Configure Secure Client with Split Tunneling on an ASA

Contents

Introduction

This document describes how to configure the Cisco AnyConnect Secure Mobility Client via the ASDM on a Cisco ASA that runs software Version 9.16.1.

Prerequisites

Requirements

The Cisco AnyConnect Secure Mobility Client web deployment package can be downloaded to the local desktop from which the Cisco Adaptive Security Device Manager (ASDM) access to the Cisco Adaptive Security Appliance (ASA) is present. In order to download the client package, refer to the Cisco AnyConnect Secure Mobility Client web page. The web deployment packages for various Operating Systems (OS) can be uploaded to the ASA at the same time.

These are the web deployment file names for the various OSs:

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

- Linux OSs - AnyConnect-linux-<version>-k9.pkg

Components Used

The information in this document is based on these software and hardware versions:

- ASA Version 9.16(1)
- ASDM Version 7.16(1)
- AnyConnect Version 4.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document provides step-by-step details about how to use the Cisco AnyConnect Configuration Wizard via the ASDM in order to configure the AnyConnect Client and enable split-tunneling.

Split-tunneling is used in scenarios where only specific traffic must be tunneled, opposed to scenarios where all of the client machine-generated traffic flows across the VPN when connected.

Use of the AnyConnect Configuration Wizard can default result in a *tunnel-all* configuration on the ASA. Split tunnelling must be configured separately, which is explained in further detail in the Split Tunnel section of this document.

In this configuration example, the intention is to send traffic for the 10.10.10.0/24 subnet, which is the LAN subnet behind the ASA, over the VPN tunnel and all other traffic from the client machine is forwarded via its own Internet circuit.

AnyConnect License Information

Here are some links to useful information about the Cisco AnyConnect Secure Mobility Client licenses:

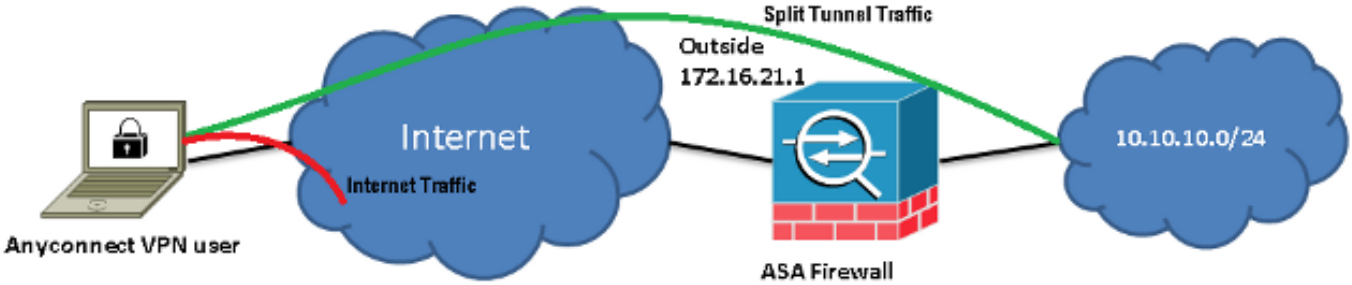
- Refer to the Cisco AnyConnect Licensing Frequently Asked Questions (FAQ) document in order to determine the licenses that are required for AnyConnect Secure Mobility Client and the related features.
- Refer to the Cisco Secure Client Ordering Guide for information about licenses.

Configure

This section describes how to configure the Cisco Secure Client on the ASA.

Network Diagram

This is the topology that is used for the examples in this document:

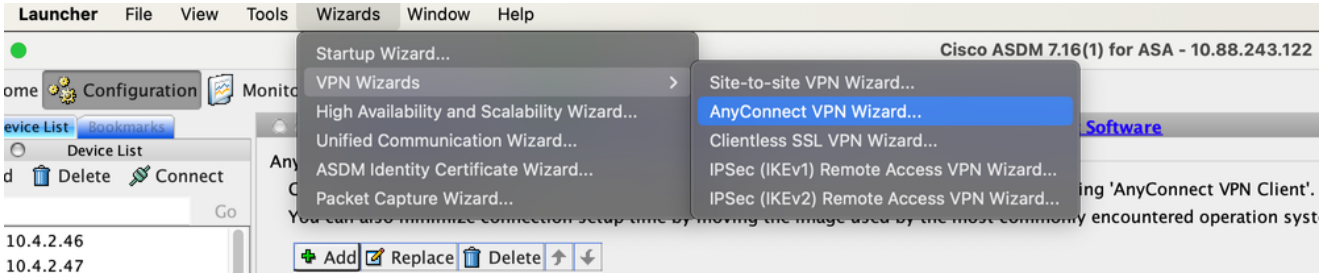


ASDM AnyConnect Configuration Wizard

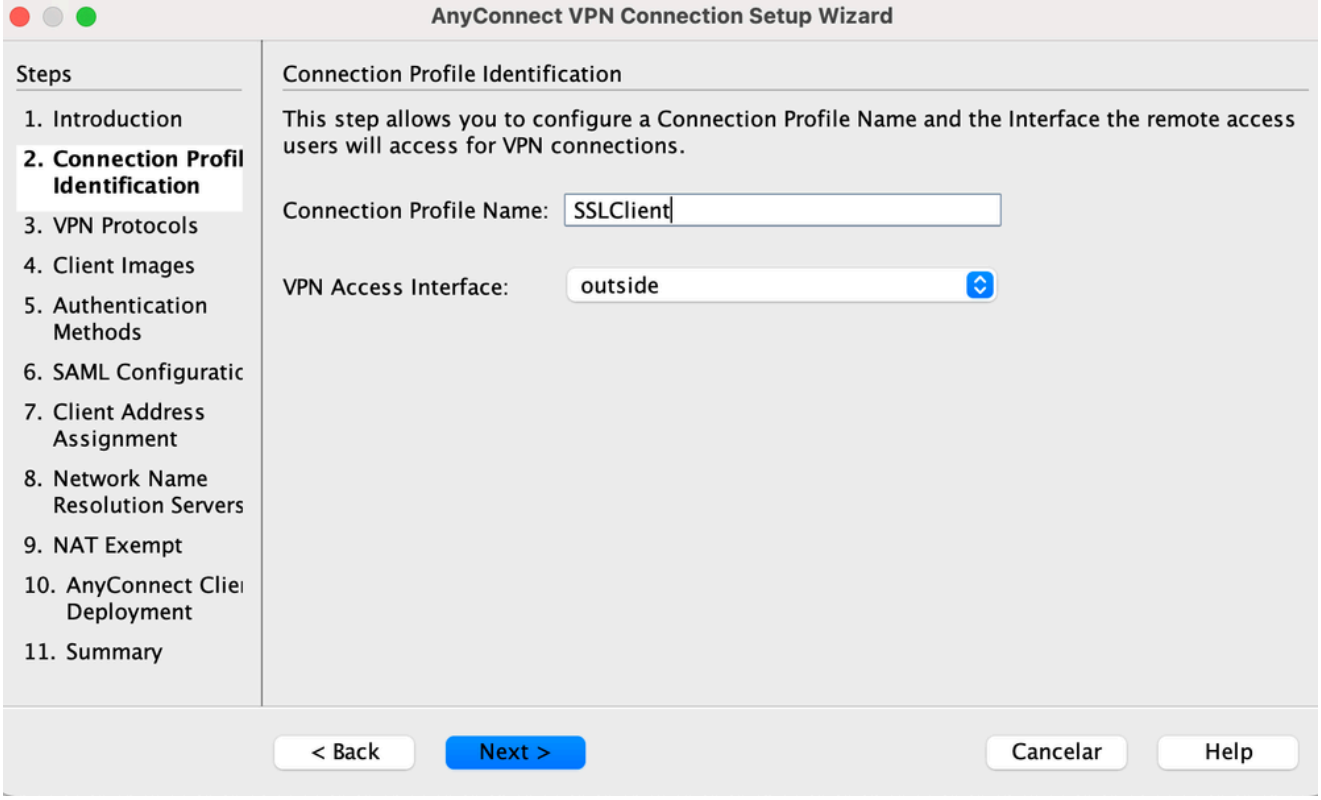
The AnyConnect Configuration Wizard can be used in order to configure the AnyConnect Secure Mobility Client. Ensure that an AnyConnect client package has been uploaded to the flash/disk of the ASA Firewall before you proceed.

Complete these steps in order to configure the AnyConnect Secure Mobility Client via the Configuration Wizard:

1. Log into the ASDM, launch the **Configuration Wizard**, and click **Next**:



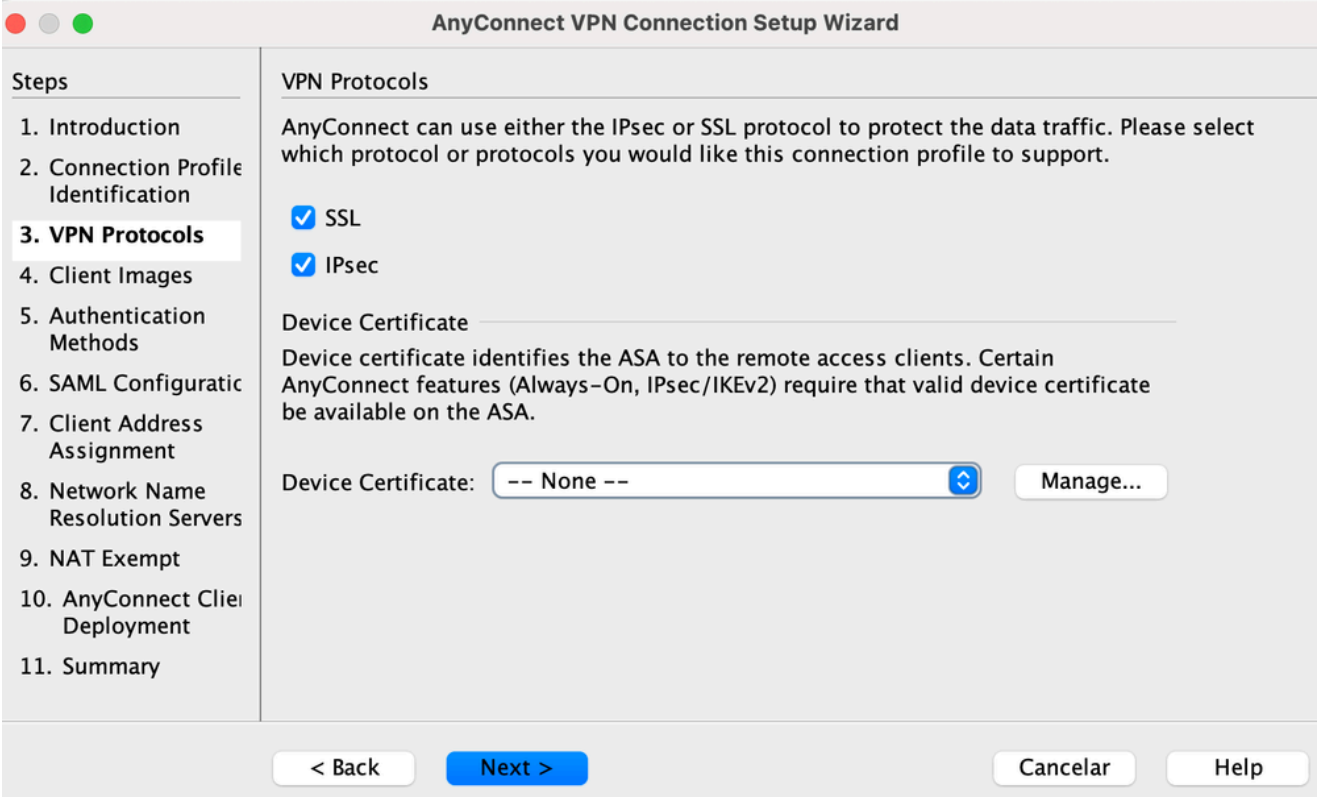
2. Enter the **Connection Profile Name**, choose the interface on which the VPN is terminated from the VPN Access Interface drop down menu, and click **Next**:



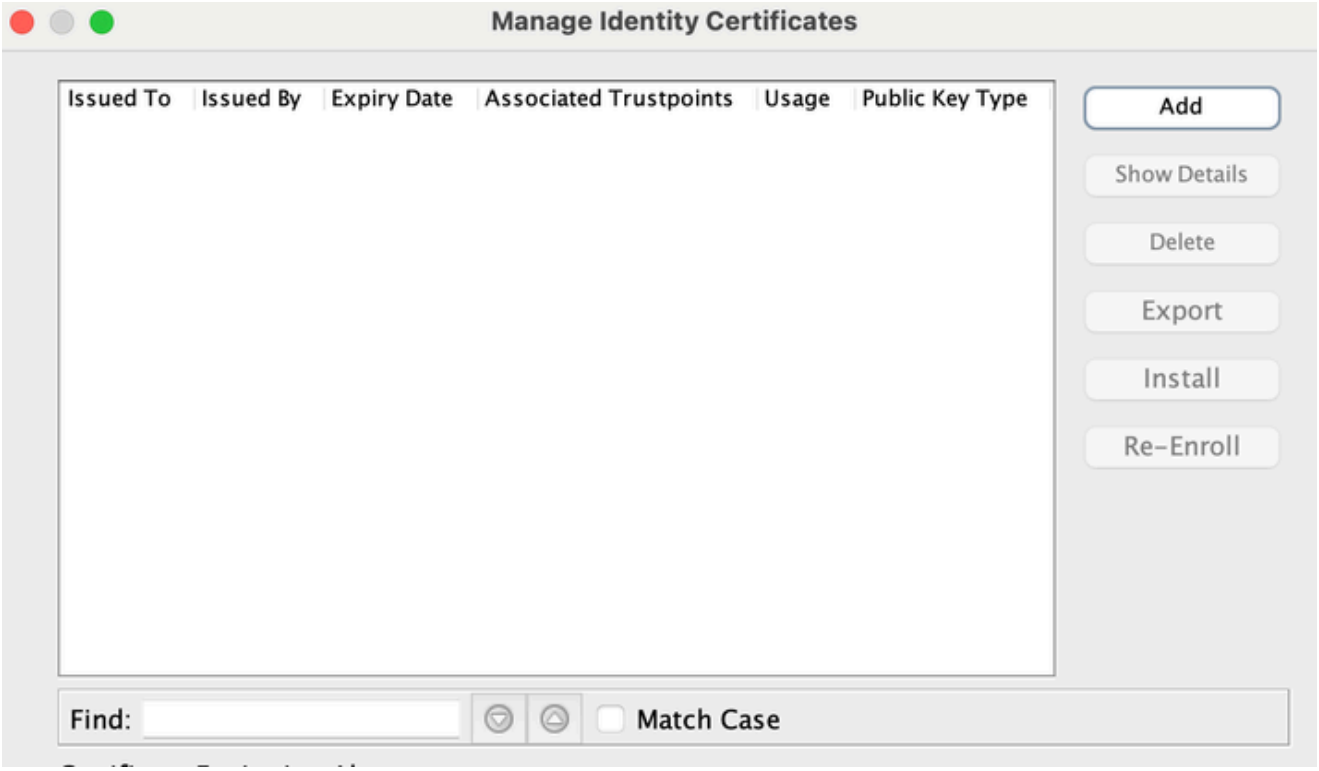
3. Check the **SSL** check box in order to enable Secure Sockets Layer (SSL). The Device Certificate can be a trusted third party Certificate Authority (CA) issued certificate (such as Verisign, or Entrust), or a self-signed certificate. If the certificate is already installed on the ASA, then it can be chosen via the drop down menu.

> **Note**: This certificate is the server-side certificate that is provided. If there are no certificates currently installed on the ASA, and a self-signed certificate must be generated, then click **Manage**.

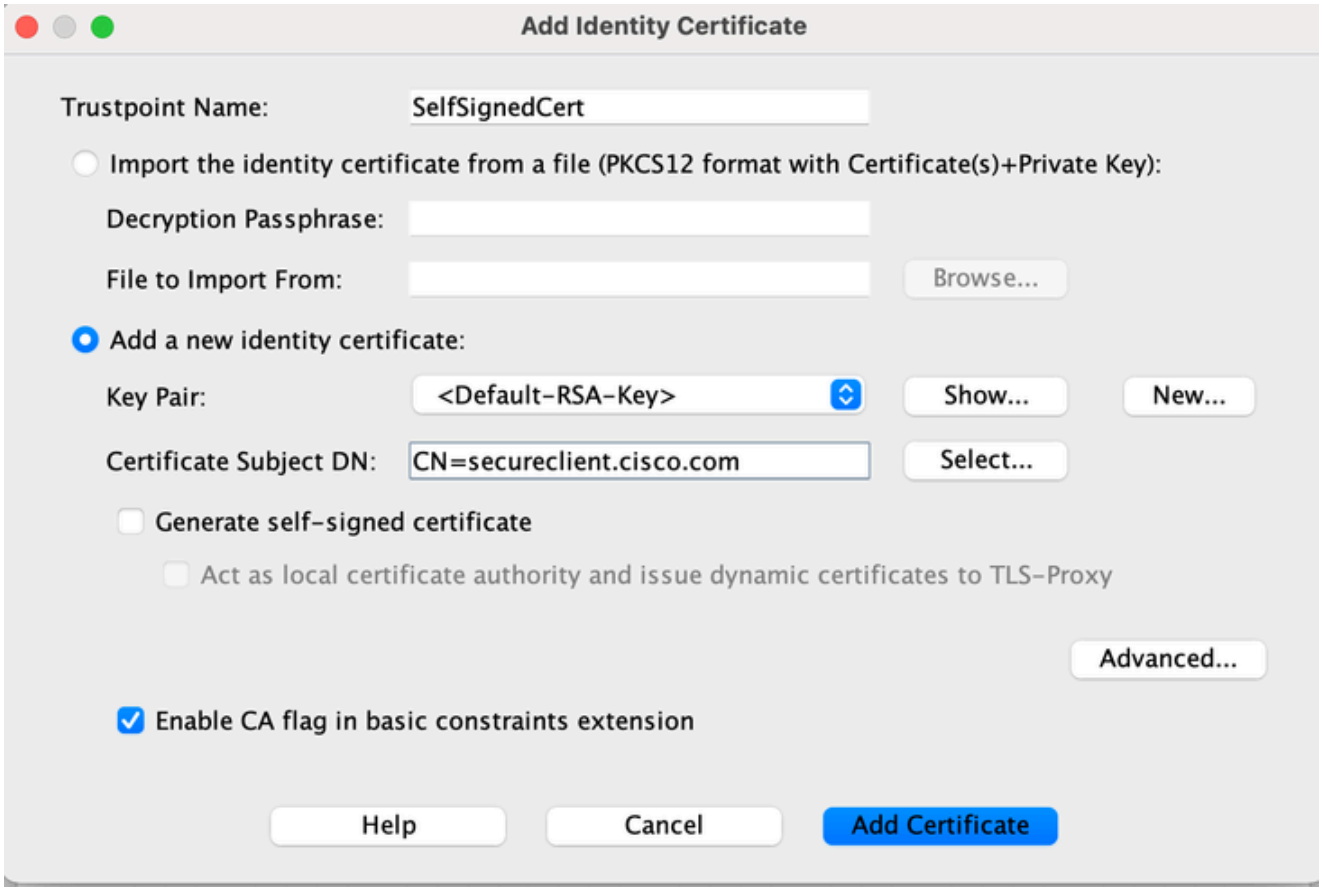
In order to install a third-party certificate, complete the steps that are described in the Configure ASA: SSL Digital Certificate Installation and Renewal Cisco document.



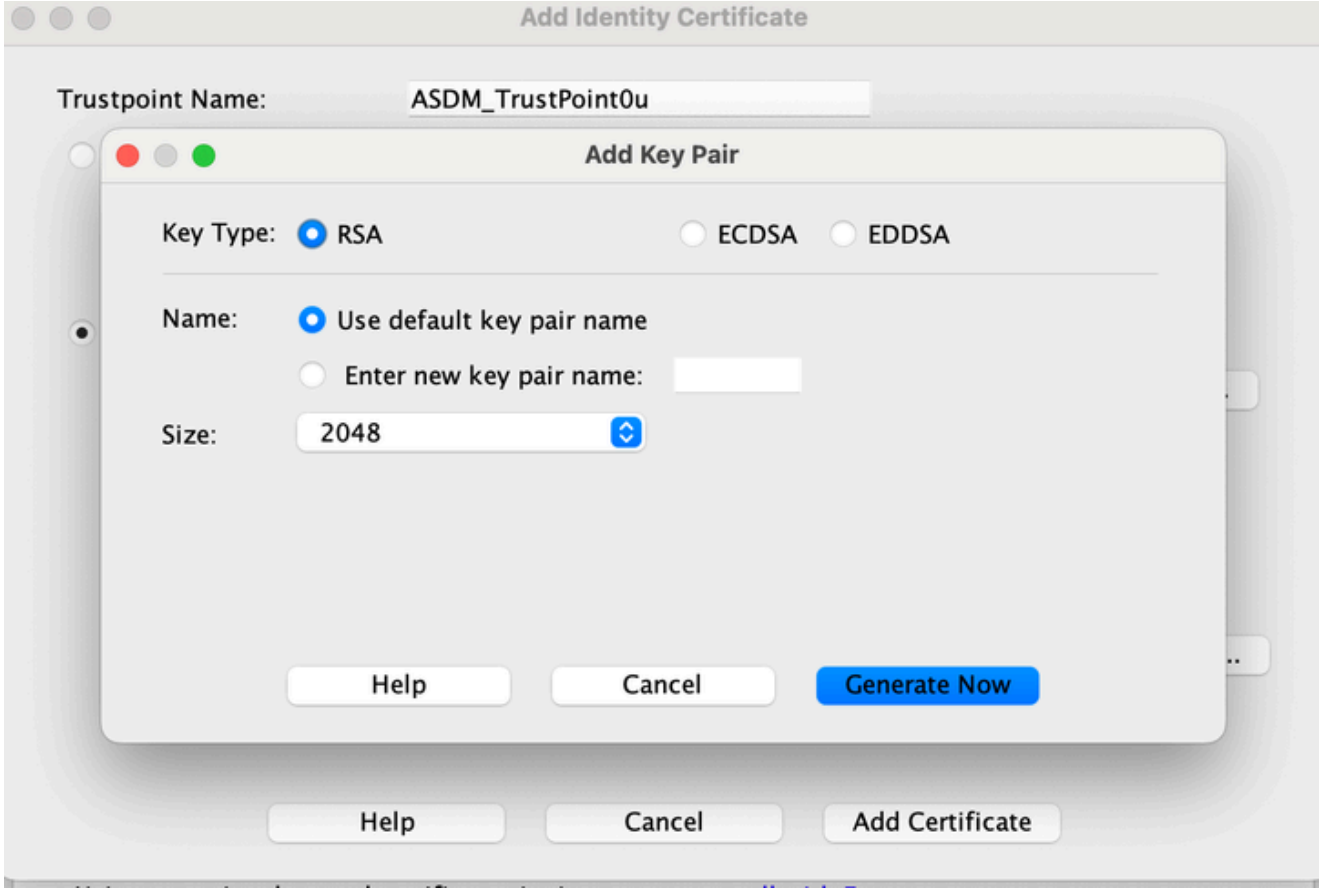
4. Click **Add**:



5. Type an appropriate name into the **Trustpoint Name** field, and click the **Add a new identity certificate** radio button. If there are no Rivest-Shamir-Addleman (RSA) key pairs present on the device, click **New** in order to generate one:

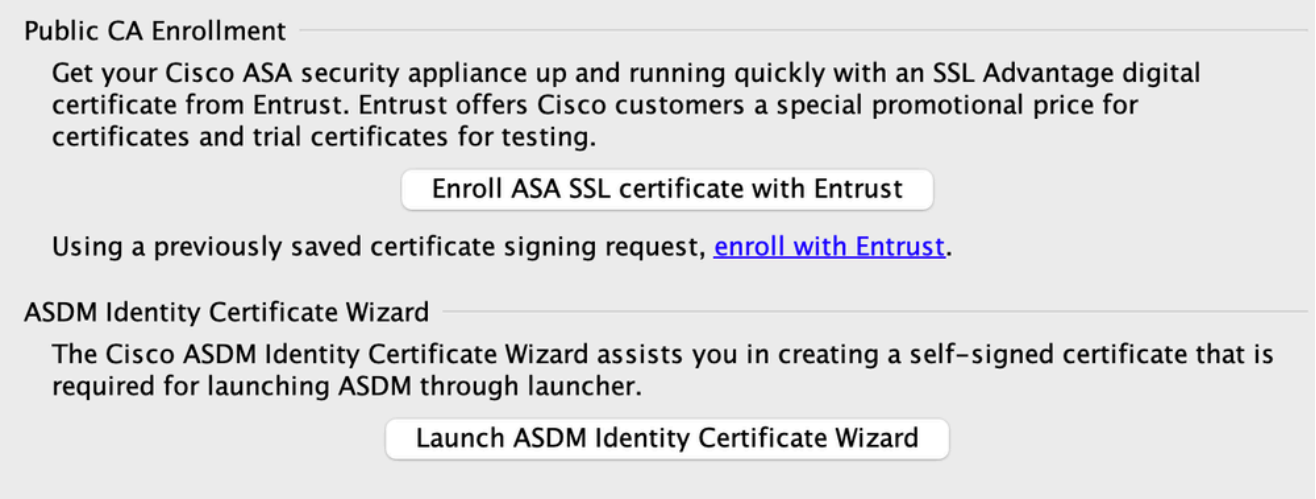


6. Click the **Use default key pair name** radio button, or click the **Enter new key pair name** radio button, and enter a new name. Select the size for the keys, and then click **Generate Now**:

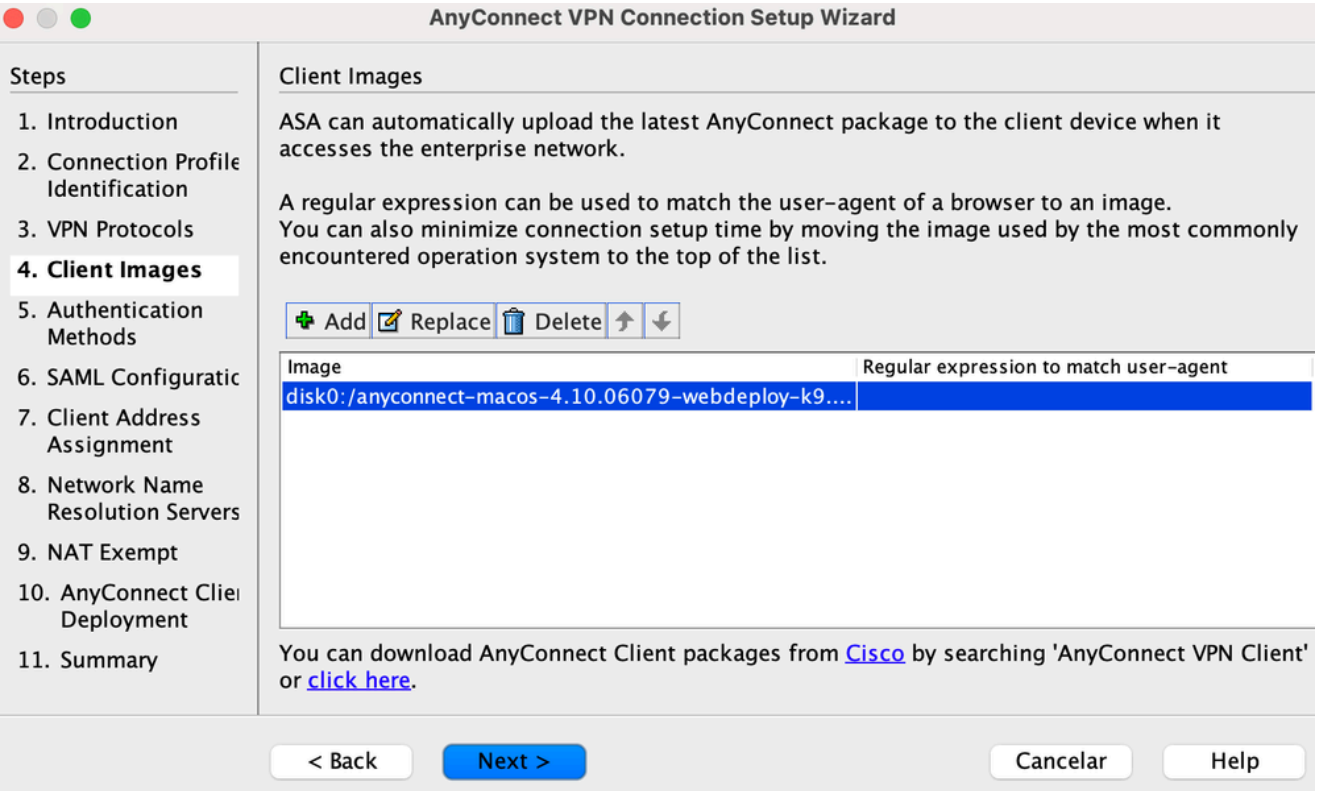


7. After the RSA key pair is generated, choose the key and check the **Generate self-signed certificate** check box. Enter the desired subject Domain Name (DN) into the **Certificate Subject DN** field, and then click **Add Certificate**:

8. Once the enrollment is complete, click **OK**, **OK**, and then **Next**:



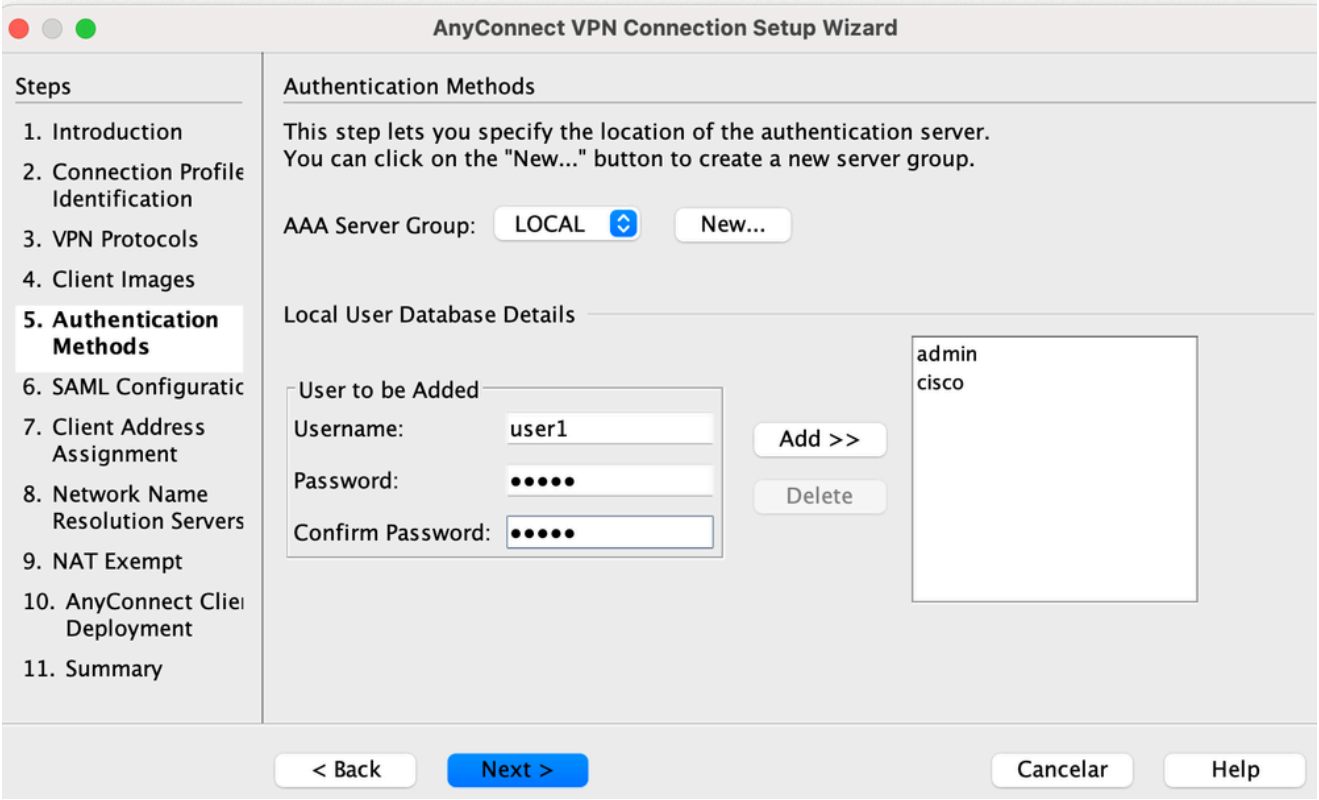
9. Click **Add** in order to add the AnyConnect Client image (the .pkg file) from the PC or from the flash. Click **Browse Flash** in order to add the image from the flash drive, or click **Upload** in order to add the image from the host machine directly:



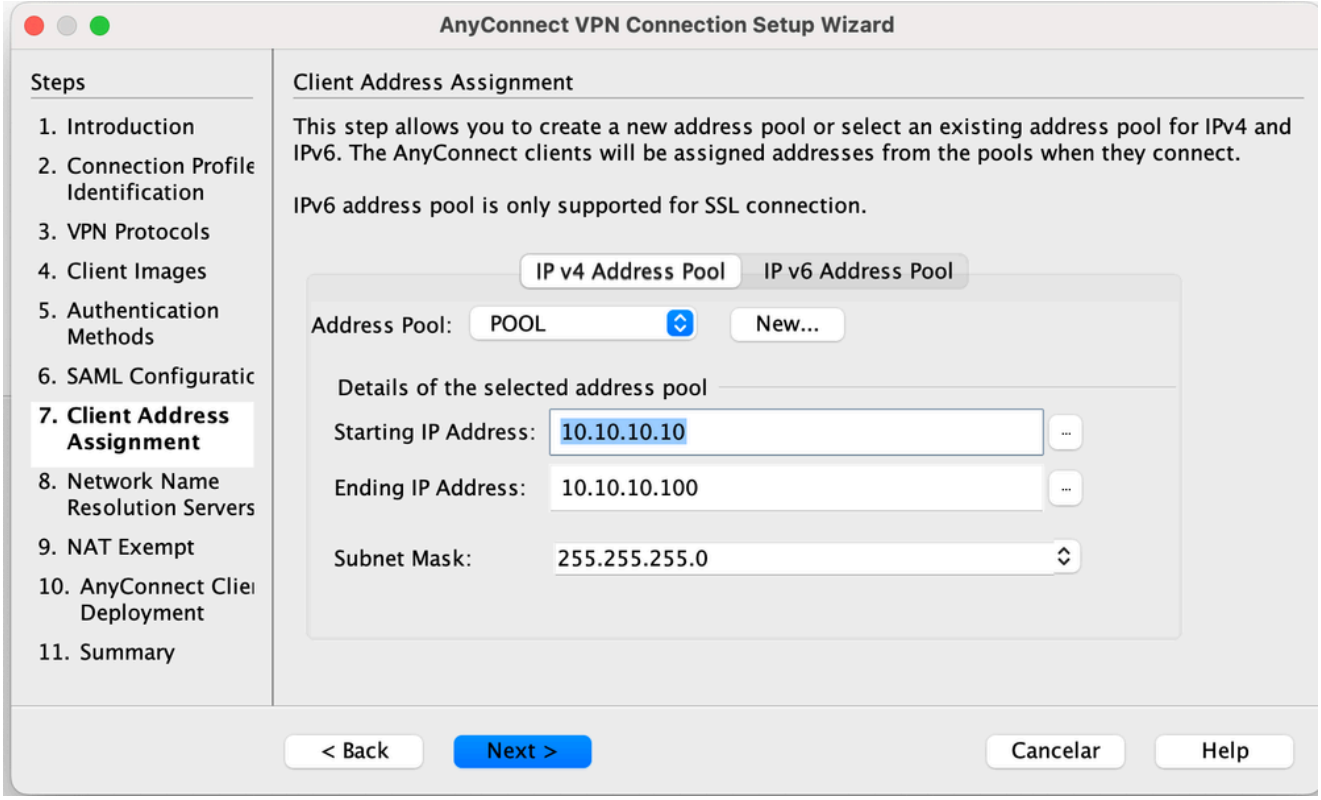
10. Once the image is added, click **Next**:

11. The user authentication can be completed via the Authentication, Authorization, and Accounting (AAA) server groups. If the users are already configured, then choose **LOCA** and click **Next**.

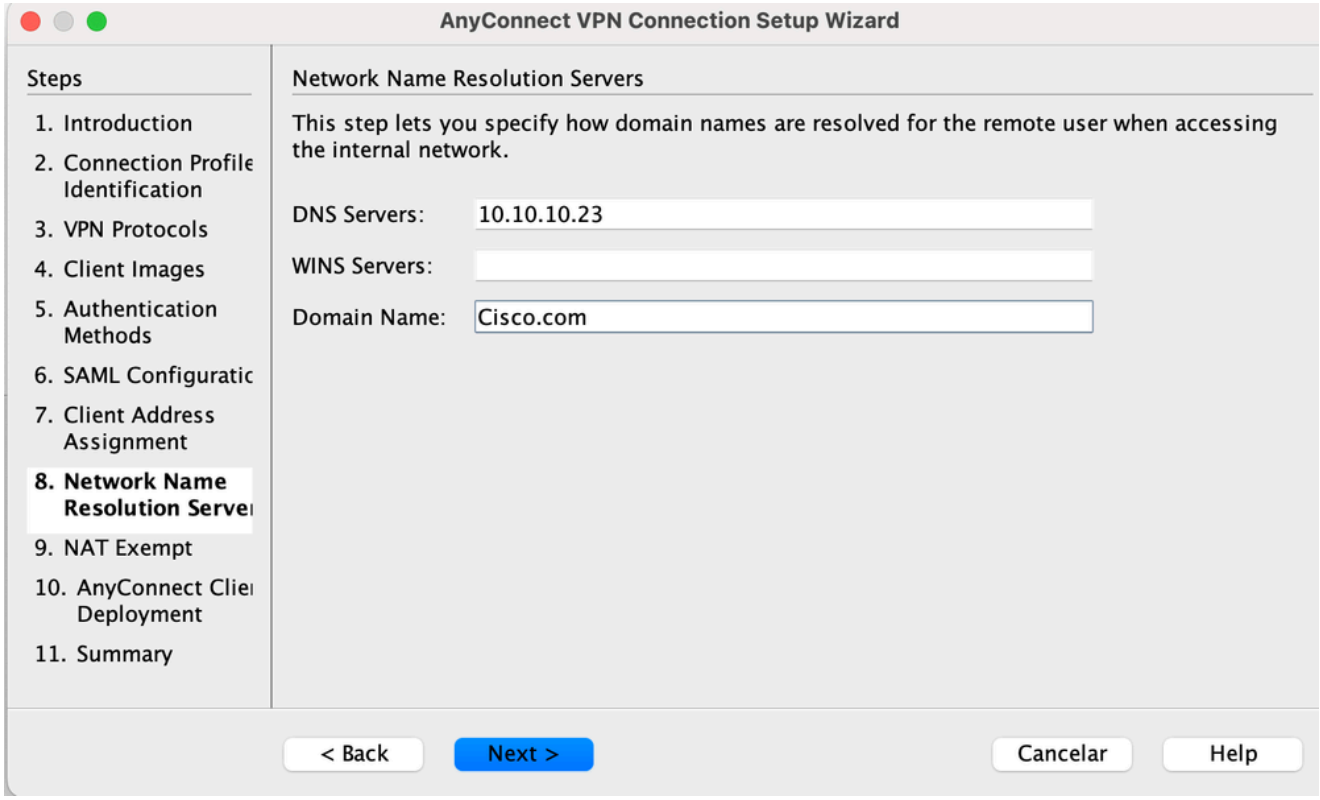
Note: In this example, LOCAL authentication is configured, which means that the local user database on the ASA can be used for authentication.



12. The address pool for the VPN client must be configured. If one is already configured, then select it from the drop down menu. If not, click **New** in order to configure a new one. Once complete, click **Next**:

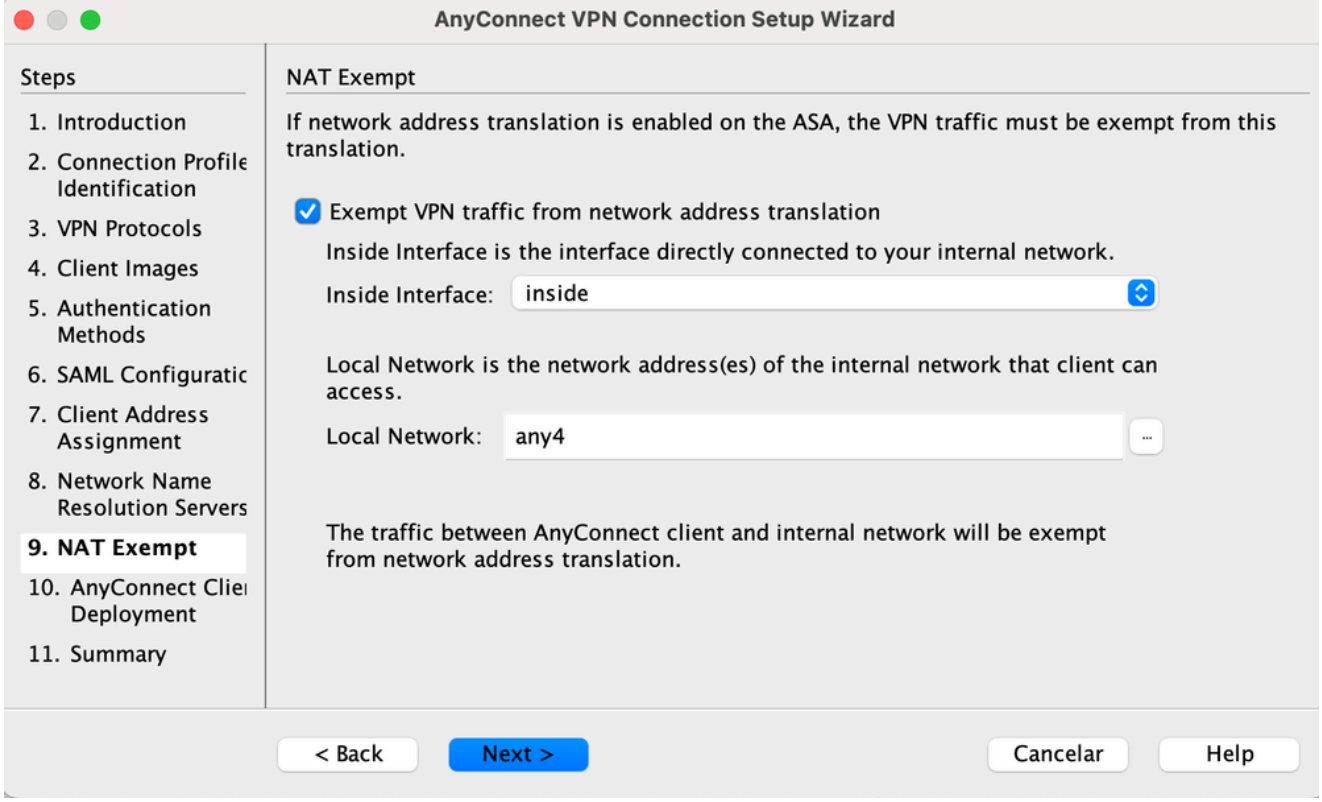


13. Input the Domain Name System (DNS) servers and DNs into the **DNS and Domain Name** fields appropriately, and then click **Next**:

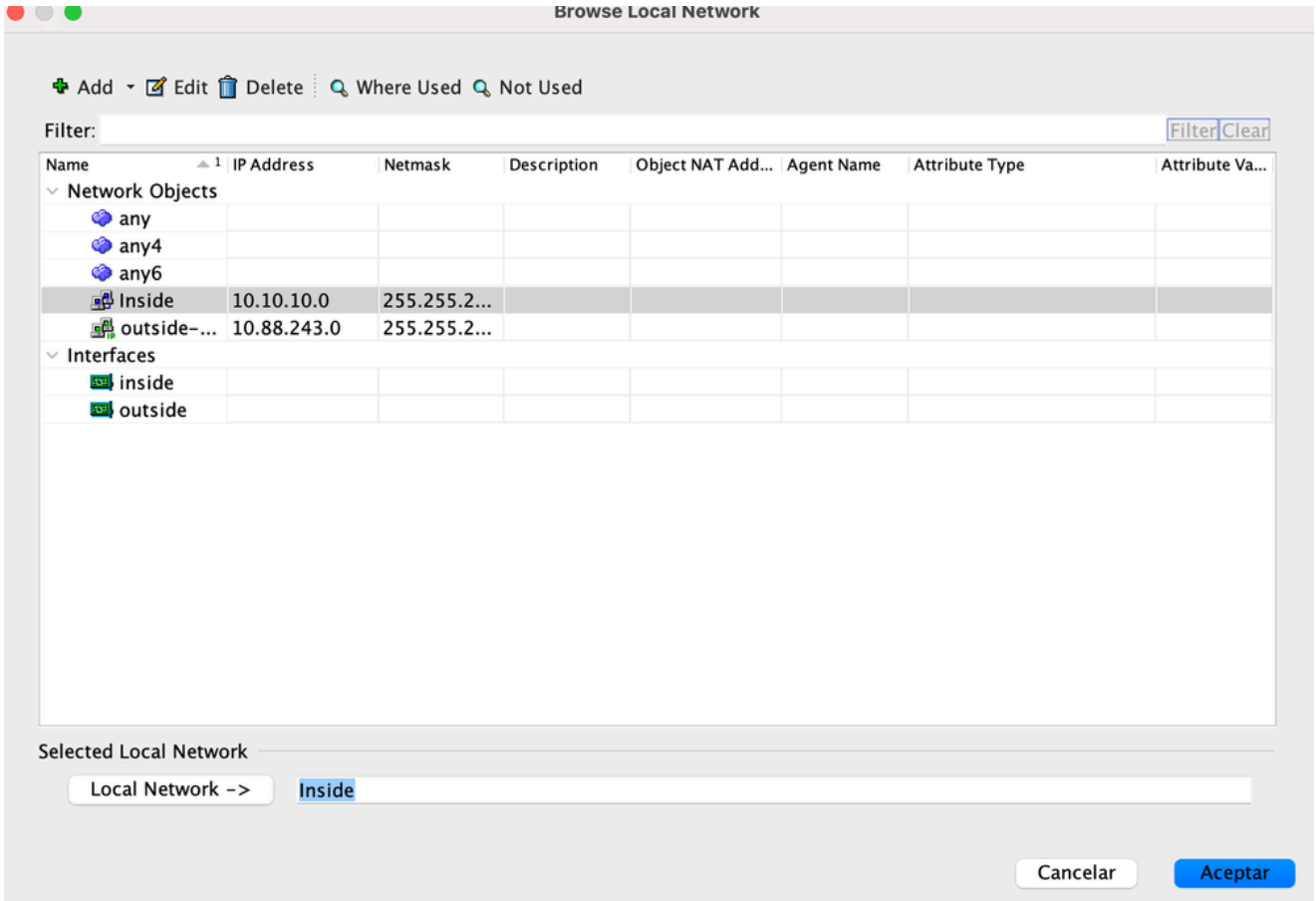


14. In this scenario, the objective is to restrict access over the VPN to the 10.10.10.0/24 network that is configured as the **Inside** (or LAN) subnet behind the ASA. The traffic between the client and the inside subnet must be exempt from any dynamic Network Address Translation (NAT).

    Check the **Exempt VPN traffic from network address translation** check box and configure the LAN and WAN interfaces that can be used for the exemption:



15. Choose the local networks that must be exempt:



16. Click **Next**, **Next**, and then **Finish**.

The AnyConnect Client configuration is now complete. However, when you configure AnyConnect via the Configuration Wizard, it configures the Split Tunnel policy as Tunnelall by default. In order to tunnel specific traffic only, split-tunneling must be implemented.

Note: If split-tunnelling is not configured, the Split Tunnel policy can be inherited from the default group-policy (DfltGrpPolicy), which is by default set to Tunnelall. This means that once the client is connected over VPN, all of the traffic (to include the traffic to the web) is sent over the tunnel.

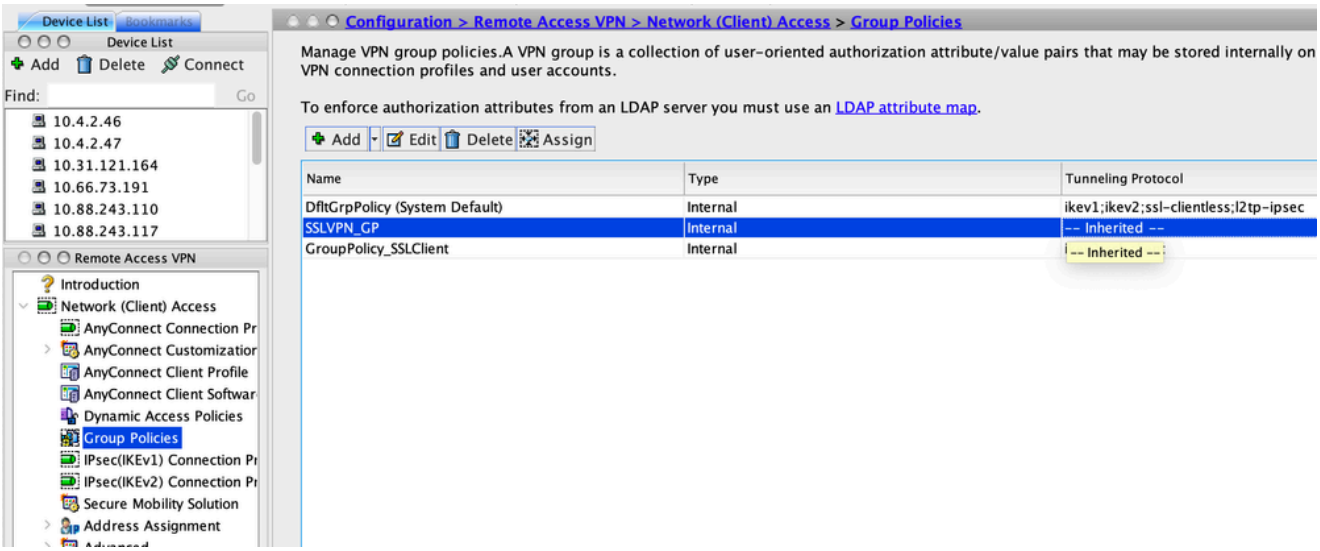
Only the traffic that is destined to the ASA WAN (or Outside) IP address can bypass the tunneling on the client machine. This can be seen in the output of the **route print** command on Microsoft Windows machines.

Split Tunnel Configuration

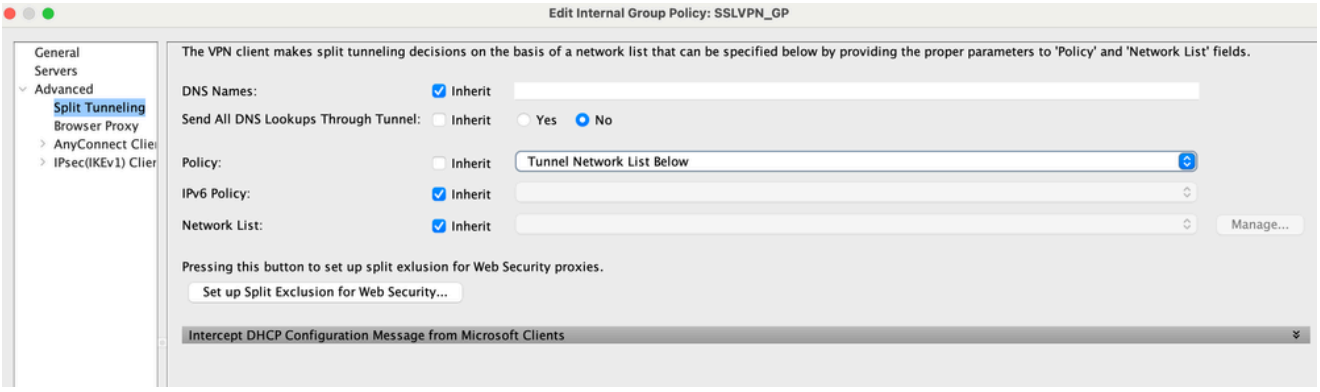
Split tunnelling is a feature that you can use in order to define the traffic for the subnets or hosts that must be encrypted. This involves the configuration of an Access Control List (ACL) that can be associated with this feature. The traffic for the subnets or hosts that is defined on this ACL can be encrypted over the tunnel from the client-end, and the routes for these subnets are installed on the PC routing table.

Complete these steps in order to move from the Tunnel-all configuration to the Split-tunnel configuration:

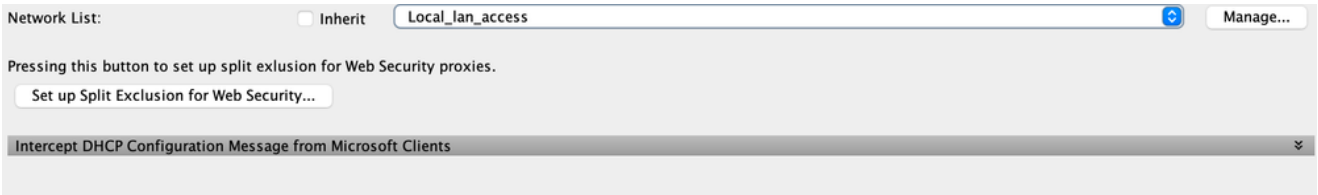
1. Navigate to **Configuration > Remote Access VPN > Group Policies**:



2. Click **Edit**, and use the navigation tree in order to navigate to **Advanced > Split Tunneling**. Uncheck the **Inherit** check box in the Policy section, and select **Tunnel Network List Below** from the drop down menu:



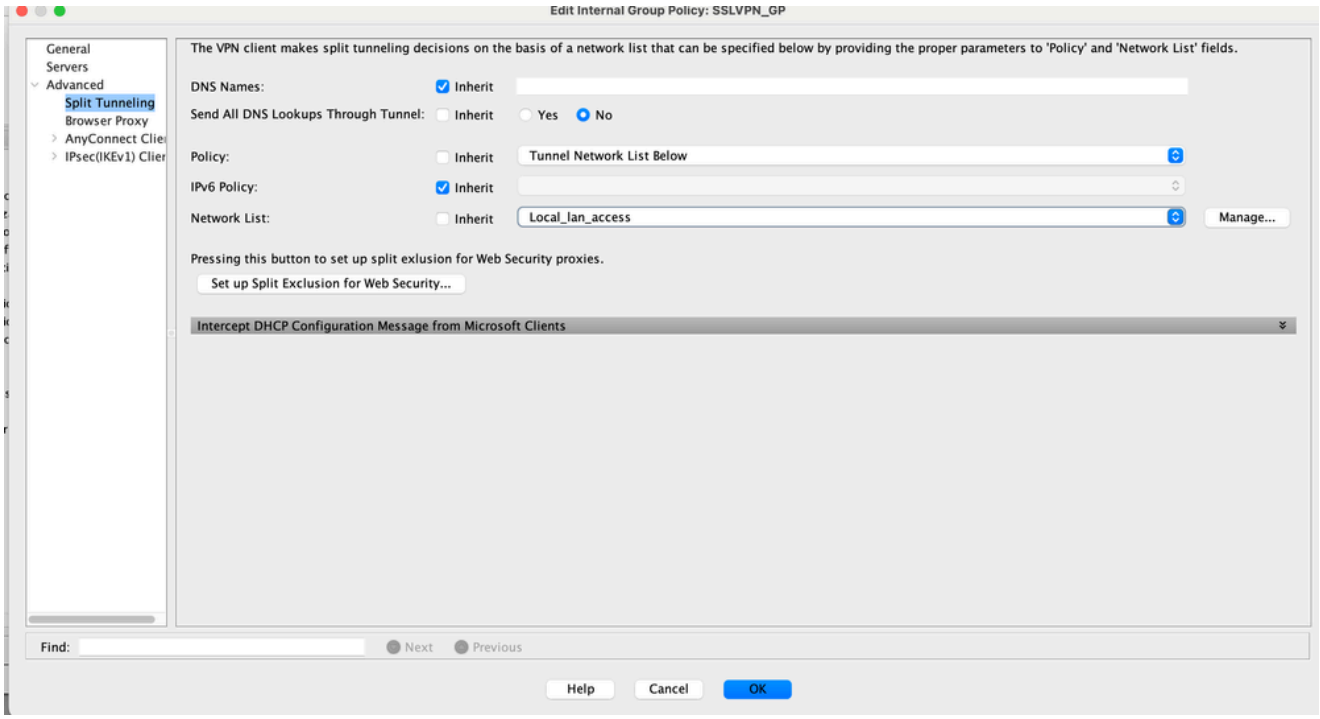
3. Uncheck the **Inherit** check box in the Network List section, and click **Manage** in order to select the ACL that specifies the LAN network(s) to which the client needs access:



4. Click **Standard ACL**, **Add**, **Add ACL**, and then **ACL name.**

5. Click **Add ACE** in order to add the rule.

6. Click **OK**.



7. Click **Apply**.

Once connected, the routes for the subnets or hosts on the split ACL are added to the routing table of the client machine. On Microsoft Windows machines, this can be viewed in the output of the **route print** command. The next hop for these routes can be an IP address from the client IP pool subnet (usually the first IP address of the subnet):

<#root>

```
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

.

On MAC OS machines, enter the **netstat -r** command in order to view the PC routing table:

<#root>

```
$
```

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

.

Download and Install AnyConnect Client

There are two methods that you can use in order to deploy Cisco AnyConnect Secure Mobility Client on the user machine:

- Web deployment
- Standalone deployment

Both of these methods are explained in greater detail in the sections that follow.

Web Deployment

In order to use the web deployment method, enter the **https://<ASA's FQDN>or<ASA's IP>** URL into a browser on the client machine, which brings you to the WebVPN portal page.

Note: If Internet Explorer (IE) is used, the installation is completed mostly via ActiveX, unless you are forced to use Java. All other browsers use Java.

Once logged into the page, the installation can begin on the client machine, and the client can connect to the ASA after the installation is complete.

Note: You can be prompted for permission to run ActiveX or Java. This must be allowed in order to proceed with the installation.

Standalone Deployment

Complete these steps in order to use the standalone deployment method:

1. Download the AnyConnect Client image from the Cisco website. In order to choose the correct image for download, refer to the Cisco AnyConnect Secure Mobility Client web page. A download link is provided on this page. Navigate to the download page and select the appropriate version. Perform a search for **Full installation package - Window / Standalone installer (ISO)**.

> **Note**: An ISO installer image is then downloaded (such as anyconnect-win-4.10.06079-pre-deploy-k9.iso).

2. Use WinRar or 7-Zip in order to extract the contents of the ISO package:

3. Once the contents are extracted, run the **Setup.exe** file and choose the modules that must be installed along with Cisco AnyConnect Secure Mobility Client.

CLI Configuration

This section provides the CLI configuration for the Cisco AnyConnect Secure Mobility Client for reference purposes.

<#root>

```
ASA Version 9.16(1)
!
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:/asa916-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-7161.bin
```

```
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

!************** NAT exemption Configuration *****************
!This can 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
```

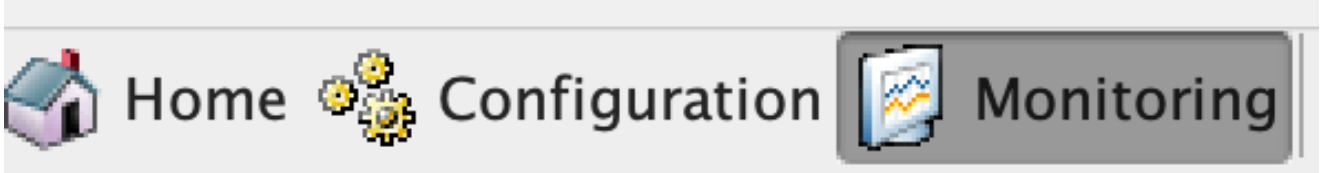
```
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 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-4.10.06079-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
```

Verify

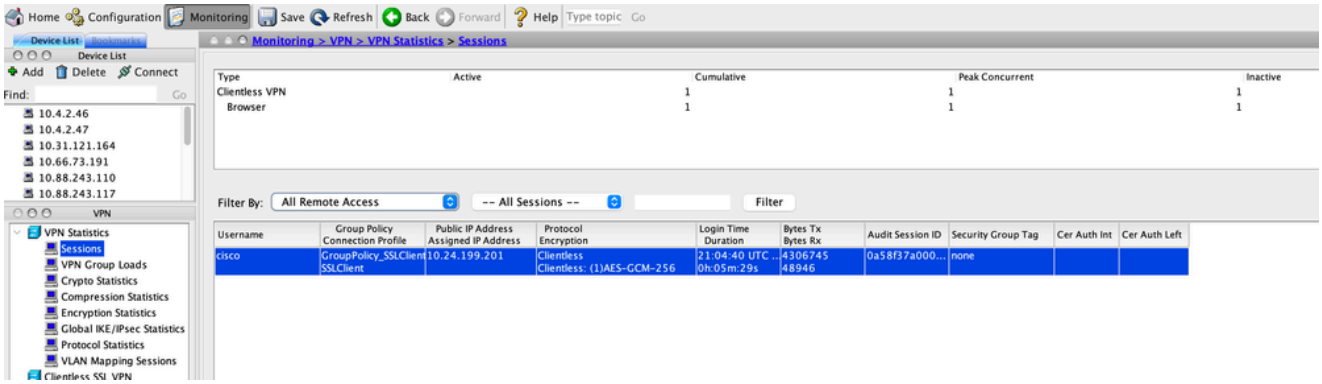
Complete these steps in order to verify the client connection and the various parameters that are associated to that connection:

1. Navigate to **Monitoring** > **VPN** on the ASDM:

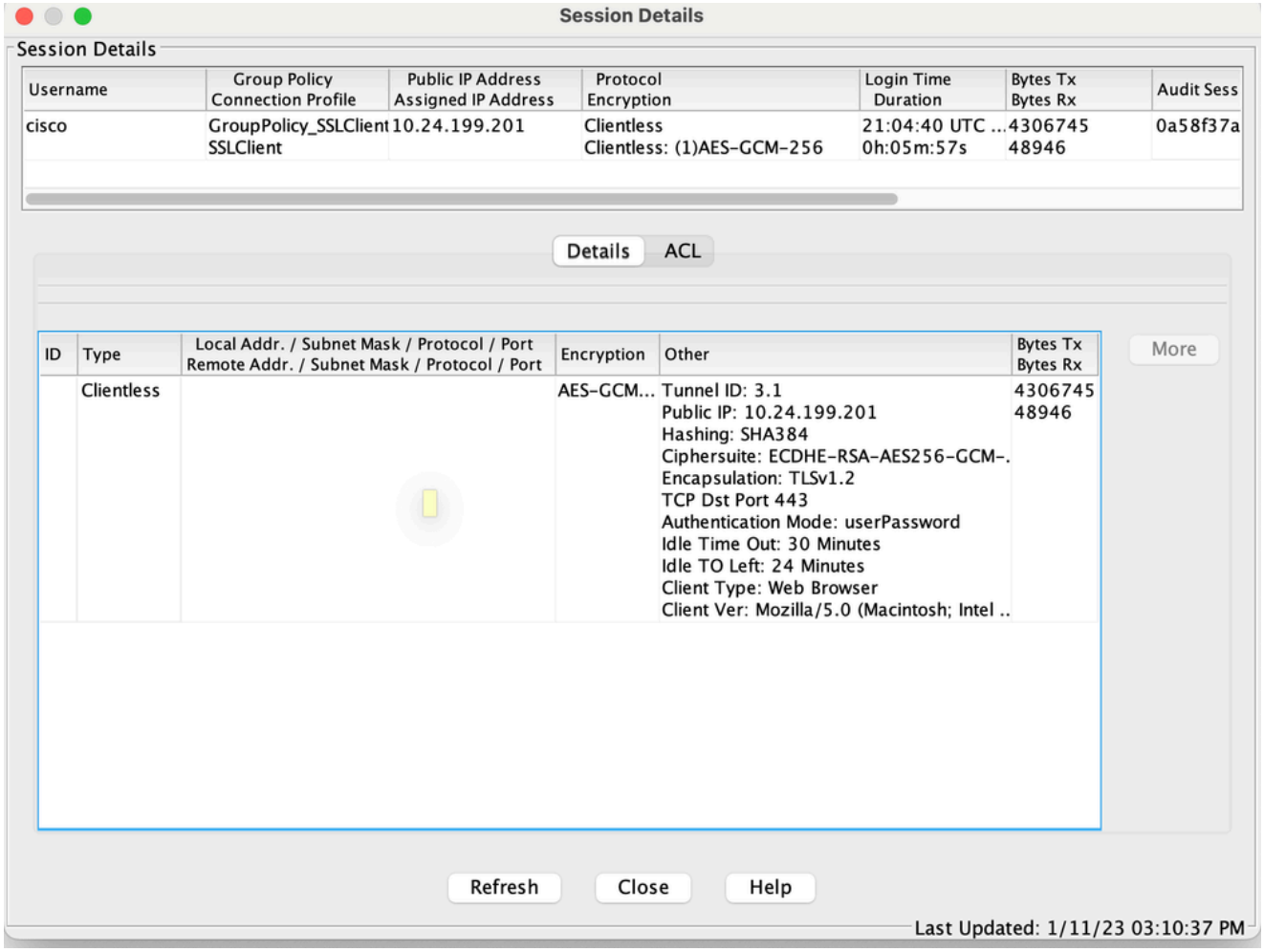


2. You can use the **Filter By** option in order to filter the type of VPN. Select **AnyConnect Client** from the drop down menu and all of the AnyConnect Client sessions.

> **Tip**: The sessions can be further filtered with the other criteria, such as Username and IP address.



3. Double-click a session in order to obtain further details about that particular session:



4. Enter the **show vpn-sessiondb anyconnect** command into the CLI in order to obtain the session details:

<#root>

```
#

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. You can use the other filter options in order to refine the results:

<#root>

#

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
```

Troubleshoot

You can use the AnyConnect Diagnostics and Reporting Tool (DART) in order to collect the data that is useful to troubleshoot AnyConnect installation and connection problems. The DART Wizard is used on the computer that runs AnyConnect. The DART assembles the logs, status, and diagnostic information for the Cisco Technical Assistance Center (TAC) analysis and does not require administrator privileges to run on the client machine.

Install the DART

Complete these steps to install the DART:

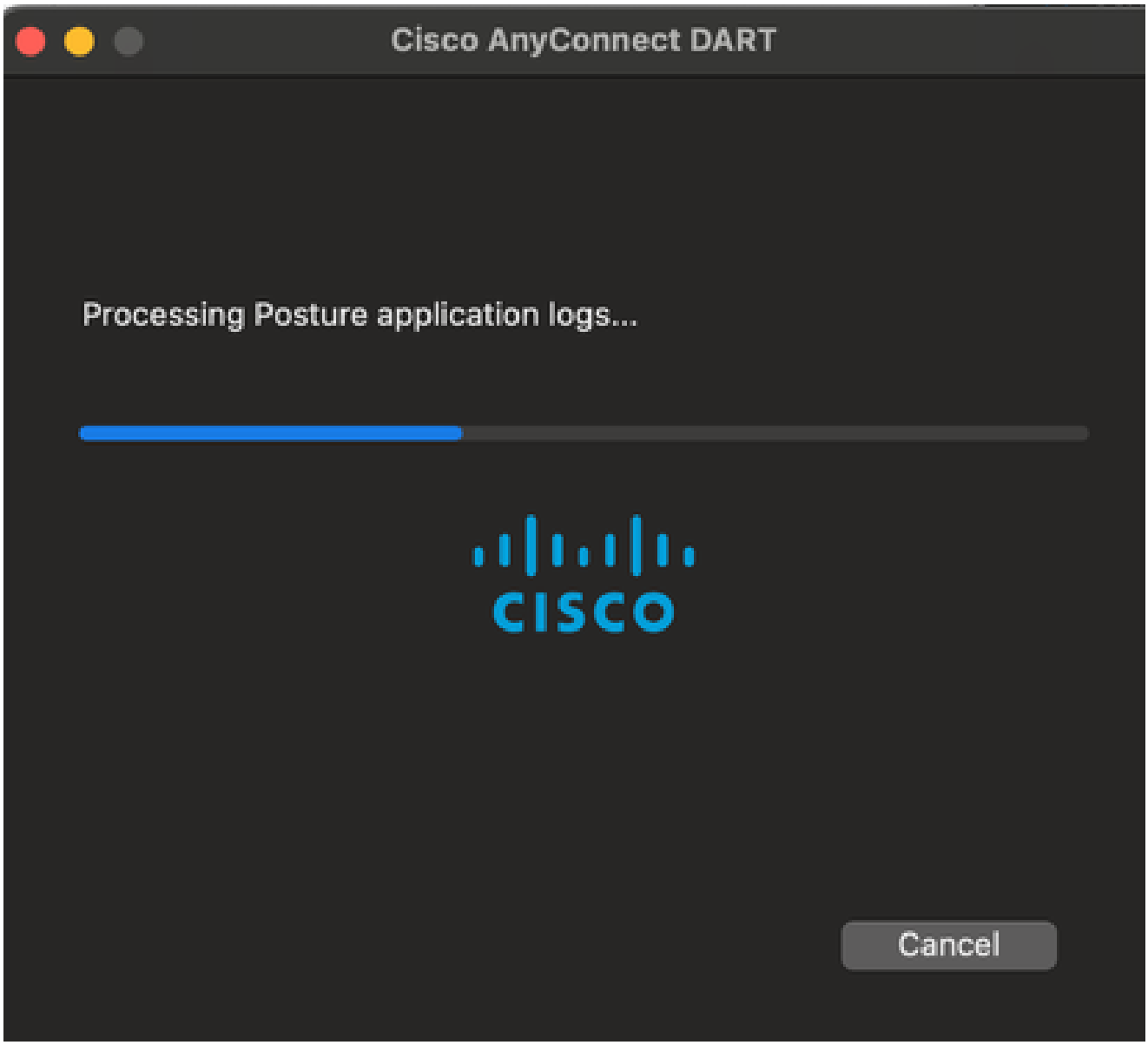
1. Download the AnyConnect Client image from the Cisco website. In order to choose the correct image for download, refer to the Cisco AnyConnect Secure Mobility Client web page. A download link is provided on this page. Navigate to the download page and select the appropriate version. Perform a search for **Full installation package - Window / Standalone installer (ISO)**.

   > **Note**: An ISO installer image is then downloaded (such as anyconnect-win-4.10.06079-pre-deploy-k9.iso).

2. Use WinRar or 7-Zip in order to extract the contents of the ISO package:

3. Browse to the folder to which the contents were extracted.

4. Run the **Setup.exe** file and select only **Anyconnect Diagnostic And Reporting Tool**:

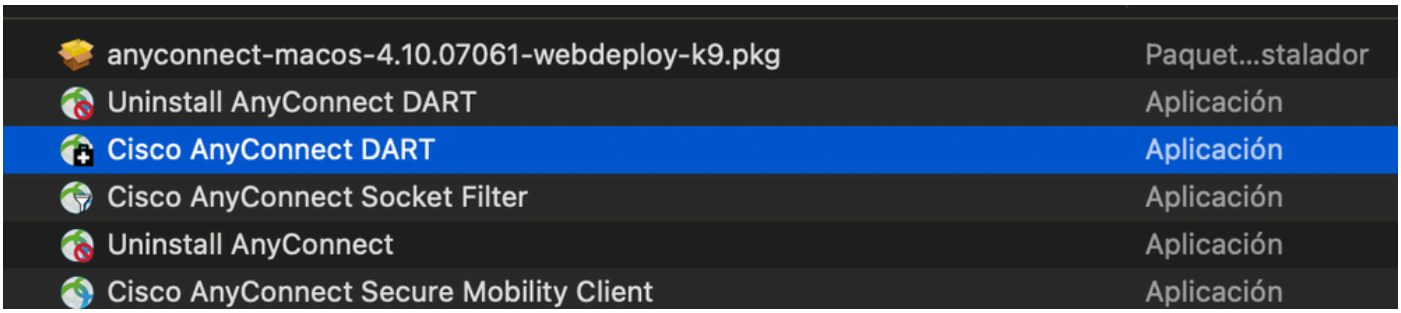


Run the DART

Here is some important information to consider before you run the DART:

- The issue must be recreated at least once before you run the DART.
- The date and time on the user machine must be noted when the issue is recreated.

Run the DART from the **Start Menu** on the client machine:



Either Default or Custom mode can be selected. Cisco recommends that you run the DART in the Default

mode so that all of the information can be captured in a single shot.

Once completed, the tool saves the DART bundle .zip file to the client desktop. The bundle can then be emailed to the TAC (after you open a TAC case) for further analysis.