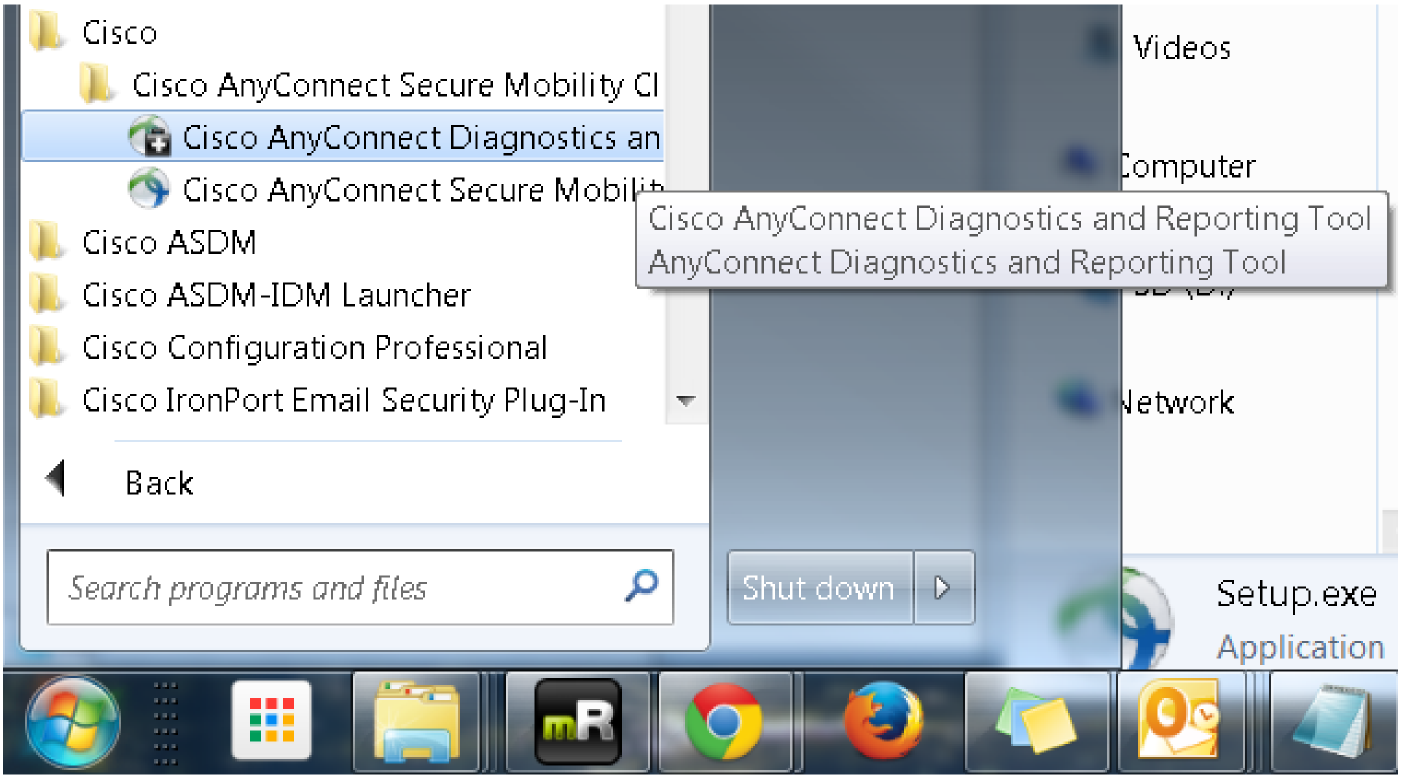
運行DART

運行DART之前需要考慮以下重要資訊：

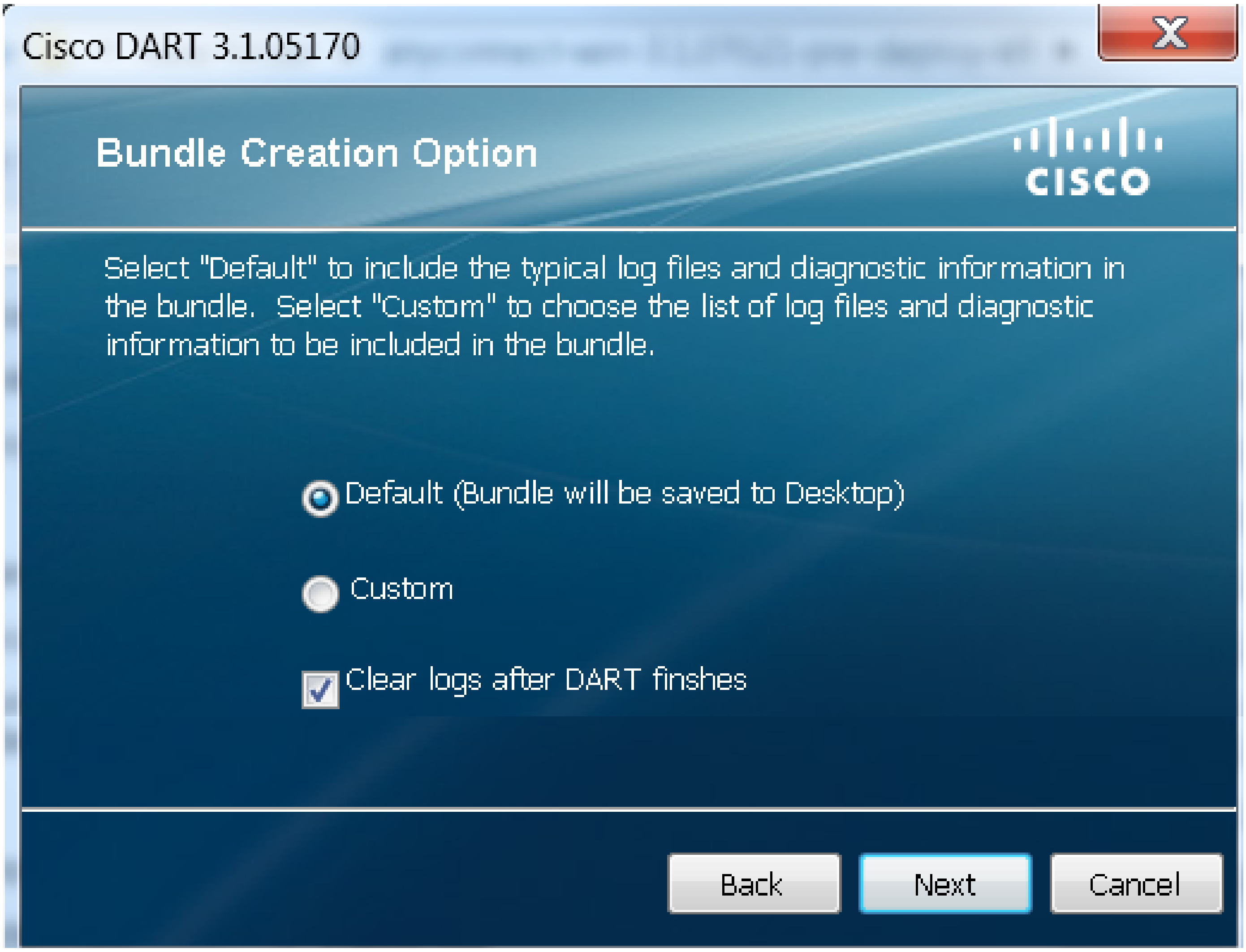
- 在運行DART之前，必須至少重新建立問題一次。

- 重新建立問題時，必須注意使用者電腦上的日期和時間。

在客戶端電腦上從*開始*選單運行DART:


Cisco
Cisco AnyConnect Secure Mobility Cl
Cisco AnyConnect Diagnostics an
Cisco AnyConnect Secure Mobilit
Cisco ASDM
Cisco ASDM-IDM Launcher
Cisco Configuration Professional
Cisco IronPort Email Security Plug-In
Back
Search programs and files
Shut down
Videos
Computer
Network
Cisco AnyConnect Diagnostics and Reporting Tool
AnyConnect Diagnostics and Reporting Tool
Setup.exe
Application

可以選擇*Default*或*Custom*模式。Cisco建議您在「預設」模式下運行DART，這樣所有資訊都可以在一次拍攝中捕獲。


Cisco DART 3.1.05170

Bundle Creation Option

Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

● Default (Bundle will be saved to Desktop)

○ Custom

☑ Clear logs after DART finshes

完成後，工具會將DART捆綁包*.zip*檔案儲存到客戶端案頭。然後，可以將套件組合以電子郵件方式

傳送到TAC（開啟TAC個案後），以進行進一步分析。

相關資訊

- AnyConnect VPN客戶端故障排除指南 — 常見問題
- AnyConnect、CSD/Hostscan和WebVPN的Java 7問題 — 故障排除指南
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。