在 ASA 上使用拆分隧道功能配置 AnyConnect Secure Mobility Client

目录

简介

本文档介绍如何在运行软件版本 9.3(2) 的思科自适应安全设备 (ASA) 上通过思科自适应安全设备管理器 (ASDM) 配置 Cisco AnyConnect Secure Mobility Client。

先决条件

要求

Cisco AnyConnect安全移动客户端网络部署软件包应下载到ASDM访问ASA的本地桌面。如需下载客户端软件包，请参阅 Cisco AnyConnect Secure Mobility Client 网页。各种操作系统(OS)的Web部署包可以同时上传到ASA。

以下是各种操作系统的Web部署文件名：

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

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

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

本文档提供有关如何通过 ASDM 使用 Cisco AnyConnect 配置向导来配置 AnyConnect 客户端并启用拆分隧道的分步详细信息。

分割隧道用于只能通过隧道传输特定流量的场景，而不是所有客户端机器生成的流量在连接时通过VPN传输的场景。使用 AnyConnect 配置向导会默认在 ASA 上生成 *tunnel-all* 配置。分割隧道必须单独配置，本文档的章节将对此作进一步详细说明。

在此配置示例中，目的是通过 VPN 隧道发送 10.10.10.0/24 子网（ASA 后面的 LAN 子网）的流量，而来自客户端计算机的所有其他流量都通过其各自的互联网线路转发。

AnyConnect 许可证信息

以下是一些指向有关 Cisco AnyConnect Secure Mobility Client 许可证的有用信息的链接：

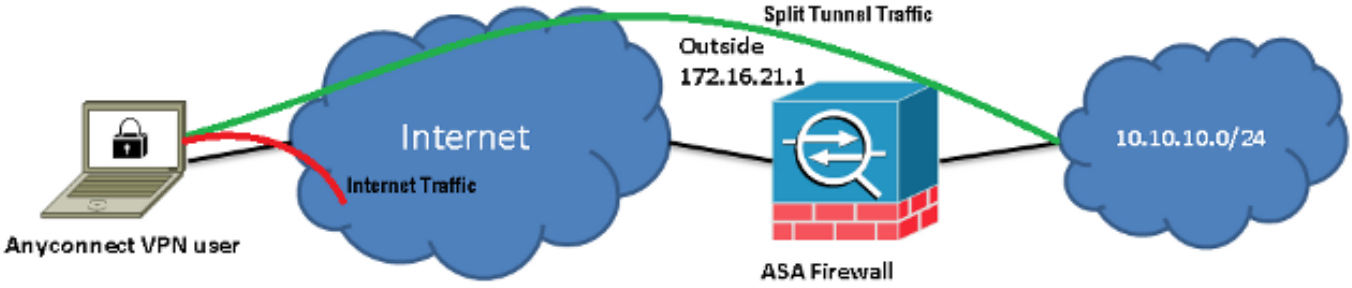
- 如需确定 AnyConnect Secure Mobility Client 和相关功能所需的许可证，请参阅《AnyConnect Secure Mobility Client 功能、许可证和操作系统，版本 3.1》文档。
- 有关 AnyConnect Apex 和 Plus 许可证的信息，请参阅《Cisco AnyConnect 订购指南》。
- 有关 IP 电话和移动连接的附加许可证要求的信息，请参阅《IP 电话和移动 VPN 连接需要什么 ASA 许可证？》文档。

配置

本节介绍如何在ASA上配置Cisco AnyConnect安全移动客户端。

网络图

本文档中的示例使用的拓扑如下所示：

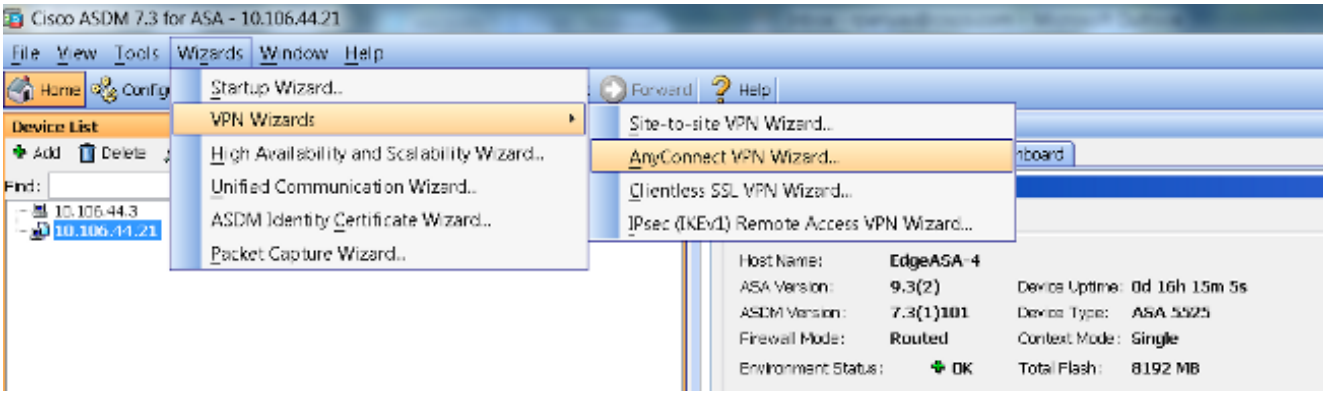


ASDM AnyConnect 配置向导

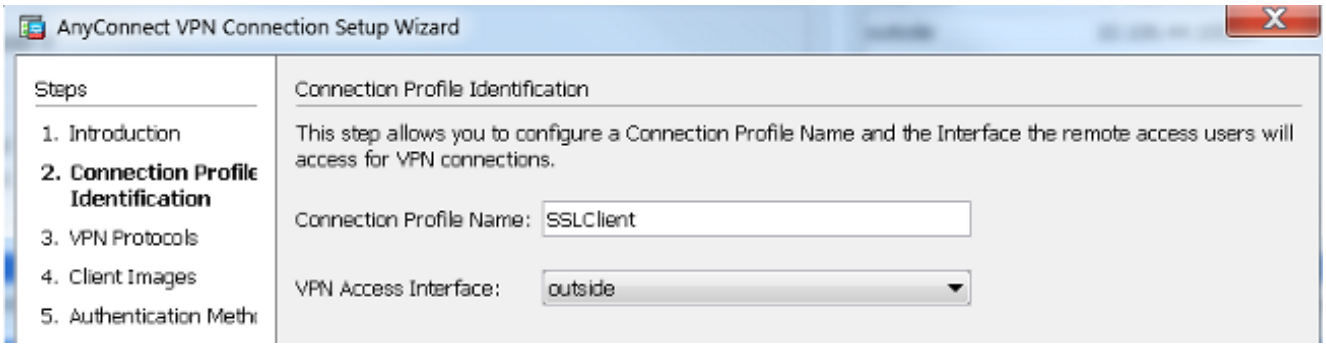
AnyConnect配置向导可用于配置AnyConnect安全移动客户端。在继续之前，请确保AnyConnect客户端软件包已上传到ASA防火墙的闪存/磁盘。

完成以下步骤，以通过配置向导配置 AnyConnect Secure Mobility Client。

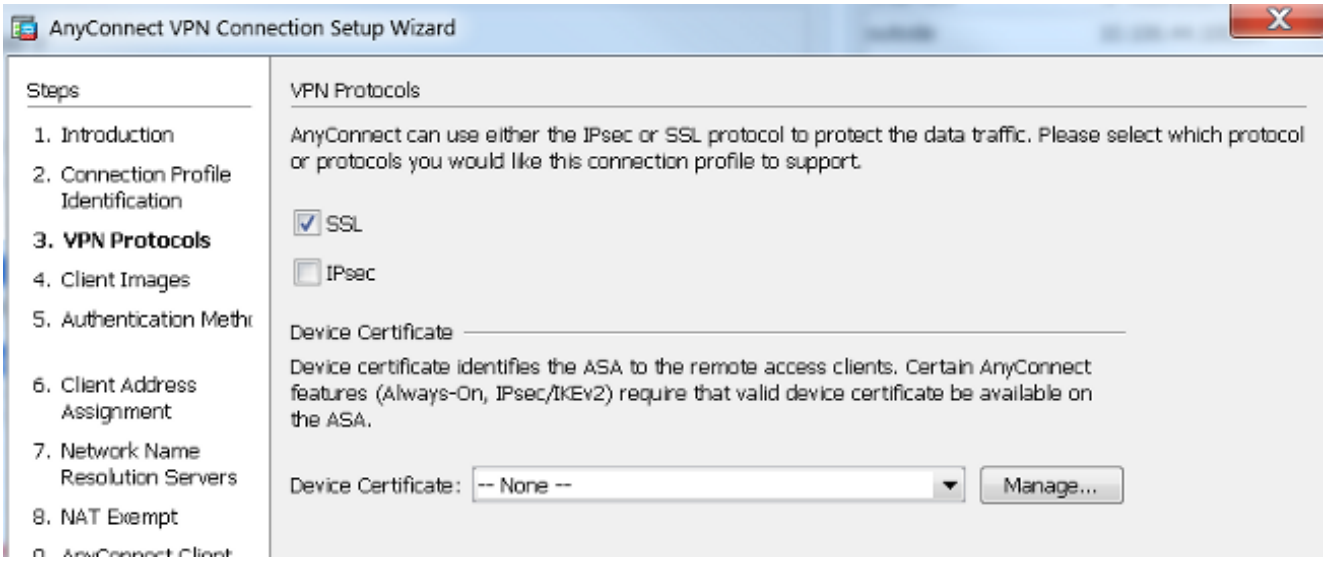
1. 登录 ASDM，启动**配置向导**，然后点击**下一步**：



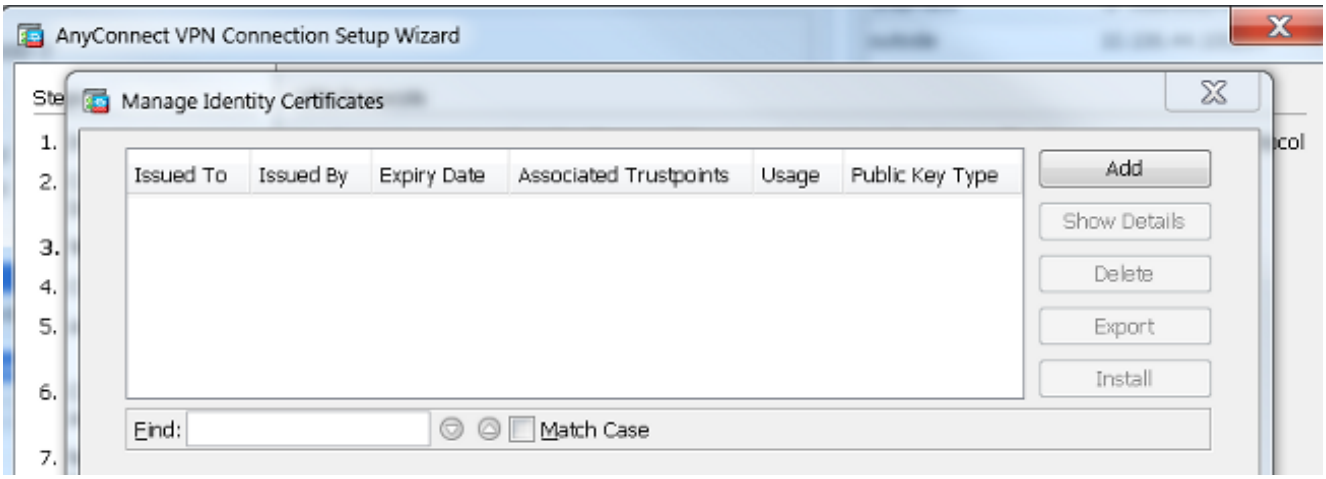
2. 输入*Connection Profile Name*，从“VPN Access Interface”下拉菜单中选择VPN将终止在*其上的接*口，然后单击**Next**:



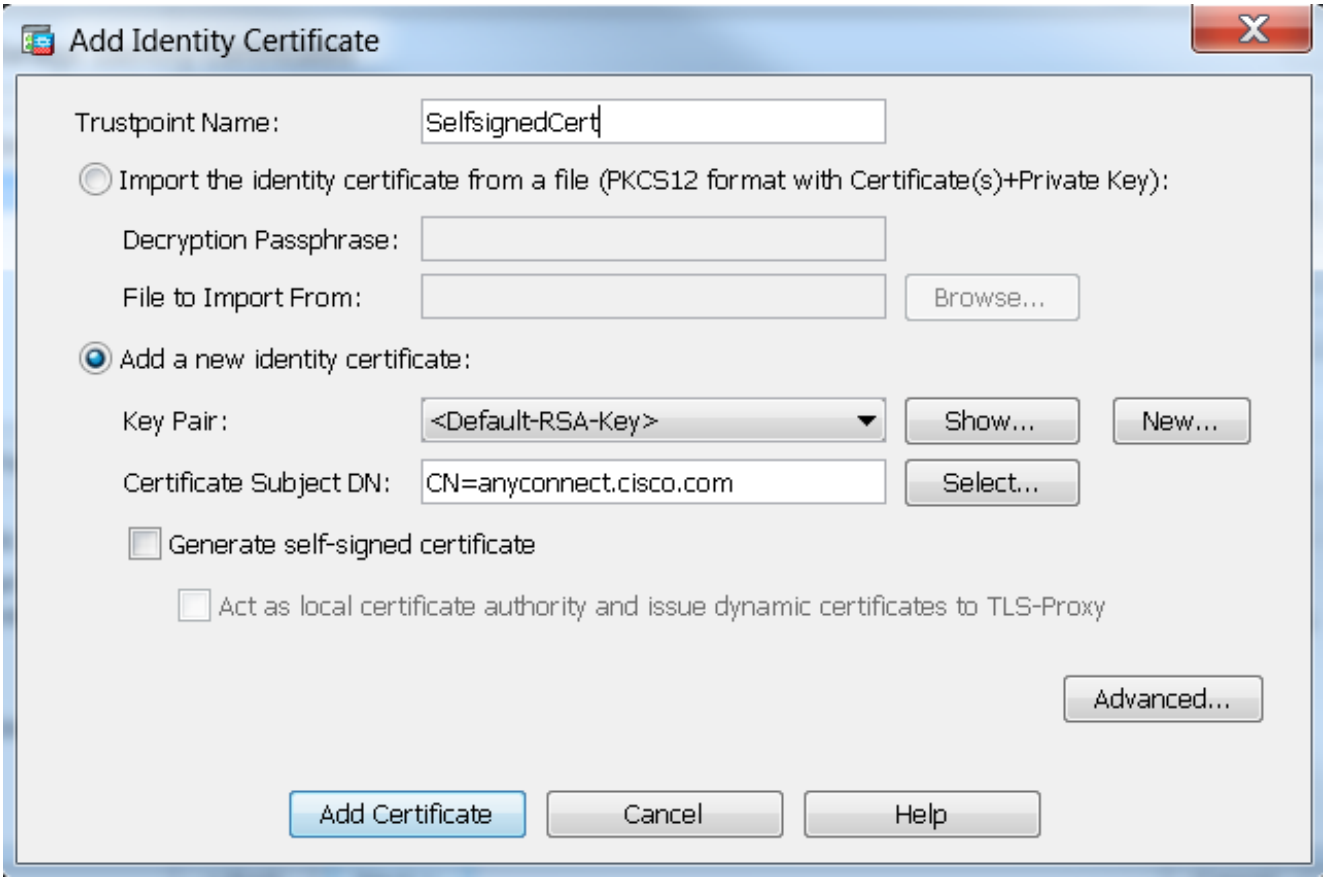
3. 选中 **SSL** 复选框以启用安全套接字层 (SSL)。 *设备证书*可以是受信任第三方证书颁发机构 (CA) 颁发的证书（例如 Verisign 或 Entrust），也可以是自签名证书。如果 ASA 上已安装证书，则可以通过下拉菜单选择证书。 **注意**：此证书是将提供的服务器端证书。如果 ASA 上当前未安装证书，并且必须生成自签名证书，则点击**管理**。要安装第三方证书，请完成[ASA 8.x手动安装第三方供应商证书以与WebVPN配置示例Cisco文档一起使用中描述的]步骤。



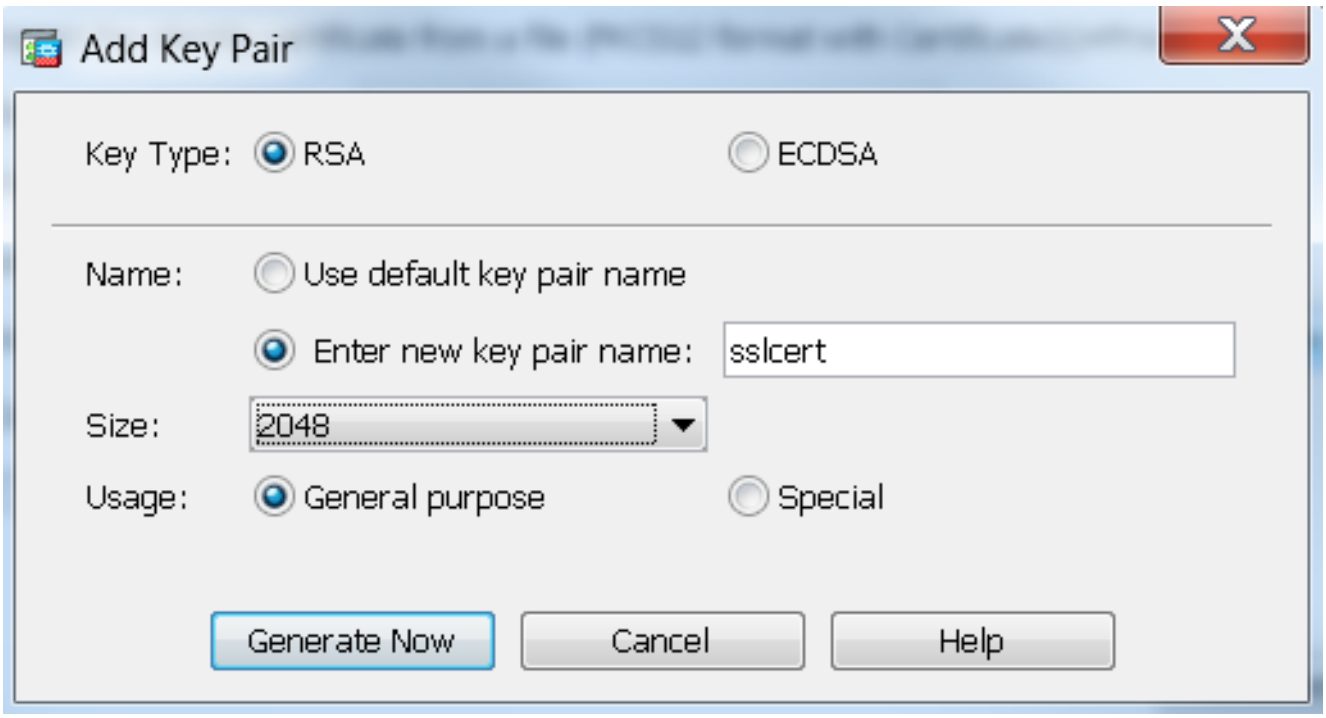
4. 单击**Add**:



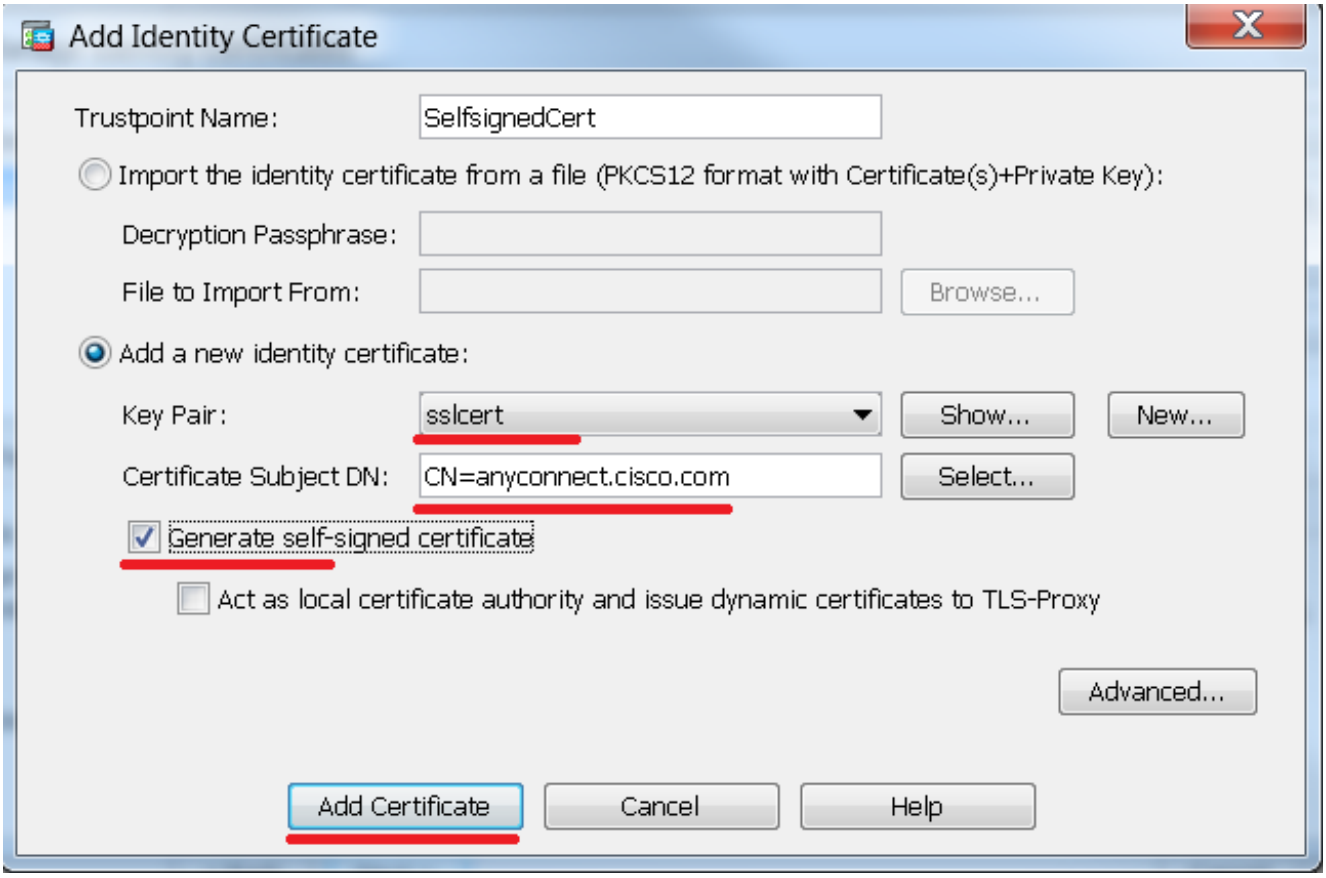
5. 在*信任点名称*字段中键入适当的名称，然后点击**添加新的身份证书**单选按钮。如果设备上不存在 Rivest-Shamir-Addleman (RSA) 密钥对，请点击**新建**来生成 RSA 密钥对：



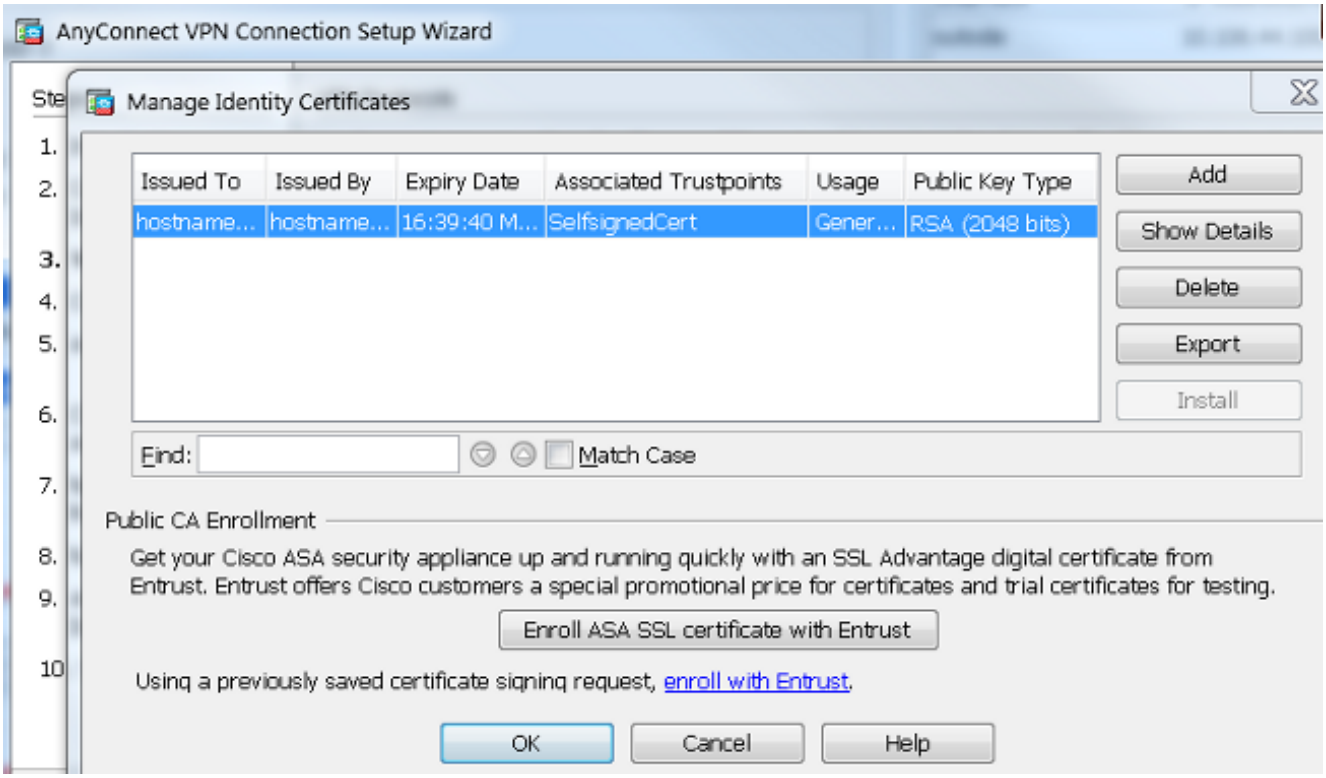
6. 单击“**Use default key pair name(使用默认密钥对名**称)”单选按钮，或单击“**Enter new key pair name(输入新密**钥对名称)”单选按钮并输入新名称。选择密钥的大小，然后单击“立即**生成”**:



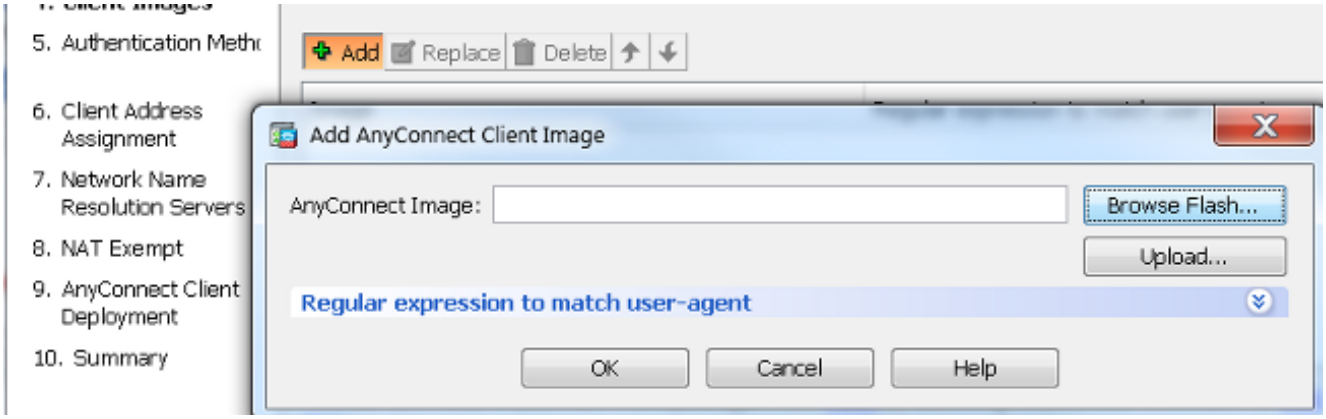
7. 在生成RSA密钥对后，选择密钥并选中生**成自签名证书复**选框。在*证书主题域名*字段中输入所需的主题域名 (DN)， 然后点击**添加证书**：

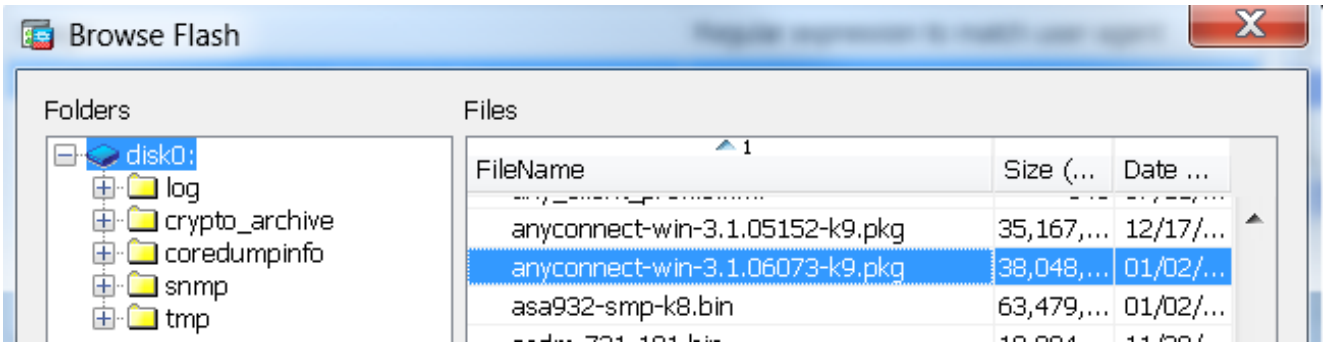


8. 完成注册后，单击**OK**、**OK**和**Next**:

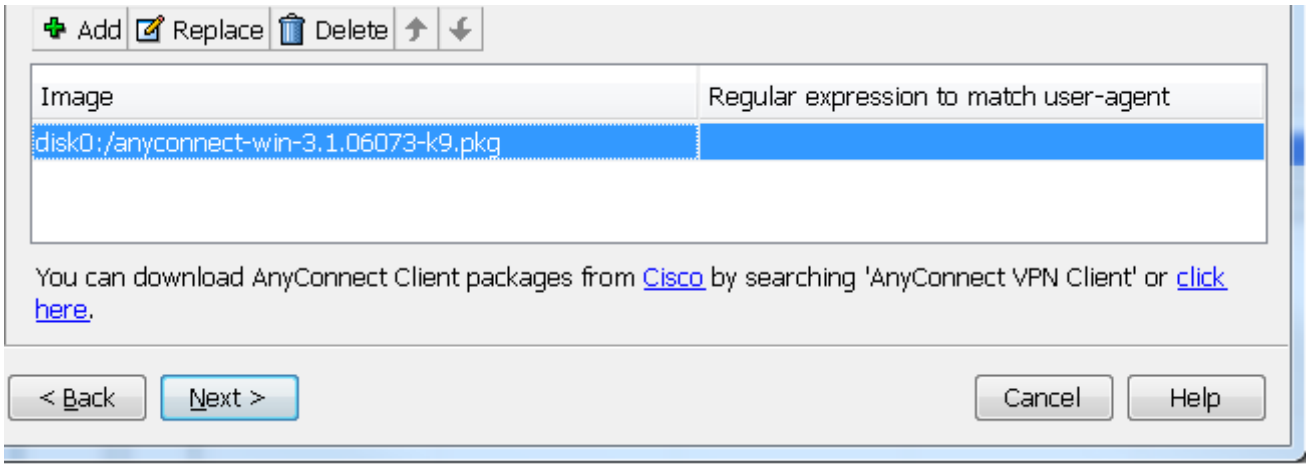


9. 单击**Add**以从PC或闪存中添加AnyConnect客户端映像(*.pkg*文件)。单击**Browse Flash**以从闪存驱动器添加映像，或单击**Upload**以直接从主机添加映像：

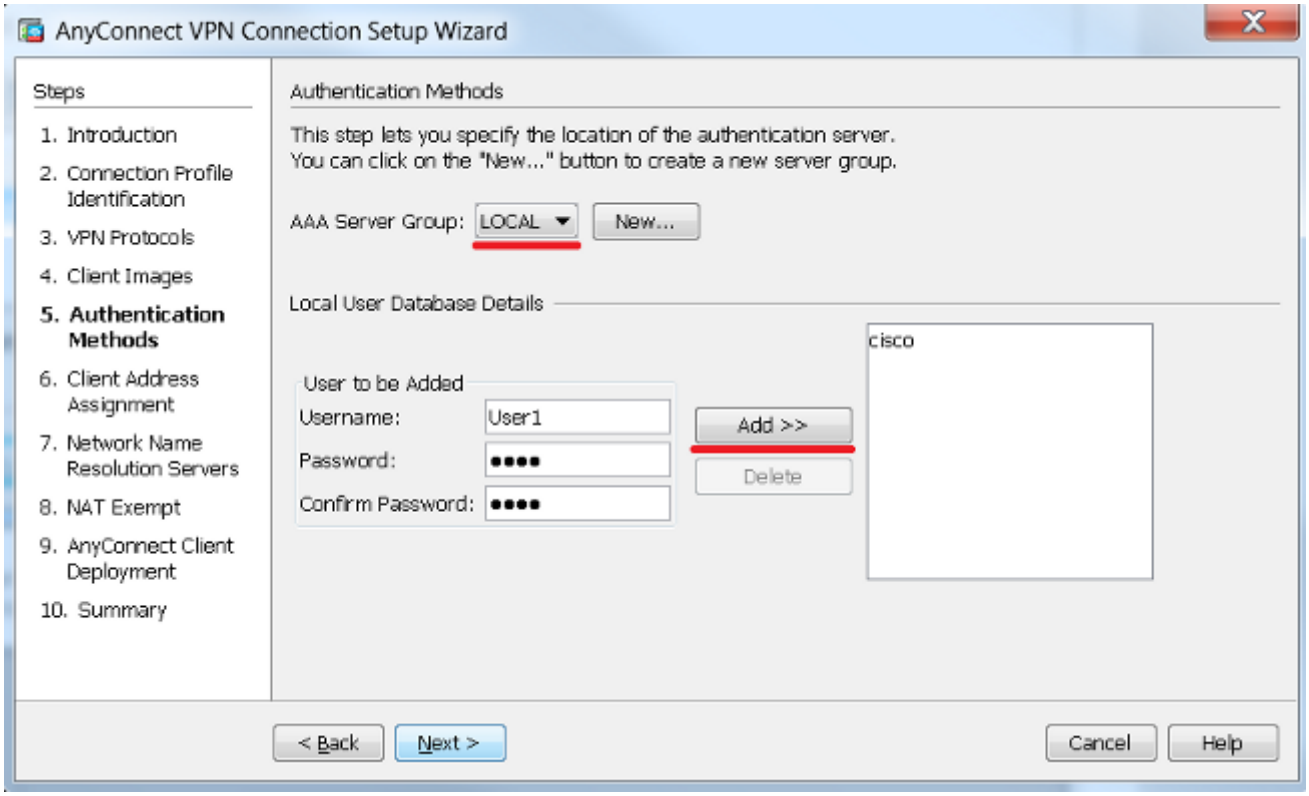




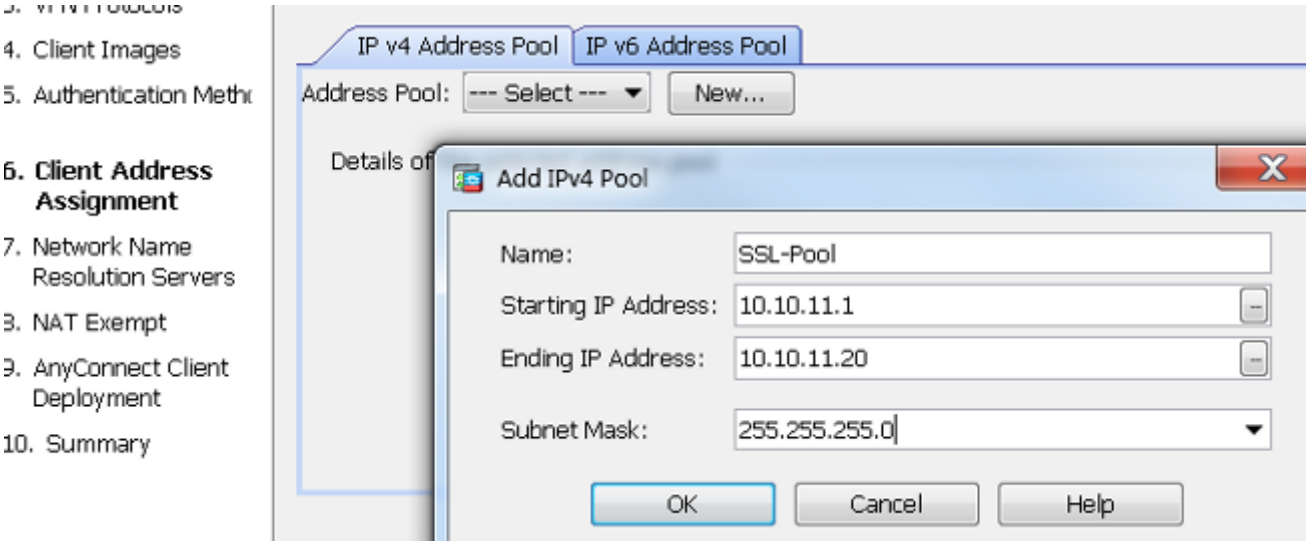
10. 添加映像后，单击“下一步”:



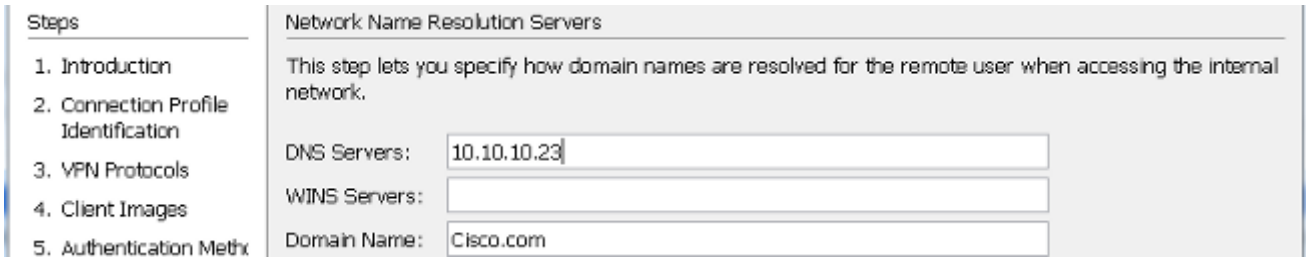
11. 用户身份验证可以通过身份验证、授权和记帐 (AAA) 服务器组完成。如果已配置用户，则选择 **LOCAL**，然后点击**下一步**。 **注意**：在本例中，配置了 **LOCAL** 身份验证，这意味着 ASA 上的本地用户数据库将用于身份验证。



12. 必须配置 VPN 客户端的地址池。如果已配置地址池，请从下拉菜单中选择。如果未配置地址池，请点击**新建**以配置新的地址池。完成后，单击**Next**:



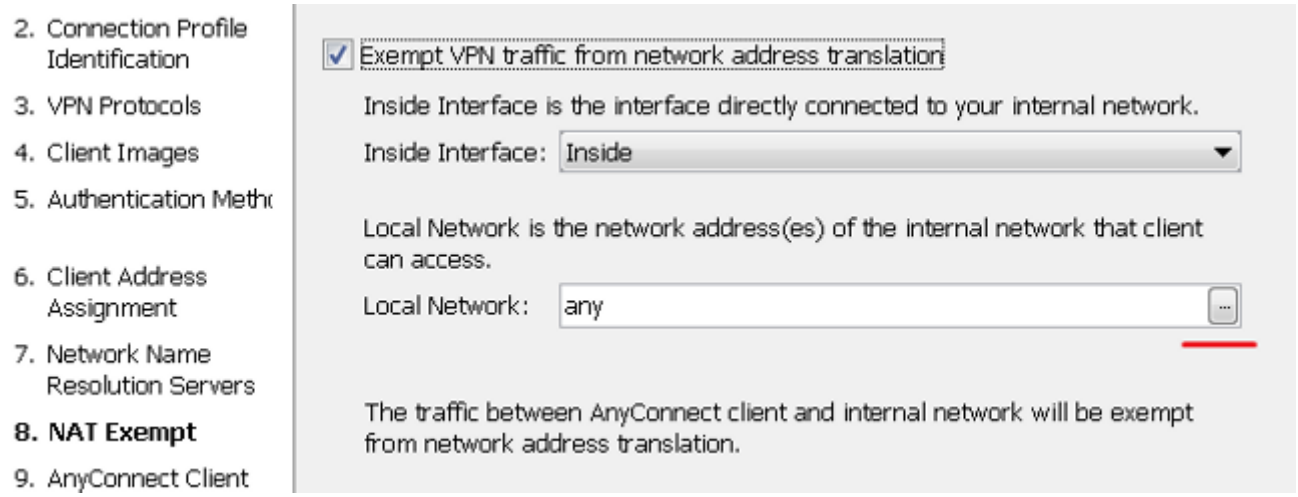
13. 在*域名系统*和*域名*字段中相应地输入域名系统 (DNS) 服务器和域名 (DN)，然后点击**下一步**：



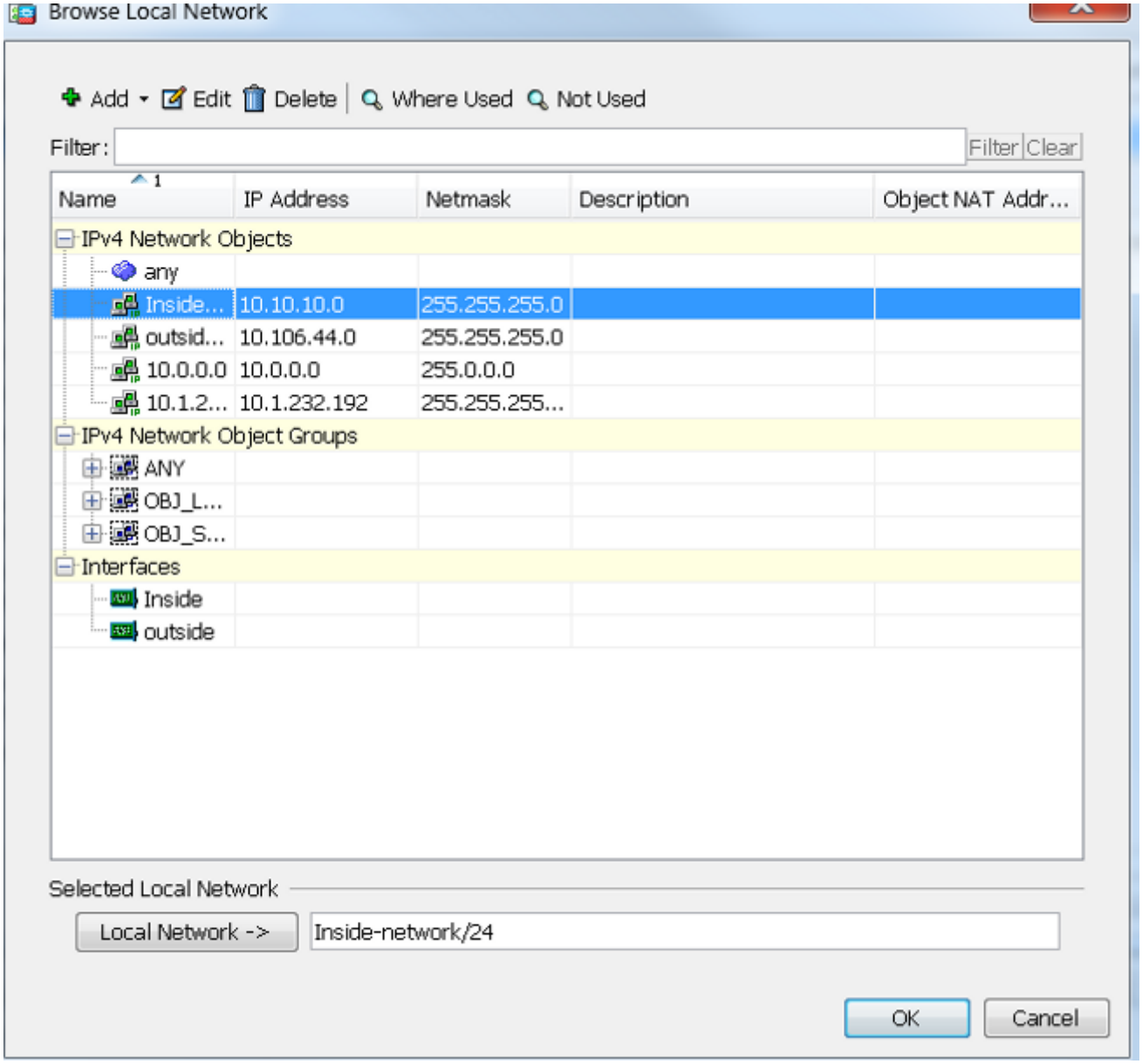
14. 在此场景中，目标是限制通过 VPN 访问配置为 ASA 后面的*内部*（或 LAN）子网的

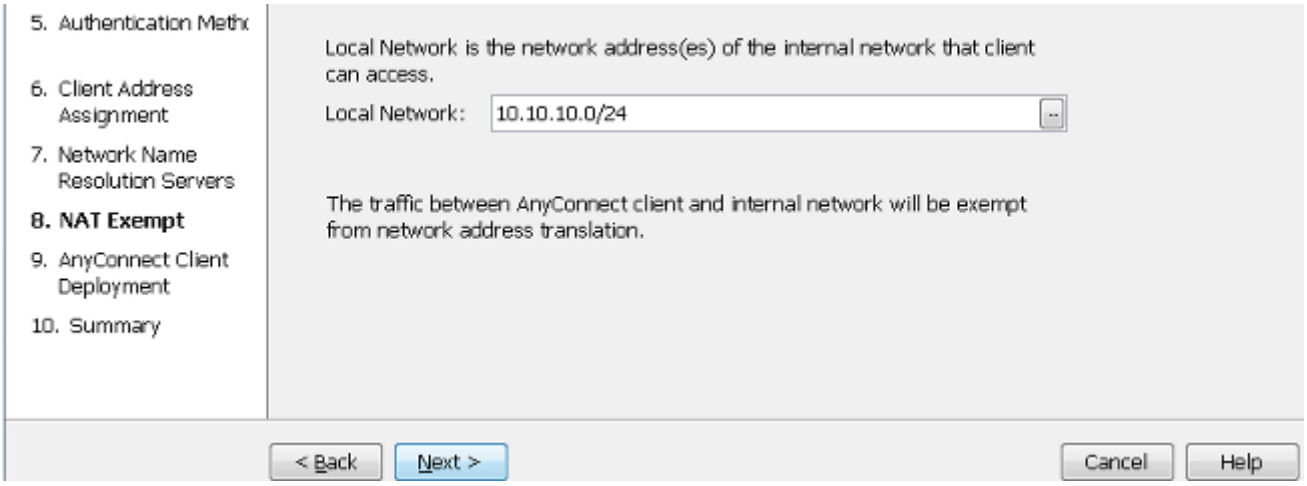
10.10.10.0/24 网络。客户端和内部子网之间的流量必须免除任何动态网络地址转换(NAT)。

选中**Exempt VPN traffic from network address translation**复选框，并配置将用于免除的LAN和WAN接口：



15. 选择必须免除的本地网络：





16. 单击**Next**、**Next**和**Finish**。

AnyConnect 客户端配置现已完成。但是，当您通过配置向导配置AnyConnect时，它会默认将拆分隧道*策略配*置为**隧道**策略。为了仅通过隧道传输特定流量，必须实施*拆分隧道*。

注意：如果未配置分割隧道，则分割隧道策略将从默认组策略(DfltGrpPolicy)继承，默认组策略设置为隧道**策略。**这意味着一旦客户端通过VPN连接，所有流量（包括到Web的流量）都

将通过隧道发送。

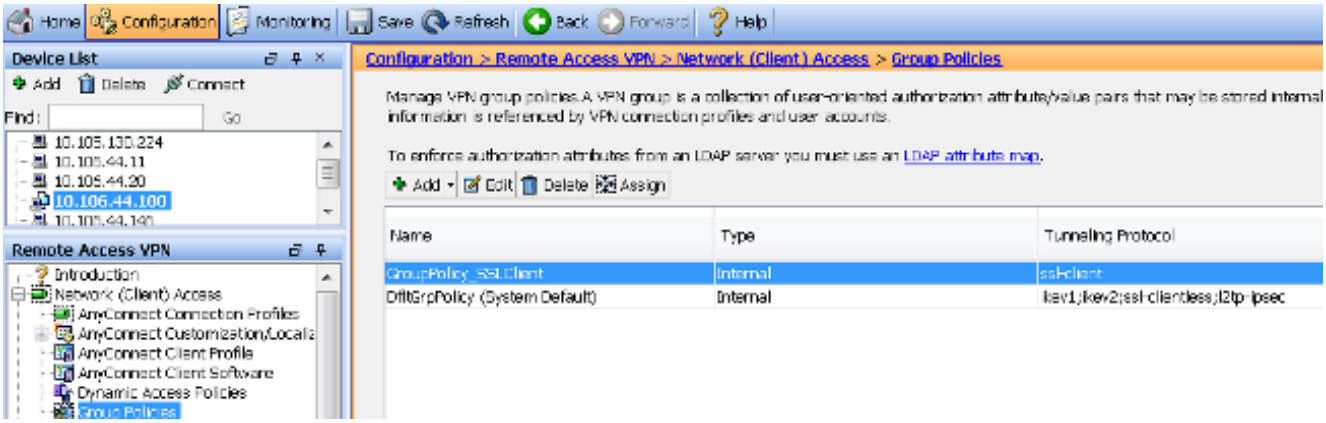
只有发往 ASA WAN（或*外部*）IP 地址的流量才会绕过客户端计算机上的隧道。在Microsoft Windows计算机上的**route print**命令输出中可以看到这一点。

拆分隧道配置

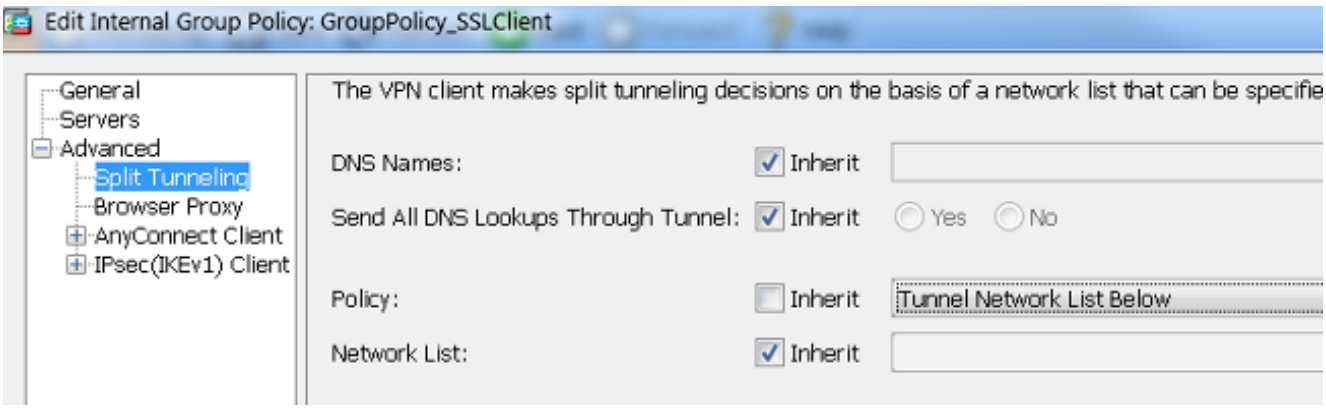
分割隧道功能可用于定义必须加密的子网或主机的流量。这包括配置将与此功能关联的访问控制列表(ACL)。此 ACL 中定义的子网或主机的流量将从客户端通过隧道进行加密，并且这些子网的路由安装在 PC 路由表中。

完成以下步骤，以从*全隧道*配置更改为*拆分隧道*配置：

1. 导航到**配置 > 远程接入 VPN > 组策略**：

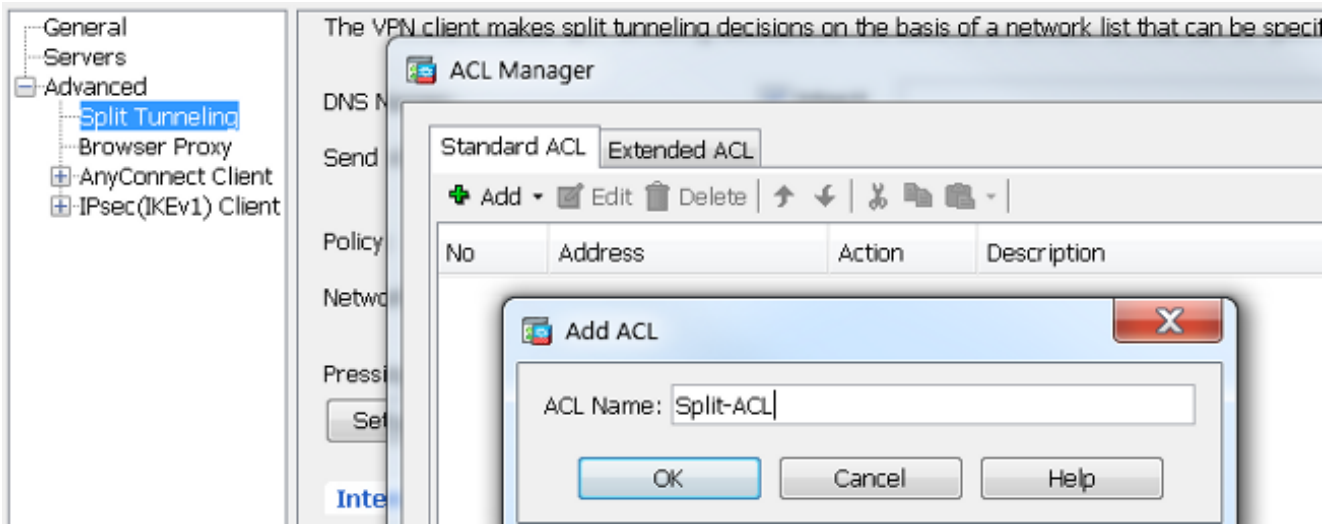


2. 单击**Edit**，然后使用导航树导航到Advanced > Split Tunneling。取消选中**Inherit**复选框*Policy*部分，然后从下拉菜单中选择**Tunnel Network List Below**:

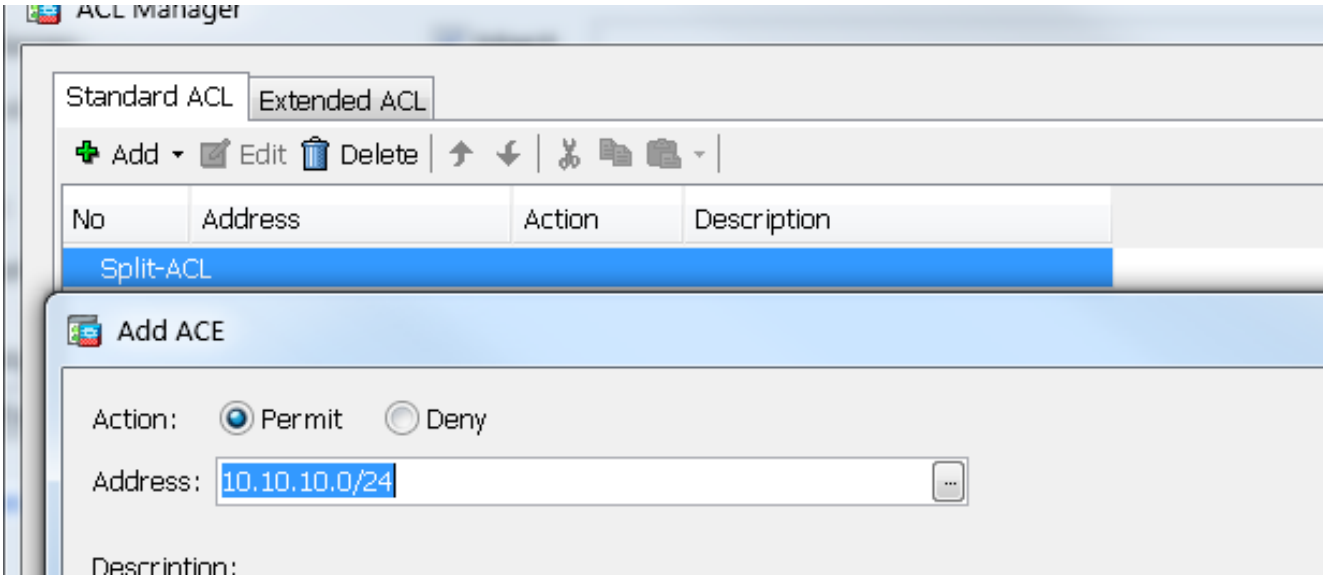


3. 取消选中*网络列表*部分中的**继承**复选框，然后单击*管理*以选择指定客户端需要访问的LAN网络的ACL:

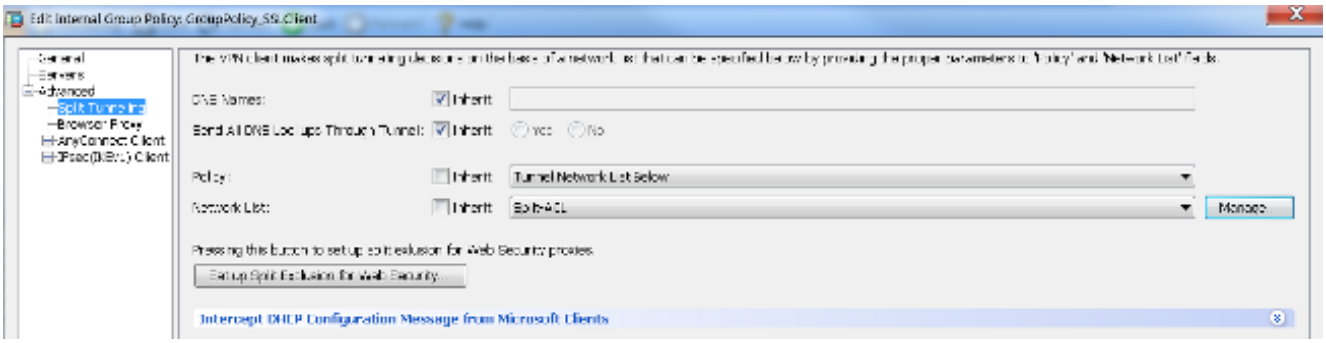
4. 依次点击**标准 ACL**、**添加**、**添加 ACL**，然后点击 **ACL 名称**：



5. 单击**Add ACE** 以添加规则：



6. Click **OK**.



7. 单击 **Apply**。

连接后，拆分 ACL 中的子网或主机路由会添加到客户端计算机的路由表中。在 Microsoft Windows 计算机上，这可以在 **route print** 命令的输出中查看。这些路由的下一跳将是来自客户端 IP 池子网的 IP 地址（通常是该子网的第一个 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 计算机上，输入 **netstat -r** 命令来查看 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.
```

下载并安装 AnyConnect 客户端

在用户计算机上部署Cisco AnyConnect安全移动客户端时，可以使用两种方法：

- 网络部署
- 独立式部署

以下各节将更详细地介绍这两种方法。

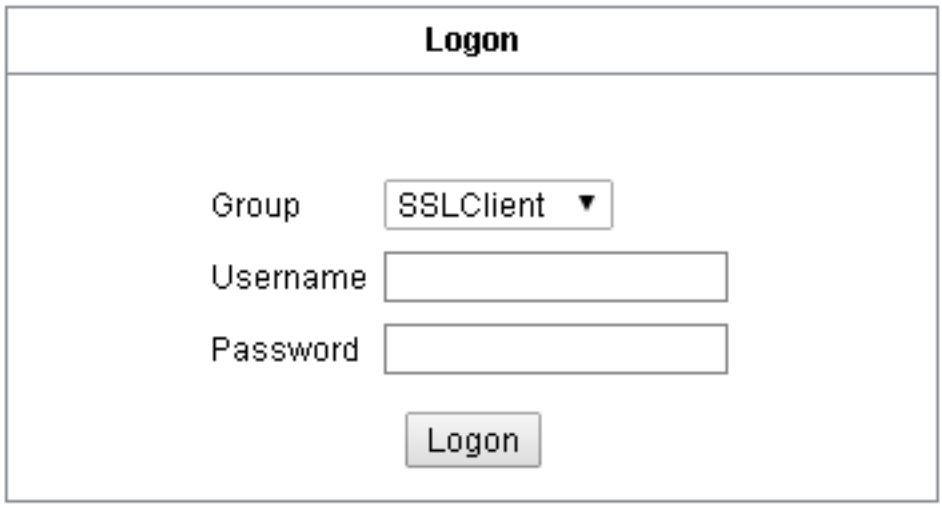
网络部署

要使用Web部署方法，请在客户机的浏览器中输入**https://<ASA's FQDN>或<ASA's IP>** URL，从而进入*WebVPN*门户页。

> **注意**：如果使用 Internet Explorer (IE) 浏览器，安装主要通过 ActiveX 完成，除非您被迫使用 Java。所有其他浏览器都使用 Java。

登录该页面后，应该会在客户端计算机上开始安装，并且客户端应在安装完成后连接到 ASA。

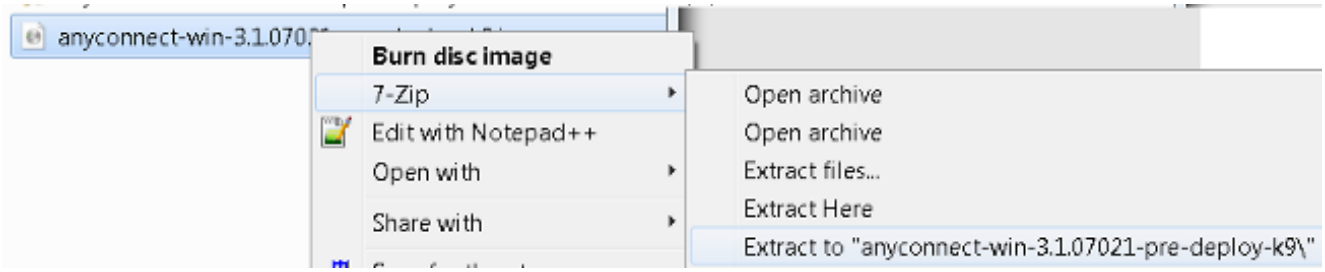
> **注意**：系统可能会提示您授予运行 ActiveX 或 Java 的权限。必须允许此操作才能继续安装。



独立部署

完成以下步骤，以使用独立部署方法：

1. 从思科网站下载 AnyConnect 客户端映像。要选择正确的映像进行下载，请参阅 Cisco AnyConnect Secure Mobility Client 网页。此页上提供了下载链接。请导航到下载页并选择相应的版本。搜索完**整安装包 — 窗口/独立安装程序(ISO)。 注意：**然后下载ISO安装程序映像(*例如anyconnect-win-3.1.06073-pre-deploy-k9.iso*)。
2. 使用 *WinRar* 或 *7-Zip* 提取 ISO 软件包的内容：



3. 提取内容后，运行 **Setup.exe** 文件并选择必须与 Cisco AnyConnect Secure Mobility Client 一起安装的模块。

   提示：要配置 VPN 的其他设置，请参阅《使用 CLI 的 Cisco ASA 5500 系列配置指南，8.4 和 8.6》的配置 AnyConnect VPN 客户端连接一节。

CLI 配置

本节介绍 Cisco AnyConnect Secure Mobility Client 的 CLI 配置，以供参考。

```
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
```

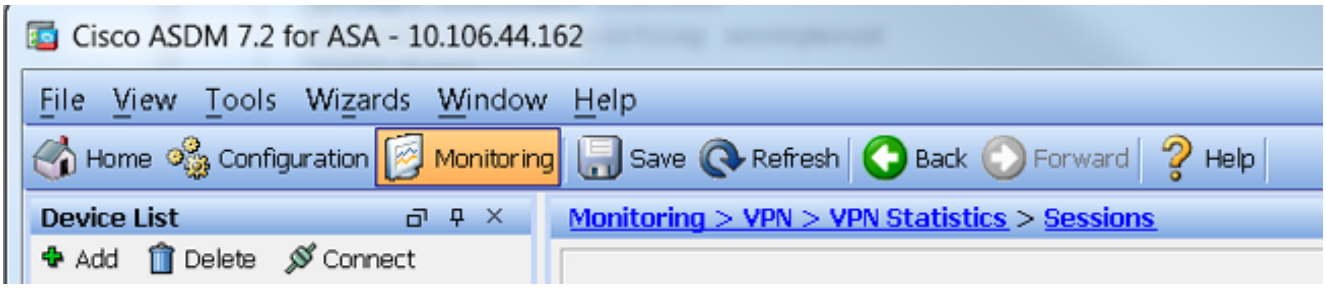
```
!************** NAT exemption Configuration *****************
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.

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
```

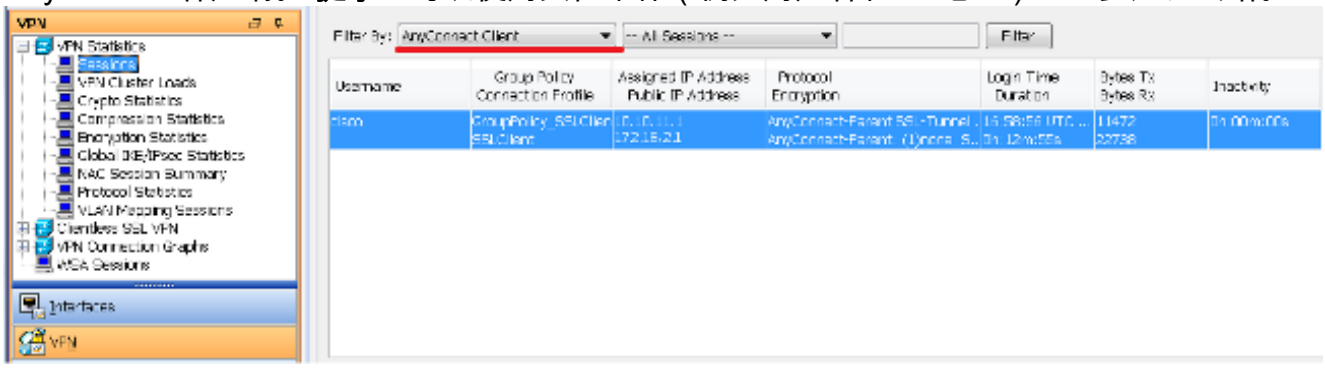
验证

完成以下步骤以验证客户端连接和与该连接关联的各种参数：

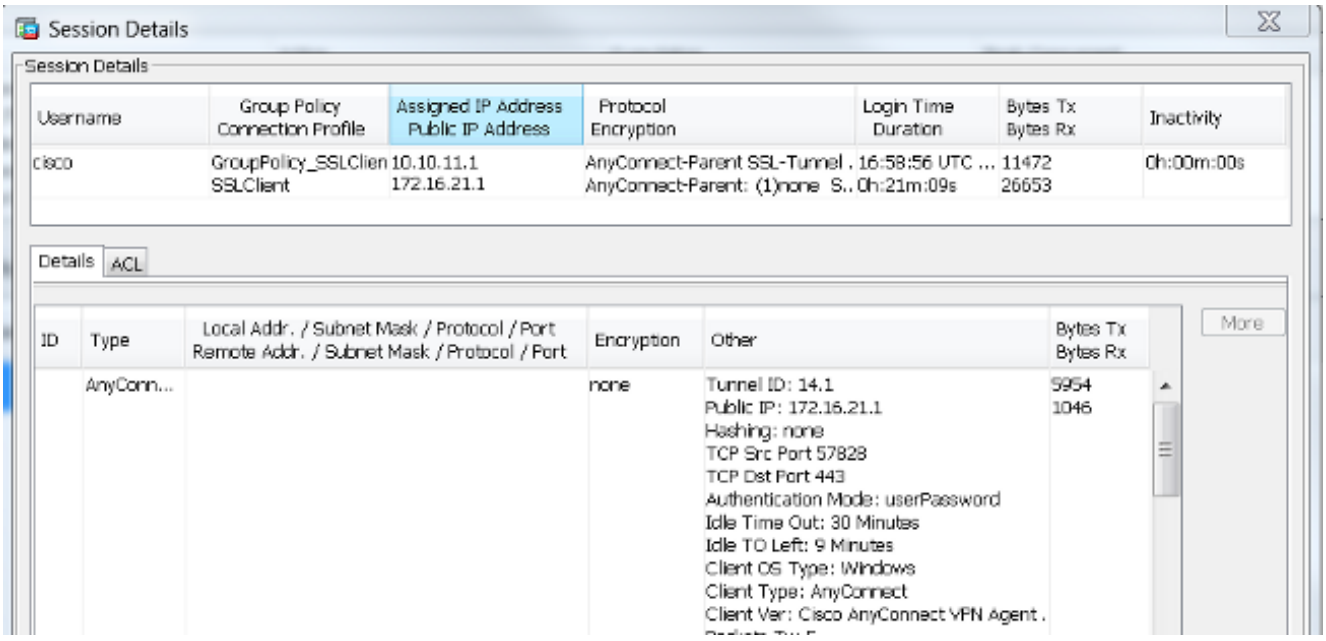
1. 在 ASDM 上导航到**监控 > VPN**：



2. 可以使用**Filter By** 选项来过滤VPN的类型。从下拉**菜单和所**有AnyConnect客户端会话中选择AnyConnect客户端。 **提示：**可以使用其他条件（例如*用户名*和 *IP 地址*）进一步过滤会话。



3. 双击某个会话以获取有关该特定会话的更多详细信息：



4. 在 CLI 中输入 **show vpn-sessiondb anyconnect** 命令以获取会话详细信息：

```
# 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. 您可以使用其他过滤器选项来优化结果：

```
# 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
```

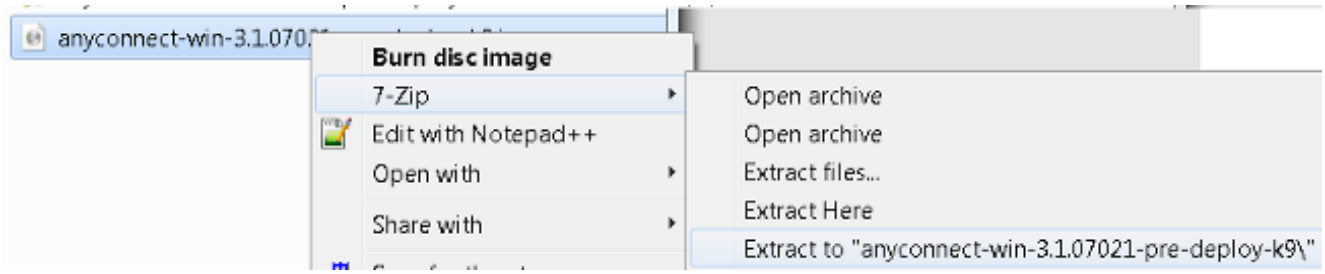
故障排除

您可以使用 AnyConnect 诊断和报告工具 (DART)，来收集有助于排除 AnyConnect 安装和连接问题的数据。在运行 AnyConnect 的计算机上使用 DART 向导。DART 可以收集日志、状态和诊断信息供思科技术支持中心 (TAC) 执行分析，并且不需要管理员权限即可在客户端计算机上运行。

安装 DART

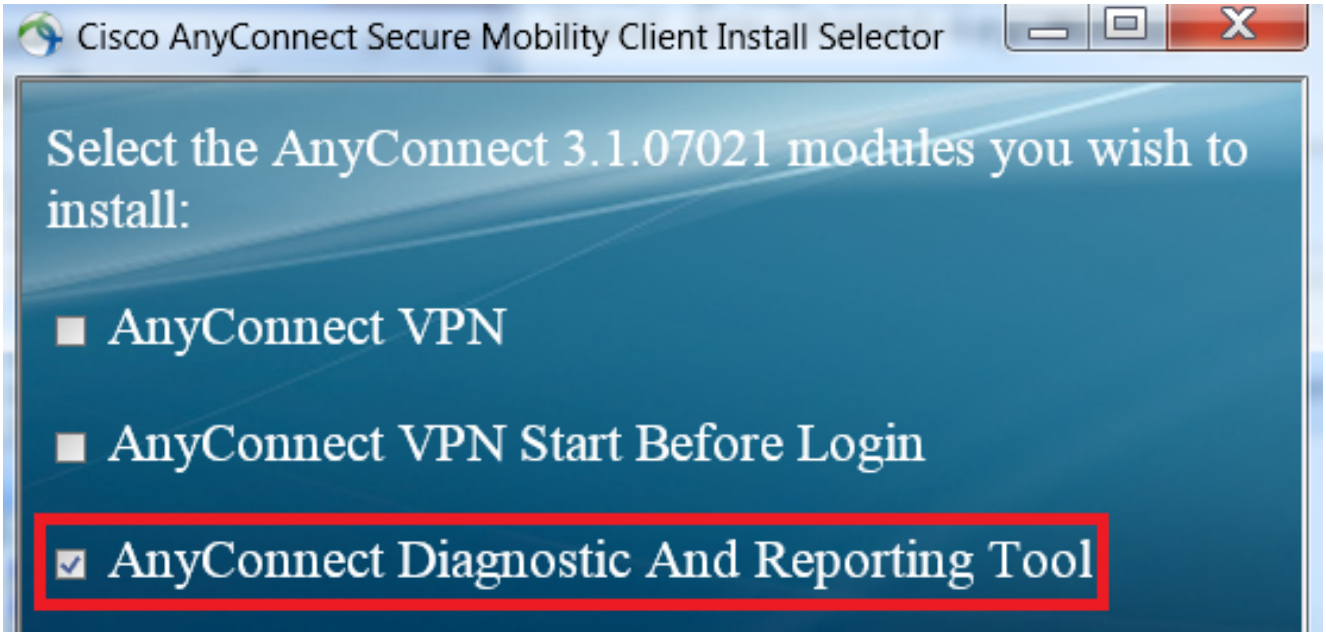
完成以下步骤，以安装 DART：

1. 从思科网站下载 AnyConnect 客户端映像。要选择正确的映像进行下载，请参阅 Cisco AnyConnect Secure Mobility Client 网页。此页上提供了下载链接。请导航到下载页并选择相应的版本。搜索完**整安装包 — 窗口/独立安装程序(ISO)。 注意：**然后下载ISO安装程序映像 (*例如anyconnect-win-3.1.06073-pre-deploy-k9.iso*)。
2. 使用 *WinRar* 或 *7-Zip* 提取 ISO 软件包的内容：



3. 浏览到内容提取到的文件夹。

4. 运行 **Setup.exe** 文件并且仅选择 **Anyconnect 诊断和报告工具**：

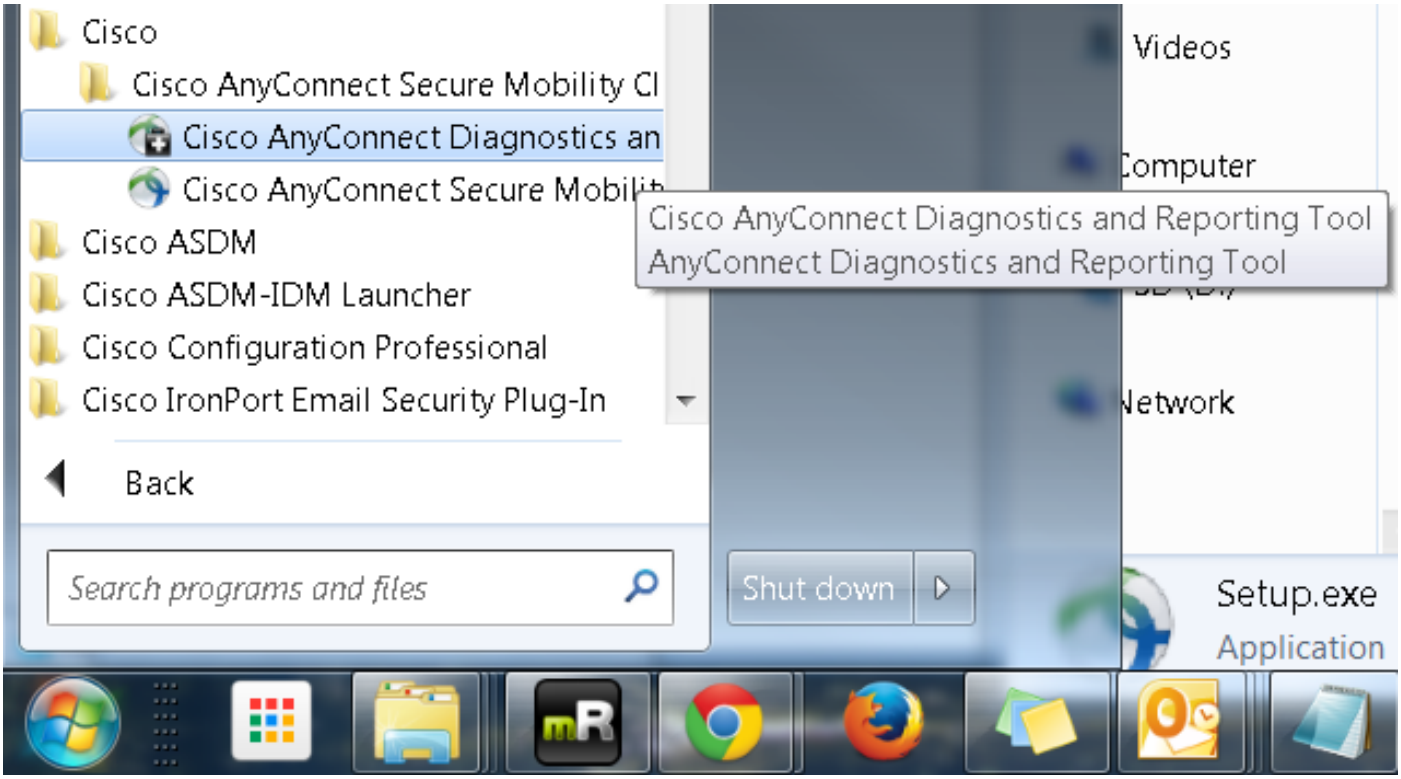


运行 DART

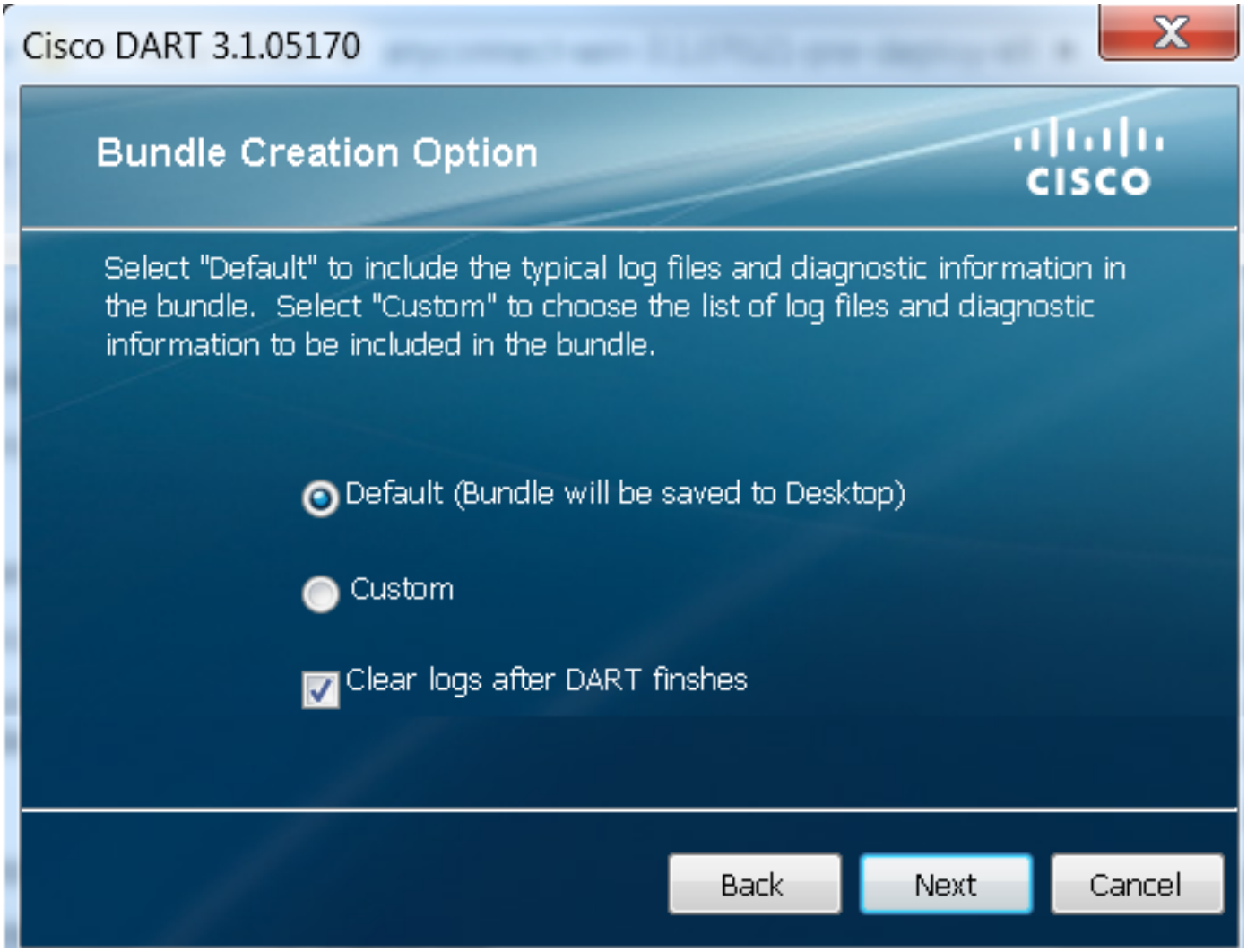
以下是运行 DART 之前需要考虑的一些重要信息：

- 在运行DART之前，必须至少重新创建一次问题。
- 重新创建问题时，必须记录用户计算机上的日期和时间。

从客户端上的“开*始*”菜单运行DART:



可以*选择*“*默认*”或“自定义”模式。思科建议您在“默认”模式下运行 DART，以便一次捕获所有信息。



完成后，该工具会将 DART 捆绑包 *.zip* 文件保存到客户端桌面。然后，可以通过电邮将捆绑包发送至TAC（在您提交TAC案例后），以便进一步分析。

相关信息

- AnyConnect VPN 客户端故障排除指南 - 常见问题
- AnyConnect、CSD/Hostscan 和 WebVPN 的 Java 7 问题 - 故障排除指南
- 技术支持和文档 - Cisco Systems

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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