Configuración de AnyConnect Secure Mobility Client con túneles divididos en ASA

Contenido

Introducción

Este documento describe cómo configurar Cisco AnyConnect Secure Mobility Client a través de Cisco Adaptive Security Device Manager (ASDM) en Cisco Adaptive Security Appliance (ASA) que ejecuta la versión de software 9.3(2).

Prerequisites

Requirements

El paquete de implementación web de Cisco AnyConnect Secure Mobility Client debe descargarse en el escritorio local donde está presente el acceso de ASDM a ASA. Para descargar el paquete del cliente, consulte la página web de Cisco AnyConnect Secure Mobility Client. Los paquetes de implementación web para diversos sistemas operativos (SO) se pueden cargar en ASA al mismo tiempo.

Estos son los nombres de archivo de implementación web para los diversos SO:

- **SO Microsoft Windows**: *AnyConnect-win-<version>-k9.pkg*

- **SO Macintosh (MAC)**: *AnyConnect-macosx-i386-<version>-k9.pkg*
- **SO Linux**: *AnyConnect-linux-<version>-k9.pkg*

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

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, make sure that you understand the potential impact of any command.

Antecedentes

Este documento proporciona detalles paso a paso sobre cómo utilizar el asistente de configuración de Cisco AnyConnect mediante ASDM para configurar AnyConnect Client y habilitar el túnel dividido.

El túnel dividido se utiliza en situaciones en las que solo se debe tunelizar tráfico específico, en lugar de situaciones en las que todo el tráfico generado por la máquina del cliente fluye a través de la VPN cuando se conecta. El uso del asistente de configuración de AnyConnect generará de manera predeterminada una configuración de *túnel completo* en ASA. El túnel dividido debe configurarse por separado, como se explica con más detalle en la sección de este documento.

En este ejemplo de configuración, la intención es enviar tráfico para la subred 10.10.10.0/24, que es la subred de la LAN detrás de ASA, a través del túnel VPN; todo el resto del tráfico de la máquina del cliente se reenvía a través de su propio circuito de Internet.

Información sobre la licencia de AnyConnect

Estos son algunos enlaces a información útil sobre las licencias de Cisco AnyConnect Secure Mobility Client:

- Consulte el documento Características, licencias y SO de AnyConnect Secure Mobility Client, versión 3.1 para determinar las licencias necesarias para AnyConnect Secure Mobility Client y las características relacionadas.
- Consulte la Guía de pedidos de Cisco AnyConnect para obtener información sobre las licencias de AnyConnect Apex y Plus.
- Consulte el documento ¿Qué licencia de ASA se necesita para las conexiones de telefonía IP y VPN móvil? para obtener información sobre los requisitos de licencia adicionales para las

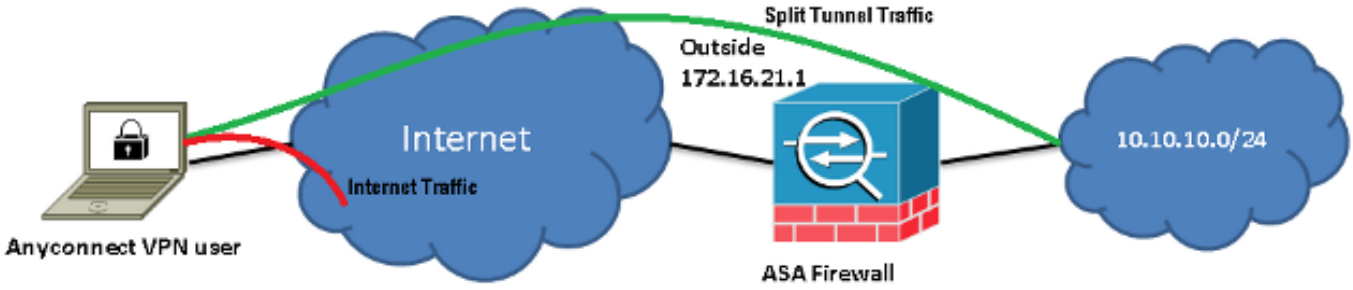
conexiones de telefonía IP y móviles.

Configurar

En esta sección se describe cómo configurar Cisco AnyConnect Secure Mobility Client en ASA.

Diagrama de la red

Esta es la topología que se usa para los ejemplos en este documento:

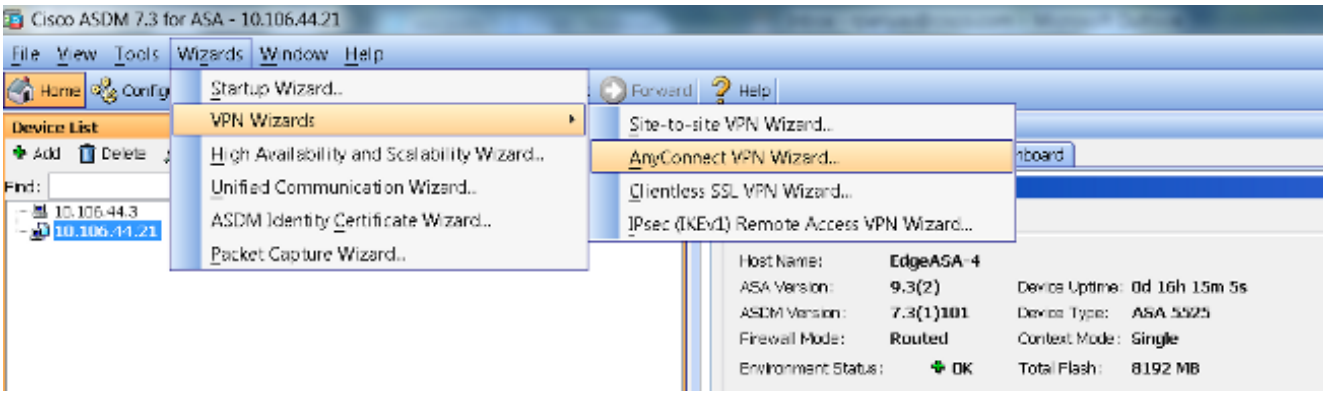


Asistente de configuración de ASDM de AnyConnect

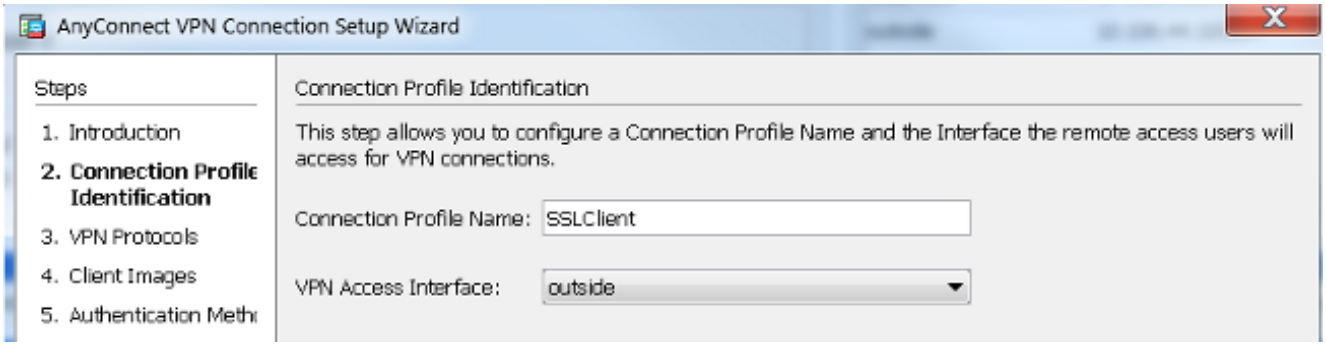
El asistente de configuración de AnyConnect se puede utilizar para configurar AnyConnect Secure Mobility Client. Asegúrese de que se haya cargado un paquete de AnyConnect Client en la memoria flash o el disco del firewall de ASA antes de continuar.

Complete estos pasos para configurar AnyConnect Secure Mobility Client mediante el asistente de configuración:

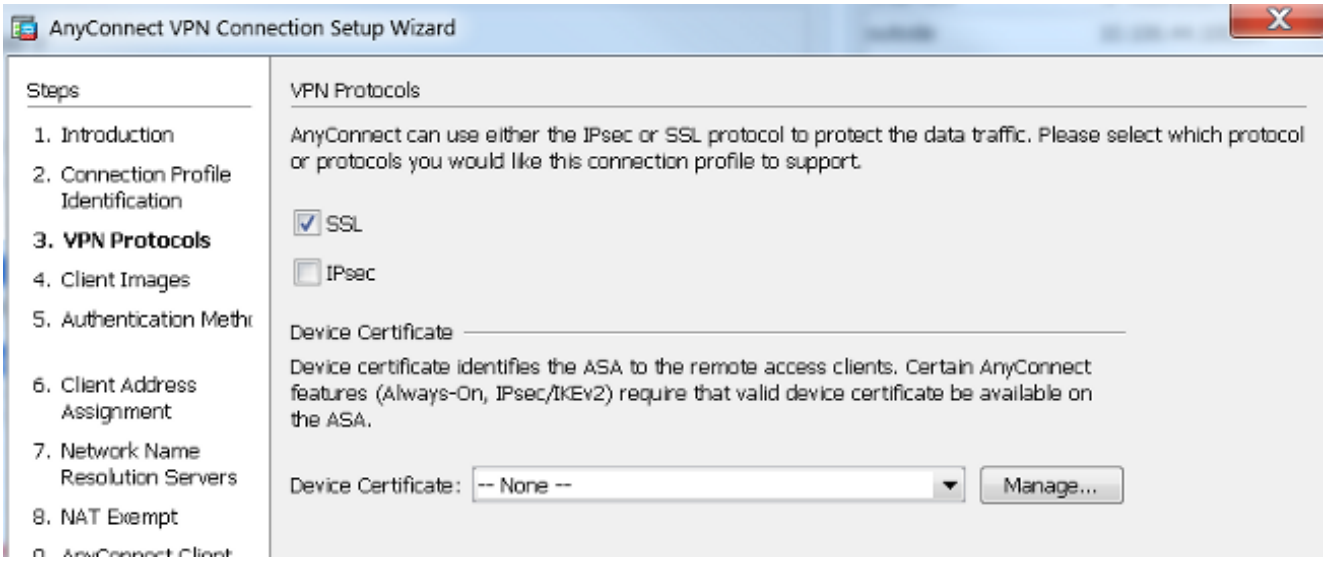
1. Inicie sesión en ASDM, inicie el **Asistente de configuración** y haga clic en **Siguiente**:



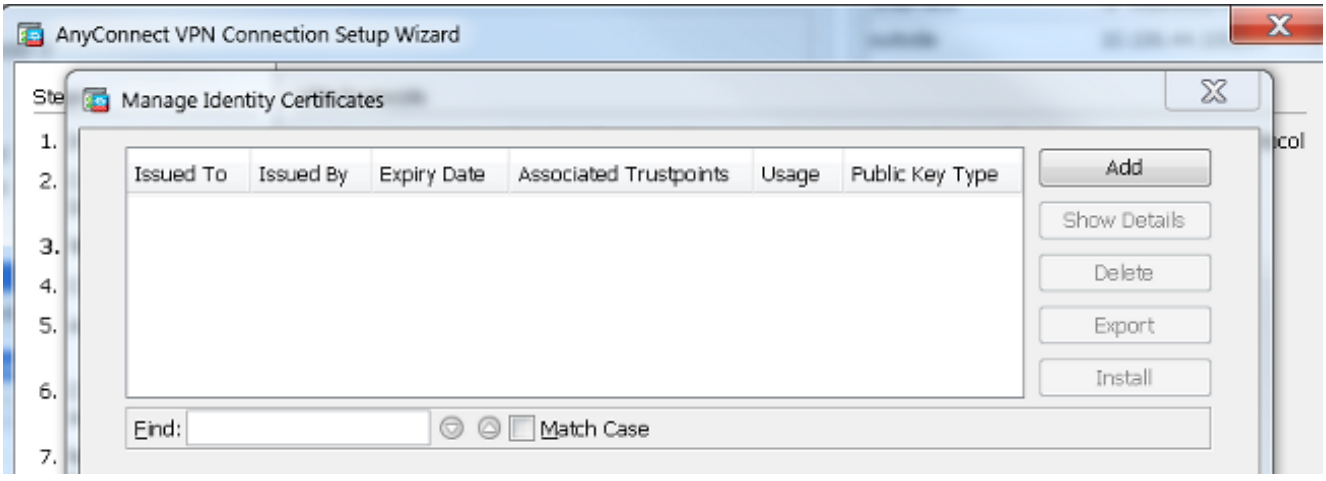
2. Ingrese el *nombre del perfil de conexión*, elija la interfaz en la que finalizará la VPN en el menú desplegable *Interfaz de acceso a la VPN* y haga clic en **Siguiente**:



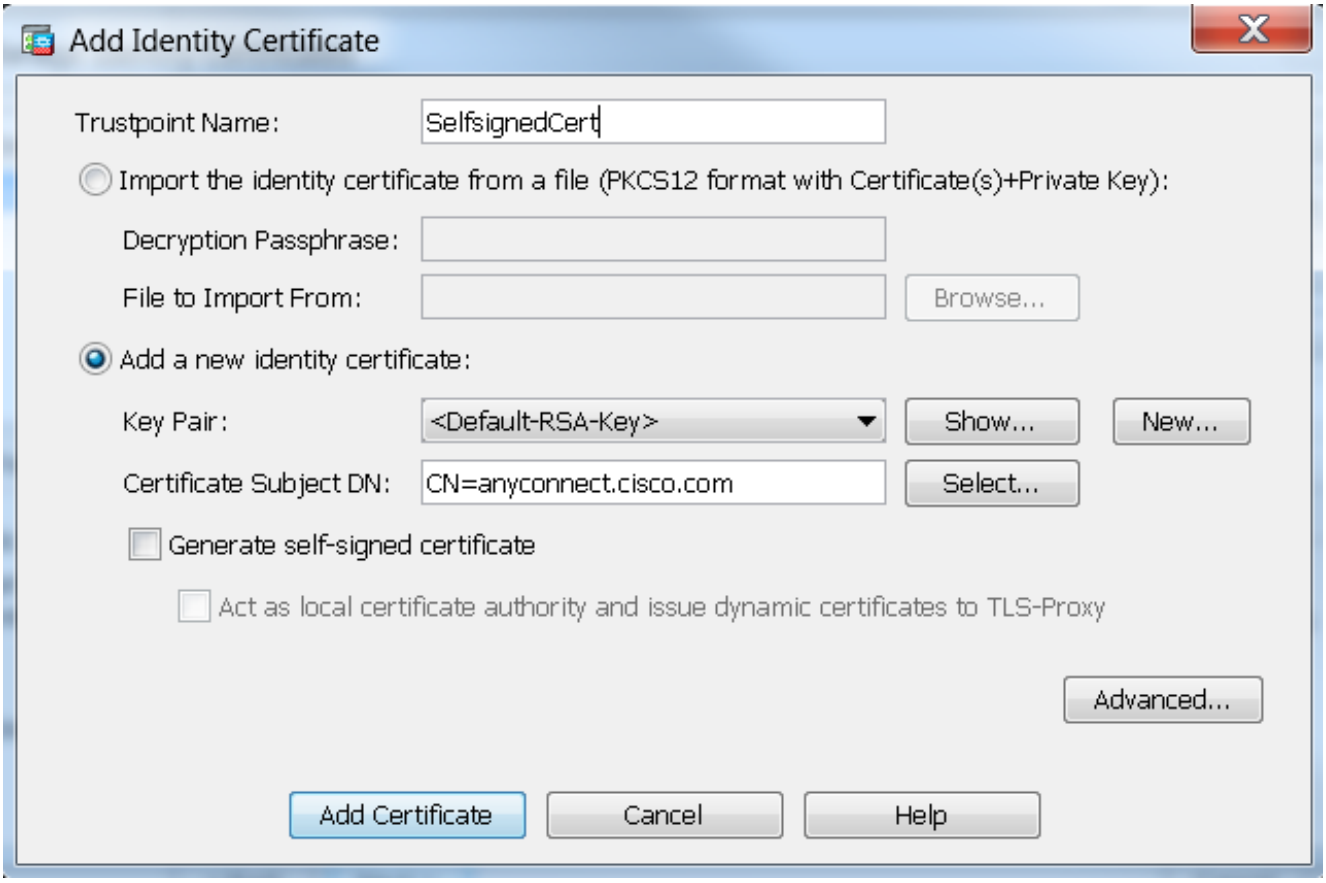
3. Marque la casilla de verificación **SSL** para habilitar la capa de sockets seguros (SSL). El *certificado del dispositivo* puede ser un certificado emitido por una autoridad de certificación (CA) de confianza (como Verisign o Entrust) o un certificado firmado automáticamente. Si el certificado ya está instalado en ASA, se puede elegir en el menú desplegable. **Nota:** Este certificado es el certificado del servidor que se proporcionará. Si no hay ningún certificado instalado actualmente en ASA y se debe generar un certificado firmado automáticamente, haga clic en **Administrar**.Para instalar un certificado de terceros, siga los pasos que se describen en el documento [Certificados de proveedores de terceros para la instalación manual de ASA 8.x para usar con el ejemplo de configuración de WebVPN](#) de Cisco.



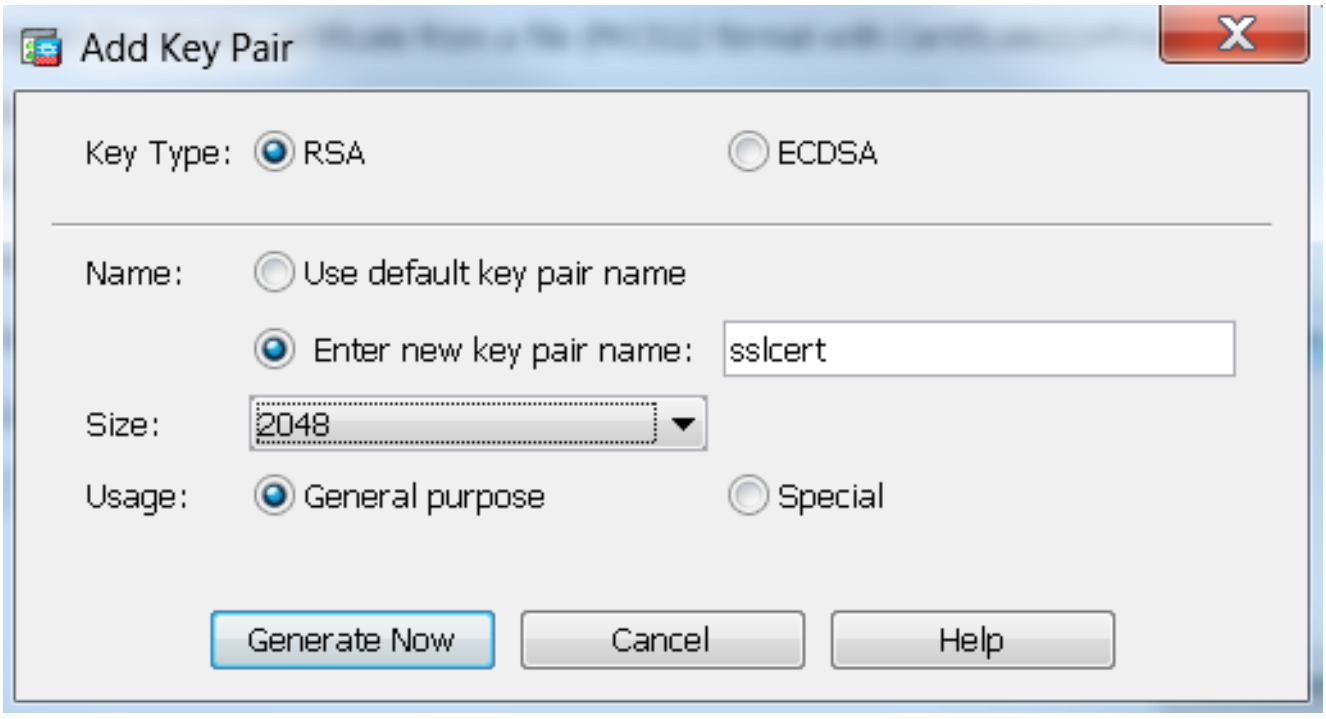
4. Haga clic en **Agregar**:



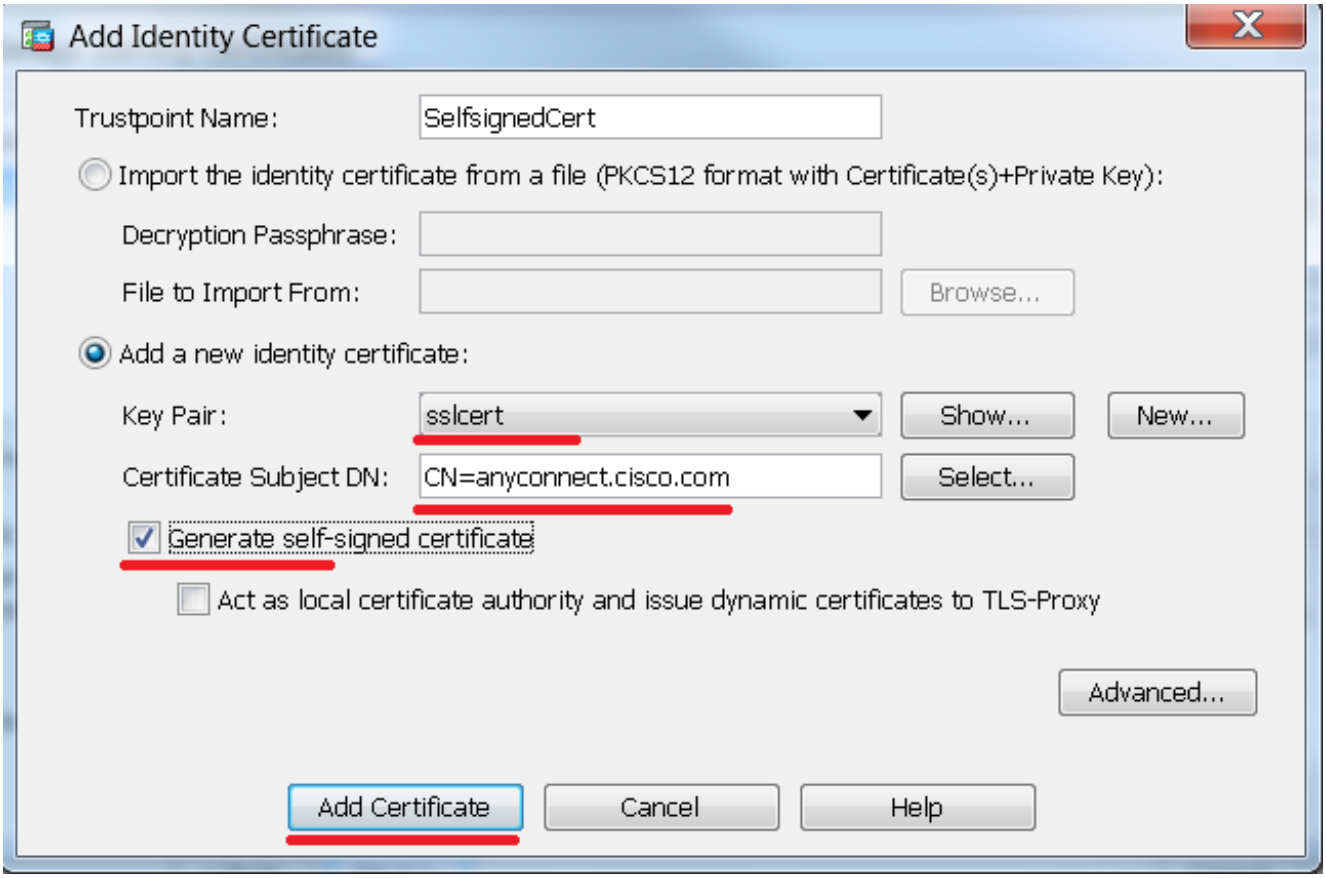
5. Escriba un nombre adecuado en el campo *Nombre del punto de confianza* y haga clic en el botón de radio **Agregar un nuevo certificado de identidad**. Si no hay pares de claves Rivest-Shamir-Addleman (RSA) presentes en el dispositivo, haga clic en **Nuevo** para generar uno:



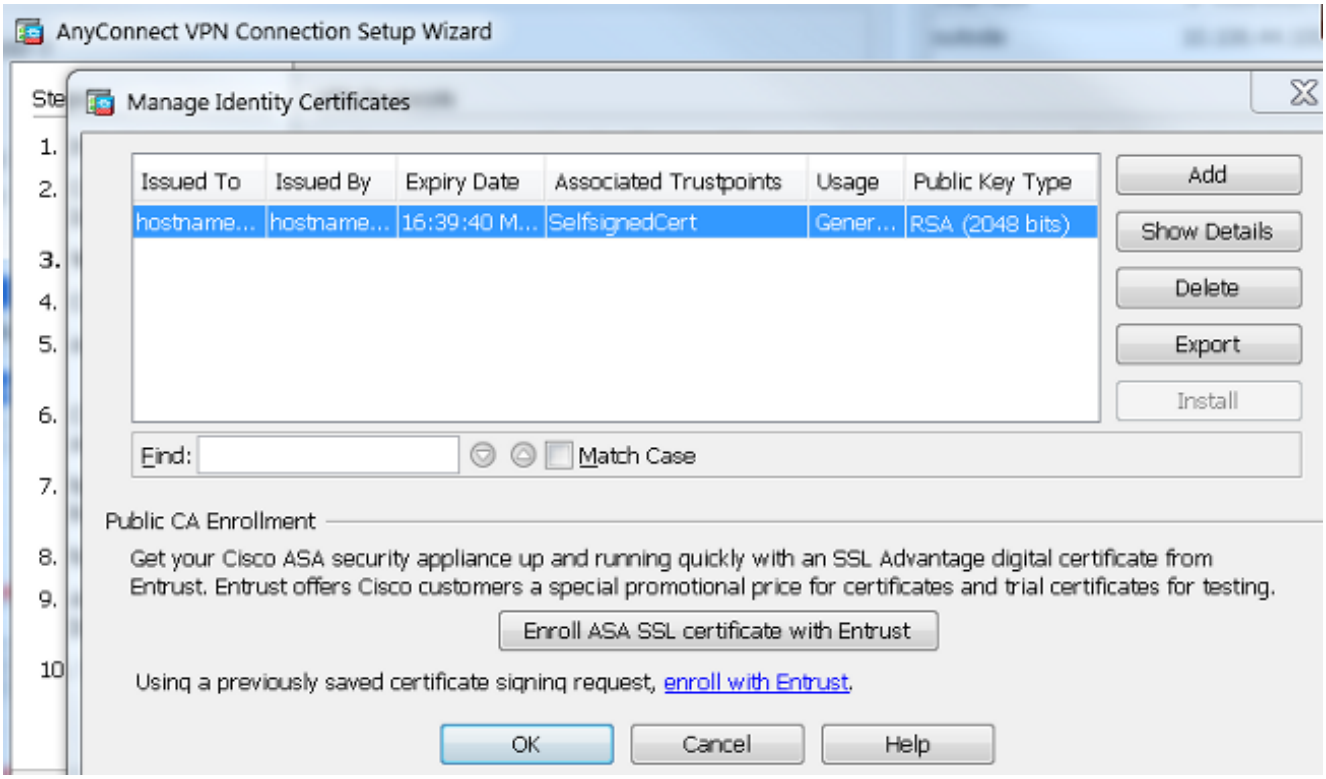
6. Haga clic en el botón de radio **Usar nombre de par de claves predeterminado** o haga clic en el botón de radio **Introducir nuevo nombre de par de claves** e introduzca un nuevo nombre. Seleccione el tamaño de las claves y haga clic en **Generar ahora**:



7. Después de generar el par de claves RSA, elija la clave y marque la casilla de verificación **Generar certificado firmado automáticamente**. Ingrese el nombre de dominio (DN) del asunto deseado en el campo *DN del asunto del certificado* y, luego, haga clic en **Agregar certificado**:

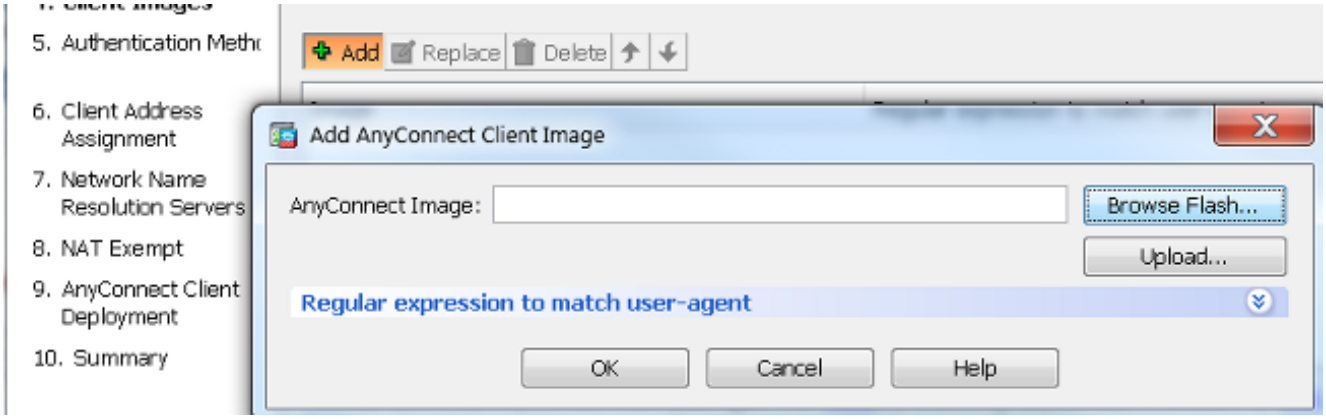


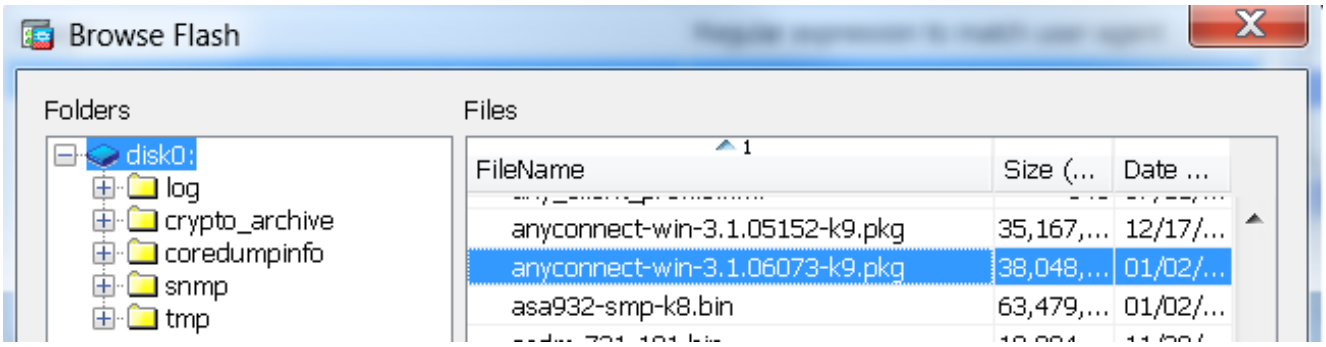
8. Una vez completada la inscripción, haga clic en **Aceptar**, **Aceptar** y, luego, en **Siguiente**:



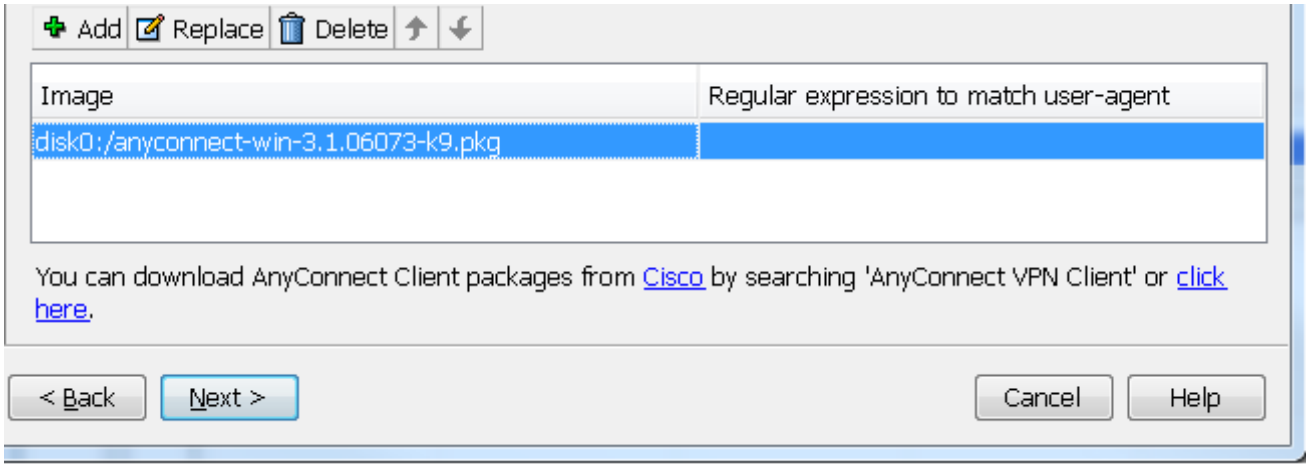
9. Haga clic en **Agregar** para agregar la imagen de AnyConnect Client (archivo *.pkg)* desde la

PC o la memoria flash. Haga clic en **Examinar la memoria flash** para agregar la imagen de la unidad de memoria flash o haga clic en **Cargar** para agregar la imagen de la máquina host directamente:

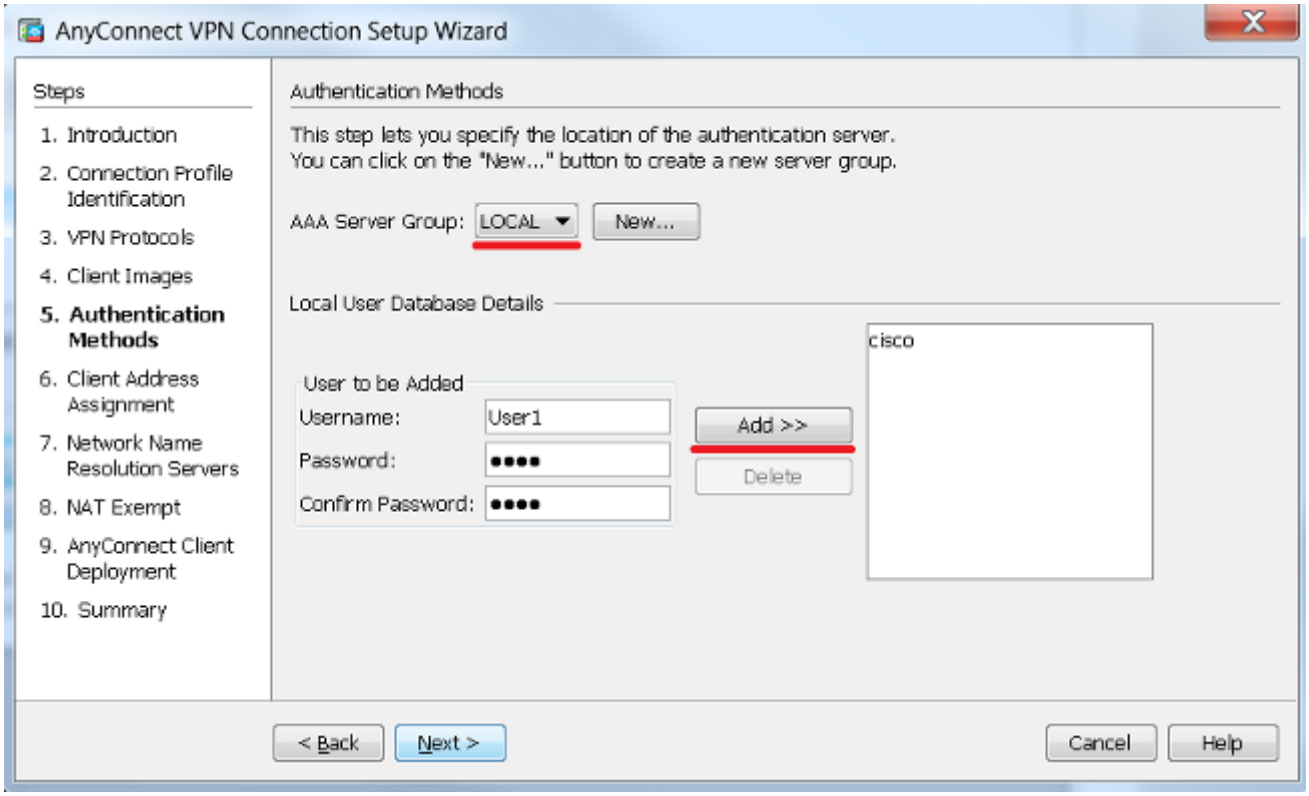




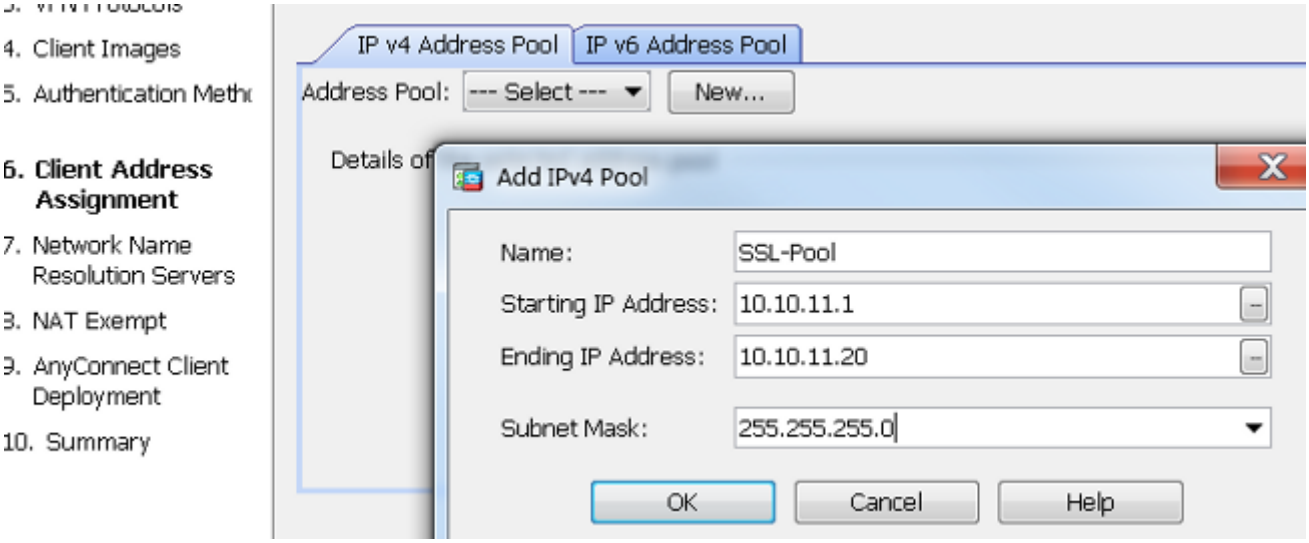
10. Una vez que se agrega la imagen, haga clic en **Siguiente**:



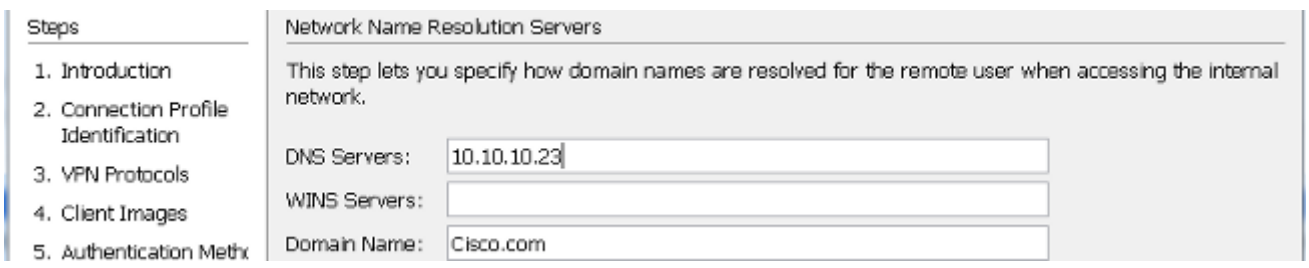
11. La autenticación de usuario se puede completar a través de los grupos de servidores de autenticación, autorización y auditoría (AAA). Si los usuarios ya están configurados, elija **LOCAL** y haga clic en **Siguiente**. **Nota:** En este ejemplo, se configura la autenticación **LOCAL**, lo que significa que la base de datos de usuarios local en ASA se utilizará para la autenticación.



12. Se debe configurar el conjunto de direcciones para el cliente VPN. Si ya hay uno configurado, selecciónelo en el menú desplegable. Si no lo hay, haga clic en **Nuevo** para configurar uno nuevo. Haga clic en **Siguiente** una vez completado:

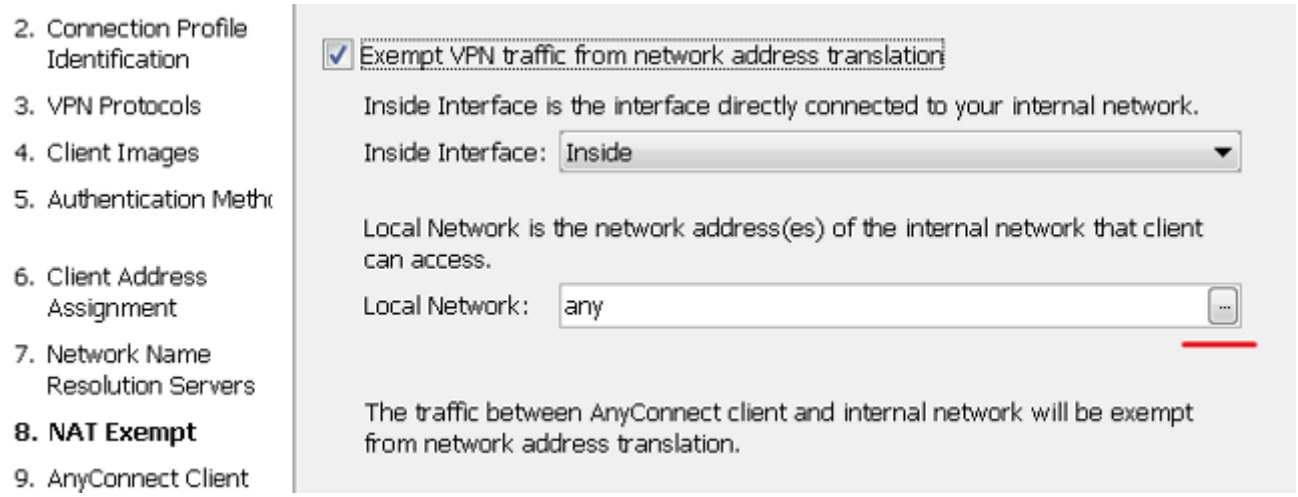


13. Ingrese los servidores y los DN del sistema de nombres de dominio (DNS) en los campos *DNS* y *Nombre de dominio*, y luego haga clic en **Siguiente**:

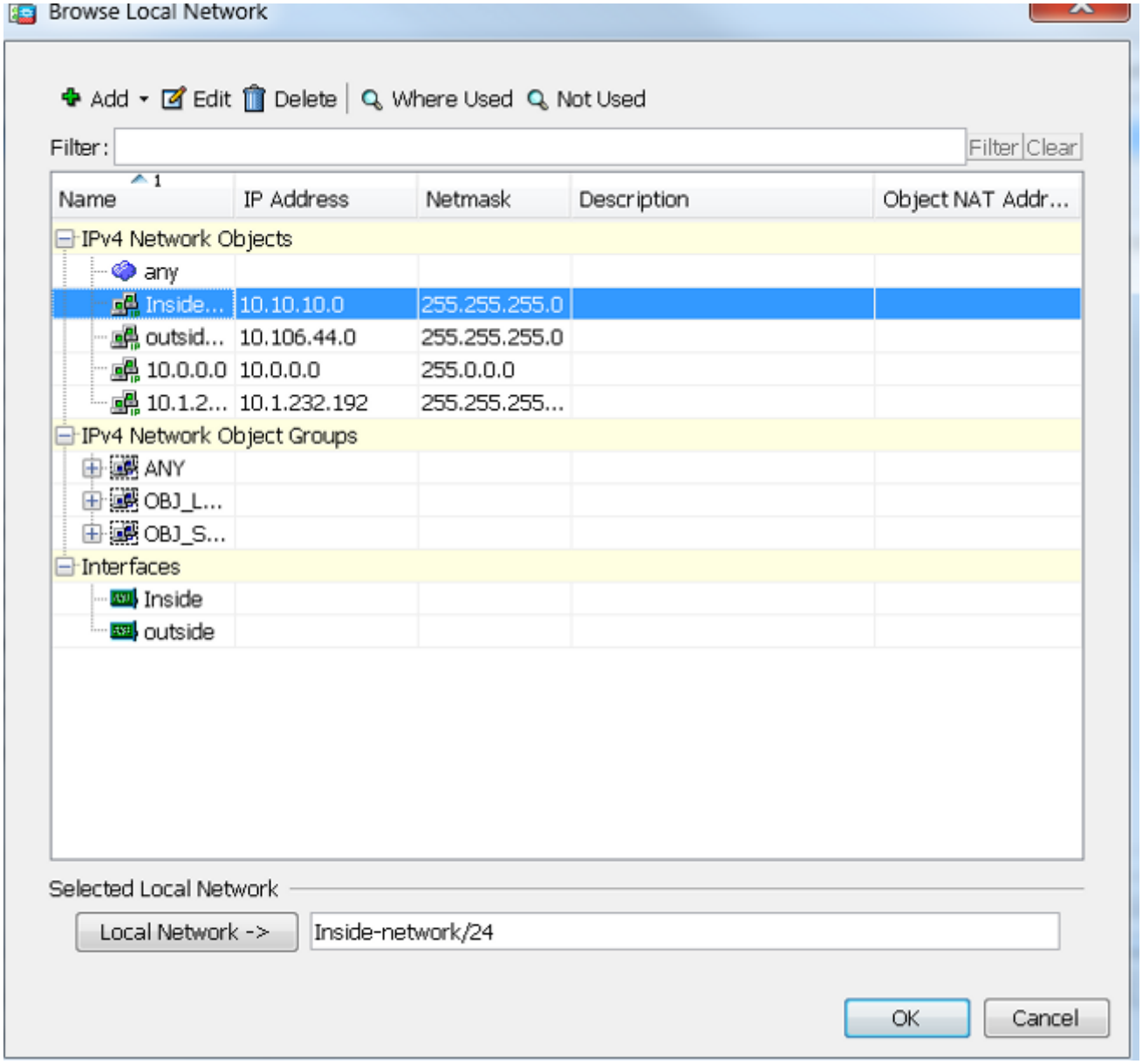


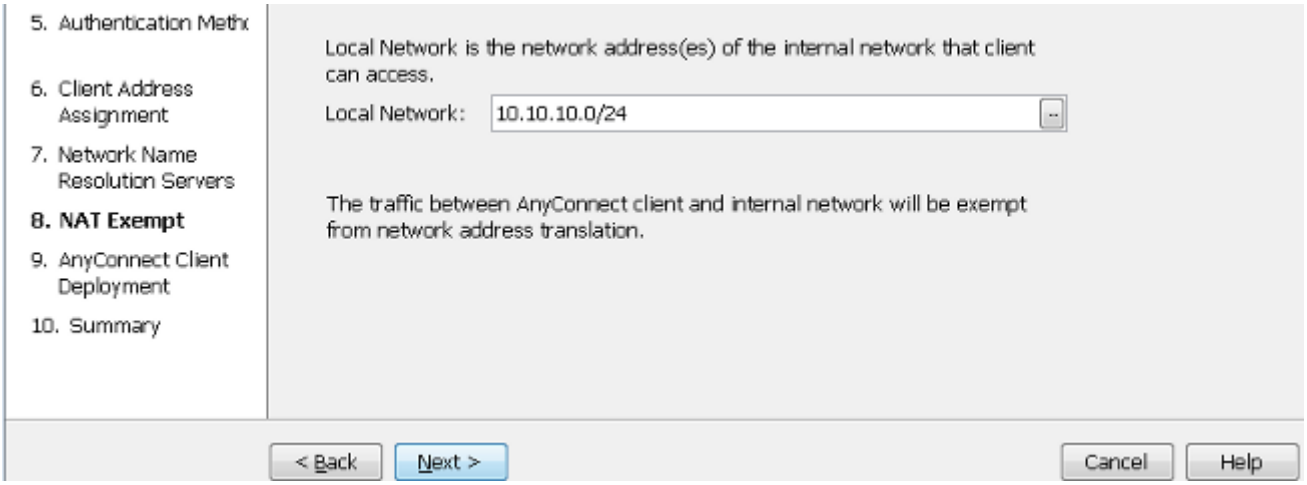
14. En esta situación, el objetivo es restringir el acceso a través de la VPN a la red **10.10.10.0/24** configurada como la subred *interna* (o LAN) detrás de ASA. El tráfico entre el cliente y la subred interna debe estar exento de cualquier traducción dinámica de direcciones de red (NAT).

    Marque la casilla **Exento de tráfico de VPN de traducción de direcciones de red** y configure las interfaces LAN y WAN que se utilizarán para la exención.



15. Elija las redes locales que deben estar exentas:





16. Haga clic en **Siguiente**, **Siguiente** y, luego, en **Finalizar**.

La configuración de AnyConnect Client ahora está completa. Sin embargo, cuando configura AnyConnect mediante el asistente de configuración, configura la política de *Túnel dividido*como **Túnel completo** de manera predeterminada. Para tunelizar solo tráfico específico, se debe implementar el *túnel dividido*.

Nota: Si no se configura el túnel dividido, la política de túnel dividido se heredará de la política de grupo predeterminada (DfltGrpPolicy), que se establece de manera predeterminada en **Túnel completo.** Esto significa que una vez que el cliente está conectado a través de la VPN, todo el tráfico (incluido el tráfico a la web) se envía a través del túnel.

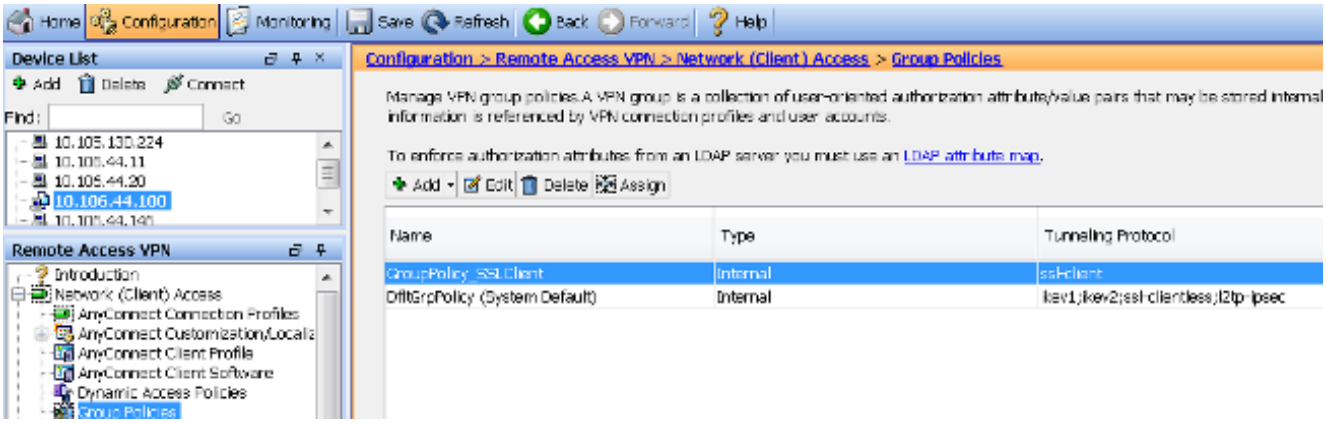
Solo el tráfico destinado a la dirección IP de la WAN (o *externa)* de ASA omitirá el túnel en la máquina del cliente. Esto se puede ver en el resultado del comando **route print** en máquinas con Microsoft Windows.

Configuración del túnel dividido

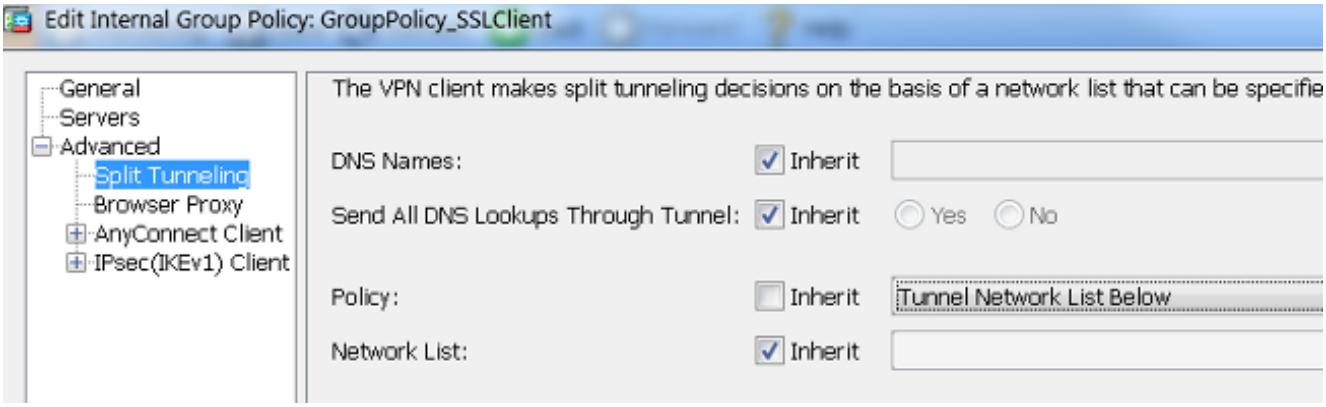
El túnel dividido es una característica que puede utilizar para definir el tráfico para las subredes o los hosts que deben cifrarse. Esto implica la configuración de una lista de control de acceso (ACL) que se asociará con esta función. El tráfico para las subredes o los hosts que se define en esta ACL se cifrará en el túnel desde el extremo del cliente y las rutas para estas subredes se instalarán en la tabla de enrutamiento de la PC.

Complete estos pasos para pasar de la configuración de *Túnel completo* a la configuración de *Túnel dividido*:

1. Vaya a **Configuración > VPN de acceso remoto > Políticas de grupo**:



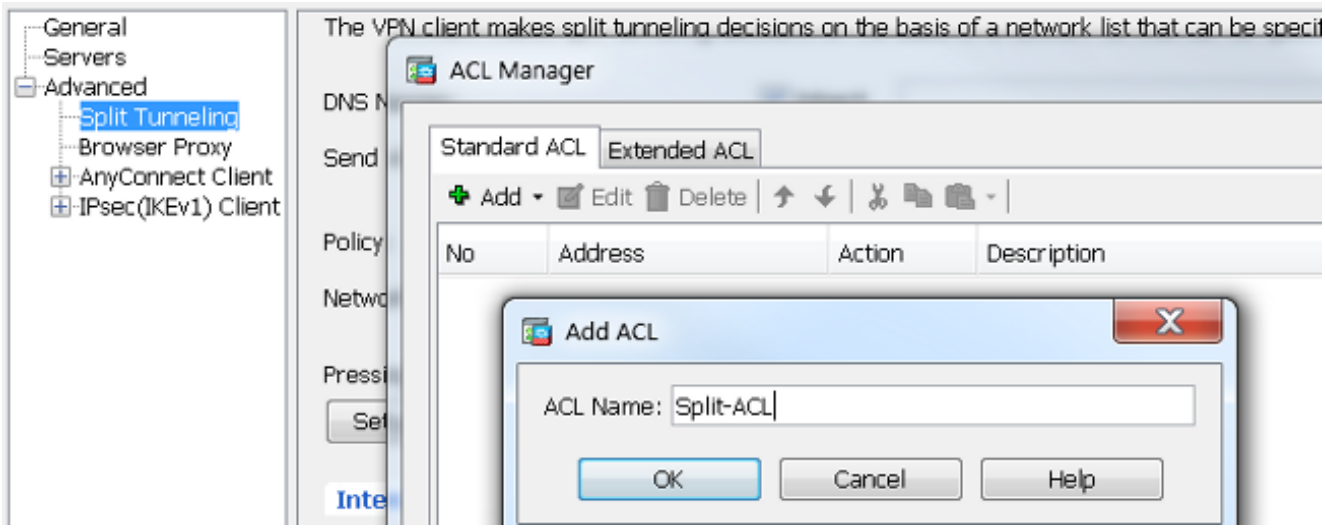
2. Haga clic en **Editar** y utilice el árbol de navegación para navegar a **Avanzado > Túnel dividido**. Desmarque la casilla de verificación **Heredar** en la sección *Política* y seleccione **Lista de redes de túneles a continuación** en el menú desplegable:



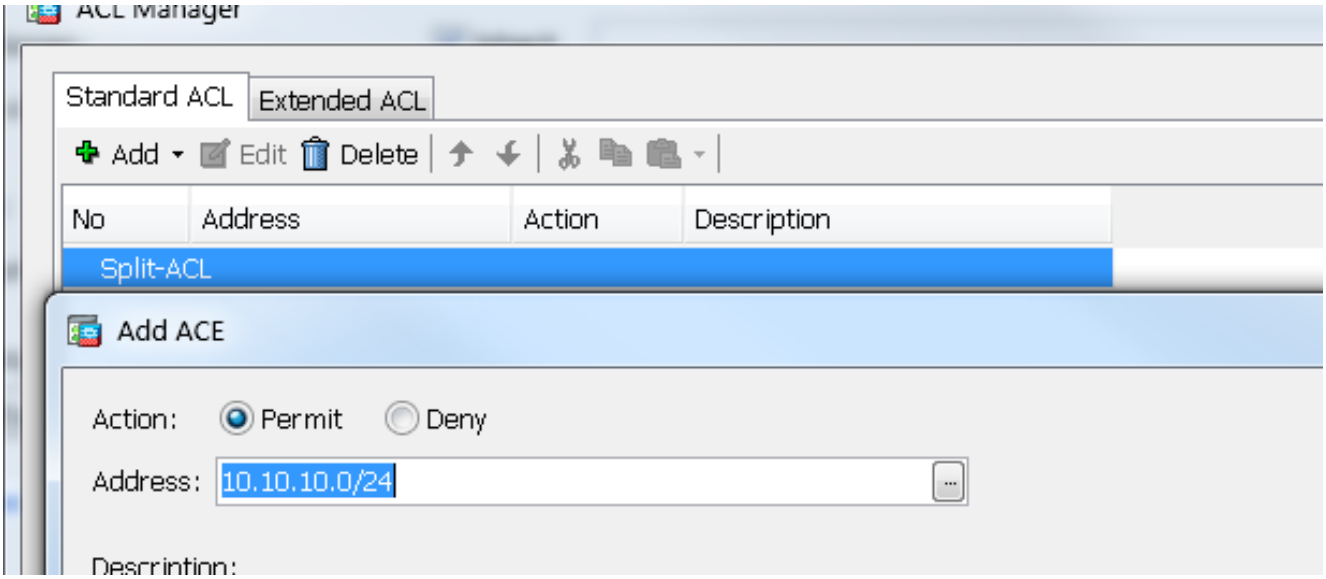
3. Desmarque la casilla de verificación **Heredar** en la sección *Lista de redes* y haga clic en

Administrar para seleccionar la ACL que especifica las LAN a las que el cliente necesita acceder:

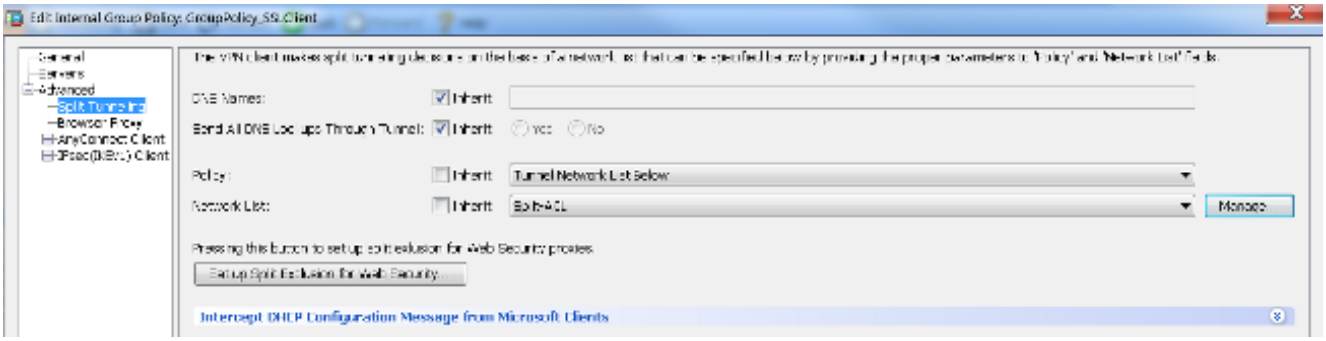
4. Haga clic en **ACL estándar**, **Agregar**, **Agregar ACL** y, luego, en **Nombre de ACL**.



5. Haga clic en **Agregar ACE** para agregar la regla:



6. Click OK.



7. Haga clic en Apply (Aplicar).

Una vez conectadas, las rutas para las subredes o los hosts en la ACL dividida se agregan a la tabla de enrutamiento de la máquina del cliente. En las máquinas con Microsoft Windows, esto se puede ver en el resultado del comando **route print**. El siguiente salto para estas rutas será una dirección IP de la subred del conjunto de IP del cliente (generalmente la primera dirección IP de la subred):

```
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.
```

En las máquinas con MAC OS, introduzca el comando **netstat -r** para ver la tabla de enrutamiento de la PC.

```
$ 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.
```

Descarga e instalación de AnyConnect Client

Existen dos métodos que puede utilizar para implementar Cisco AnyConnect Secure Mobility Client en la máquina del usuario:

- Implementación web

- Implementación independiente

Ambos métodos se explican con mayor detalle en las secciones siguientes.

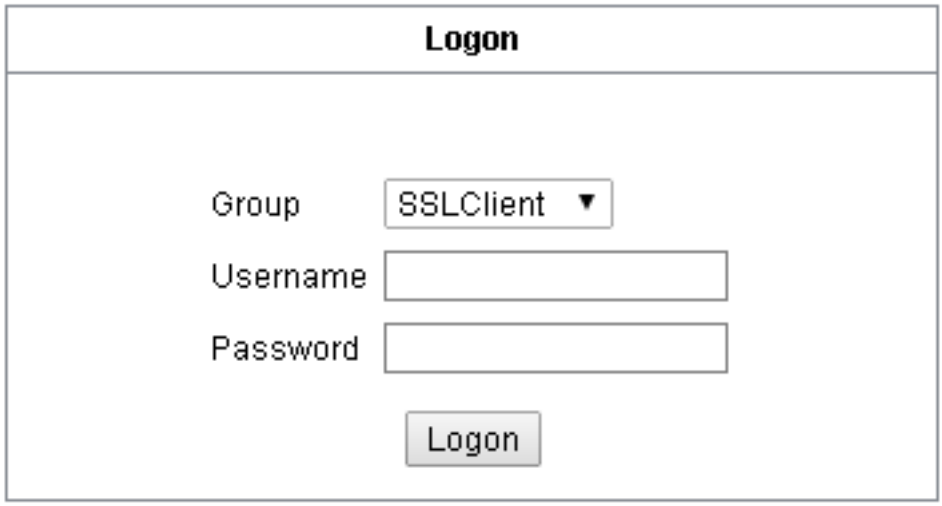
Implementación web

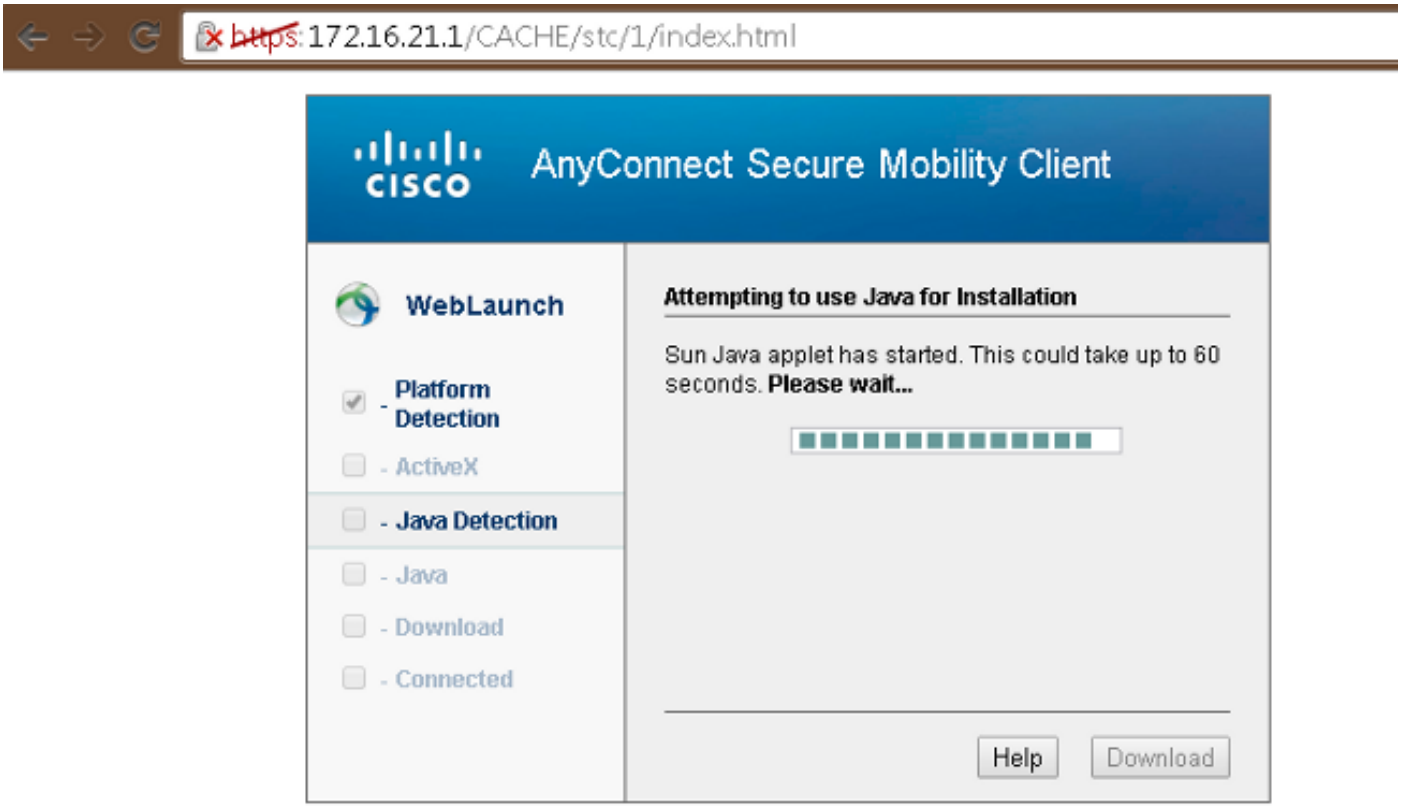
Para utilizar el método de implementación web, ingrese **https://<ASA's FQDN> o <ASA's IP>**la URL en un navegador en la máquina del cliente, que lo llevará a la página del portal de *WebVPN*.

> **Nota:** Si se utiliza Internet Explorer (IE), la instalación se realiza principalmente a través de ActiveX, a menos que se vea obligado a utilizar Java. Todos los demás navegadores utilizan Java.

Una vez iniciada la sesión en la página, la instalación debe comenzar en la máquina del cliente y el cliente debe conectarse a ASA una vez finalizada la instalación.

> **Nota:** Es posible que se le solicite permiso para ejecutar ActiveX o Java. Esto debe permitirse para continuar con la instalación.

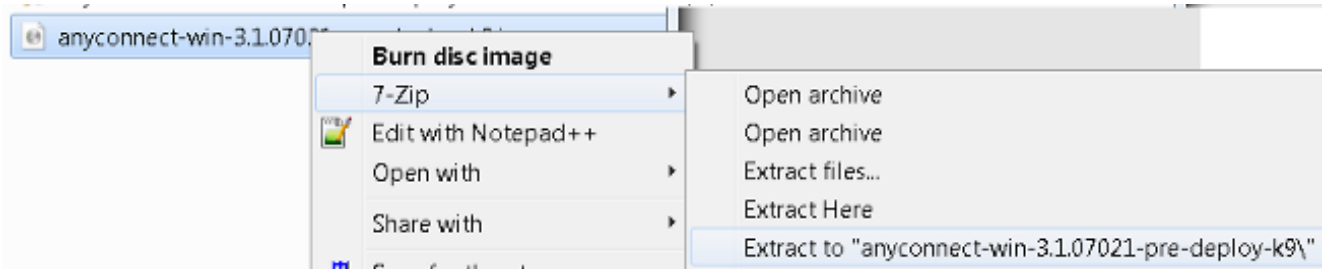




Implementación independiente

Complete estos pasos para utilizar los menús:

1. Descargue la imagen de AnyConnect Client del sitio web de Cisco. Para elegir la imagen correcta para descargar, consulte la página web de Cisco AnyConnect Secure Mobility Client. En esta página se proporciona un vínculo de descarga. Desplácese a la página de descarga y seleccione la versión adecuada. Realice una búsqueda por **Paquete de instalación completo - Ventana / Instalador independiente (ISO)**. **Nota:** Luego se descarga una imagen de instalador ISO (como *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
2. Utilice *WinRar* o *7-Zip* para extraer el contenido del paquete ISO:



3. Una vez extraído el contenido, ejecute el archivo **Setup.exe** y elija los módulos que deben instalarse junto con Cisco AnyConnect Secure Mobility Client.

   Consejo: Para configurar parámetros adicionales para la VPN, consulte la sección Configuración de conexiones de cliente VPN de AnyConnect de la *Guía de configuración de Cisco ASA serie 5500 con la CLI 8.4 y 8.6*.

Configuración de CLI

En esta sección se proporciona la configuración de la CLI para Cisco AnyConnect Secure Mobility Client con fines de referencia.

```
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
```

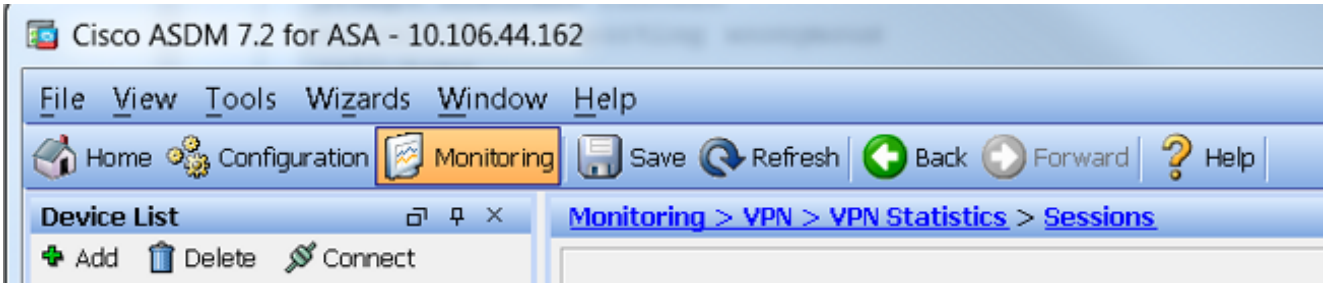
```
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact

!********** 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
```

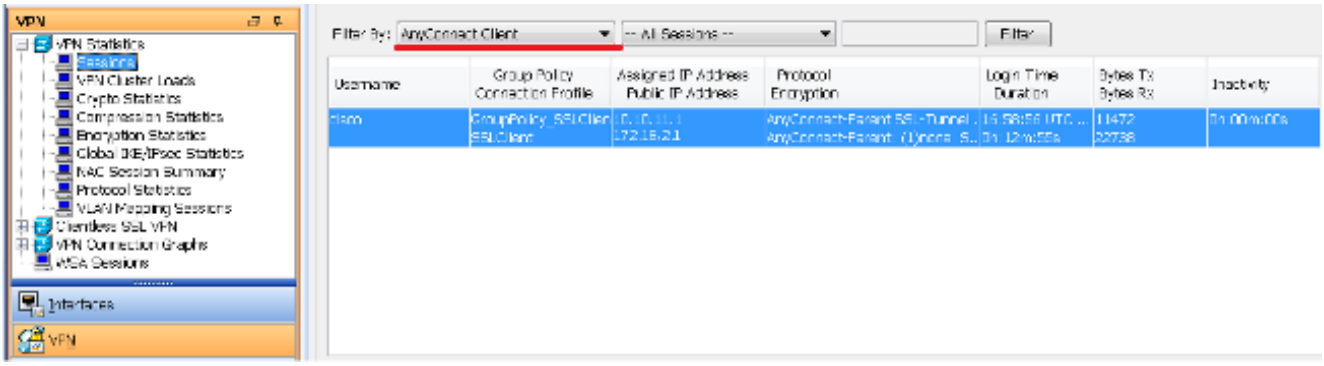
Verificación

Complete estos pasos para verificar la conexión del cliente y los diversos parámetros que están asociados a esa conexión:

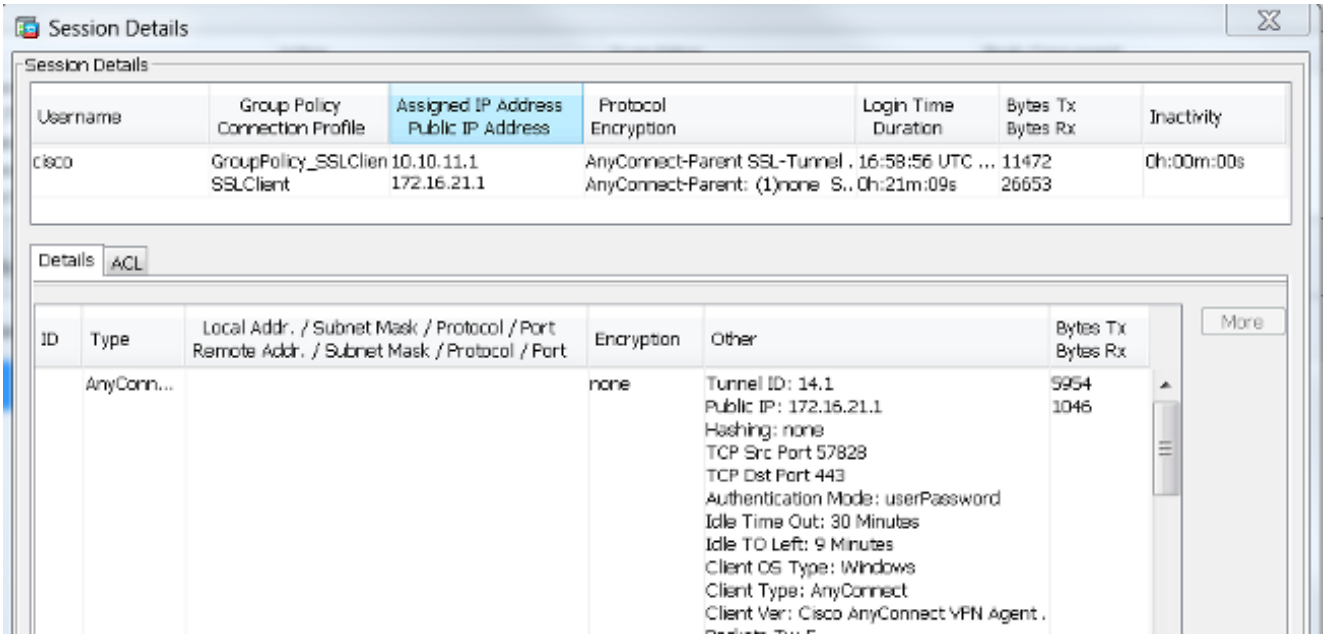
1. Vaya a **Monitoreo> VPN** en ASDM:



2. Puede utilizar la opción **Filtrar por** para filtrar el tipo de VPN. Seleccione **AnyConnect Client** del menú desplegable y todas las sesiones de AnyConnect Client. **Consejo:** Las sesiones se pueden filtrar aún más con otros criterios, como *Nombre de usuario* y *Dirección IP*.



3. Haga doble clic en una sesión para obtener más detalles sobre esa sesión en particular:



4. Ingrese el comando **show vpn-sessiondb anyconnect** en la CLI para obtener los detalles de la sesión:

```
# 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. Puede utilizar las otras opciones de filtro para refinar los resultados:

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
```

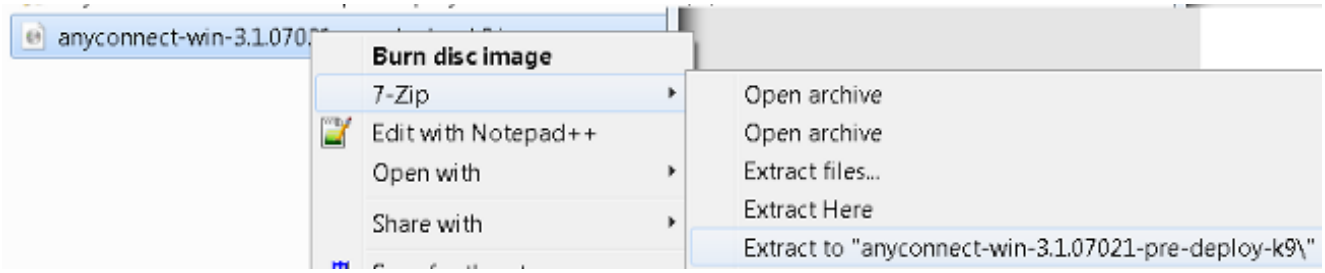
Troubleshoot

Puede utilizar la herramienta de diagnóstico e informes de AnyConnect (DART) para recopilar los datos que son útiles para solucionar los problemas de instalación y conexión de AnyConnect. El asistente de DART se utiliza en el equipo que ejecuta AnyConnect. La DART reúne los registros, el estado y la información de diagnóstico para el análisis de Cisco Technical Assistance Center (TAC) y no requiere privilegios de administrador para ejecutarse en la máquina del cliente.

Instalación de la DART

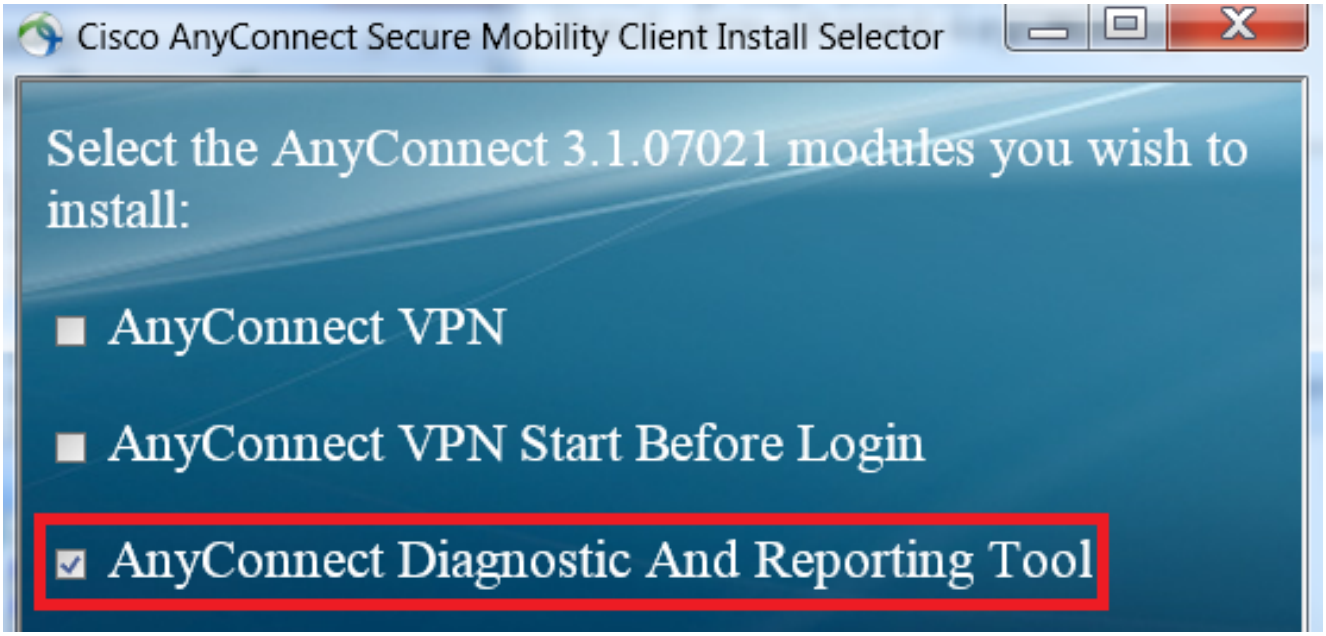
Complete estos pasos para instalar la DART:

1. Descargue la imagen de AnyConnect Client del sitio web de Cisco. Para elegir la imagen correcta para descargar, consulte la página web de Cisco AnyConnect Secure Mobility Client. En esta página se proporciona un vínculo de descarga. Desplácese a la página de descarga y seleccione la versión adecuada. Realice una búsqueda por **Paquete de instalación completo - Ventana / Instalador independiente (ISO)**. **Nota:** Luego se descarga una imagen de instalador ISO (como *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
2. Utilice *WinRar* o *7-Zip* para extraer el contenido del paquete ISO:



3. Navegue hasta la carpeta a la que se extrajo el contenido.

4. Ejecute el archivo **Setup.exe** y seleccione solo **Herramienta de diagnóstico e informes de Anyconnect**:

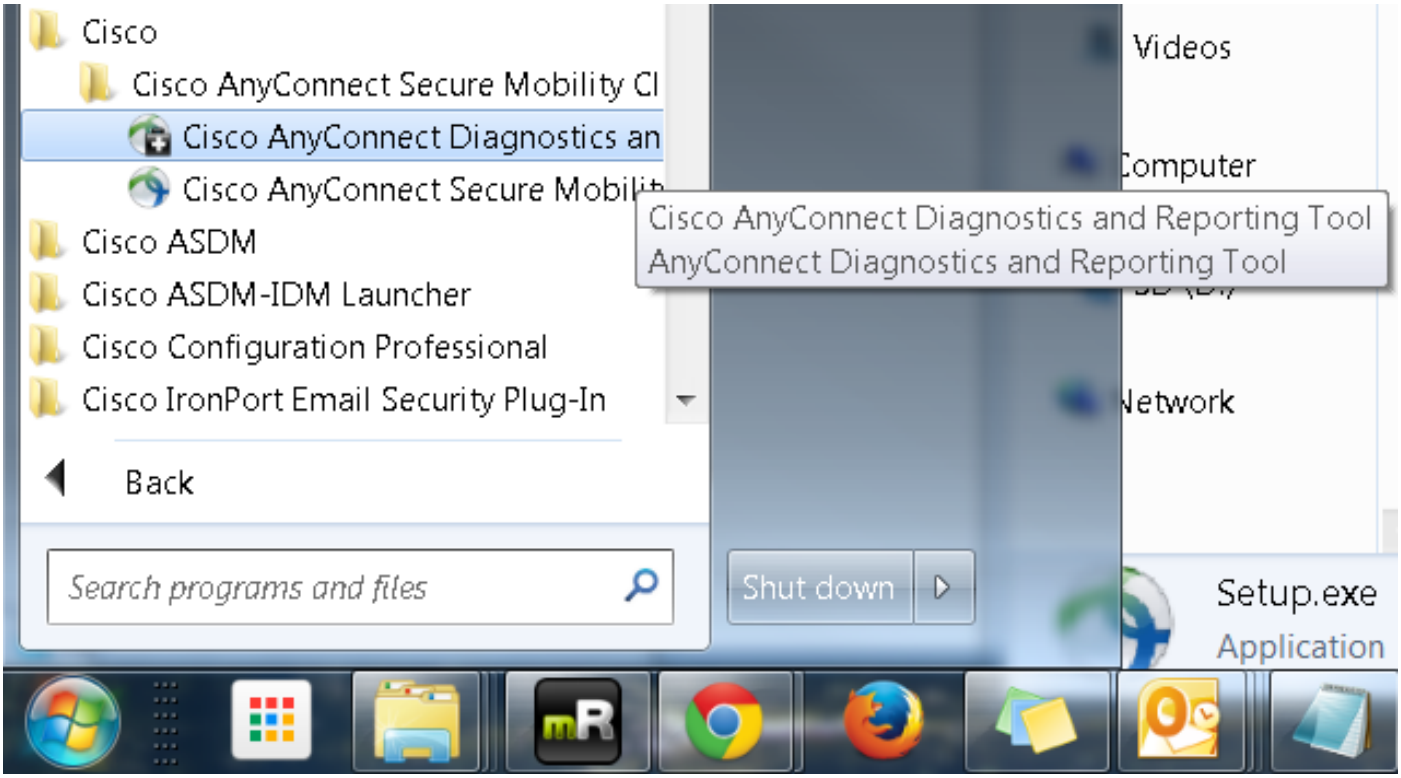


Ejecución de la DART

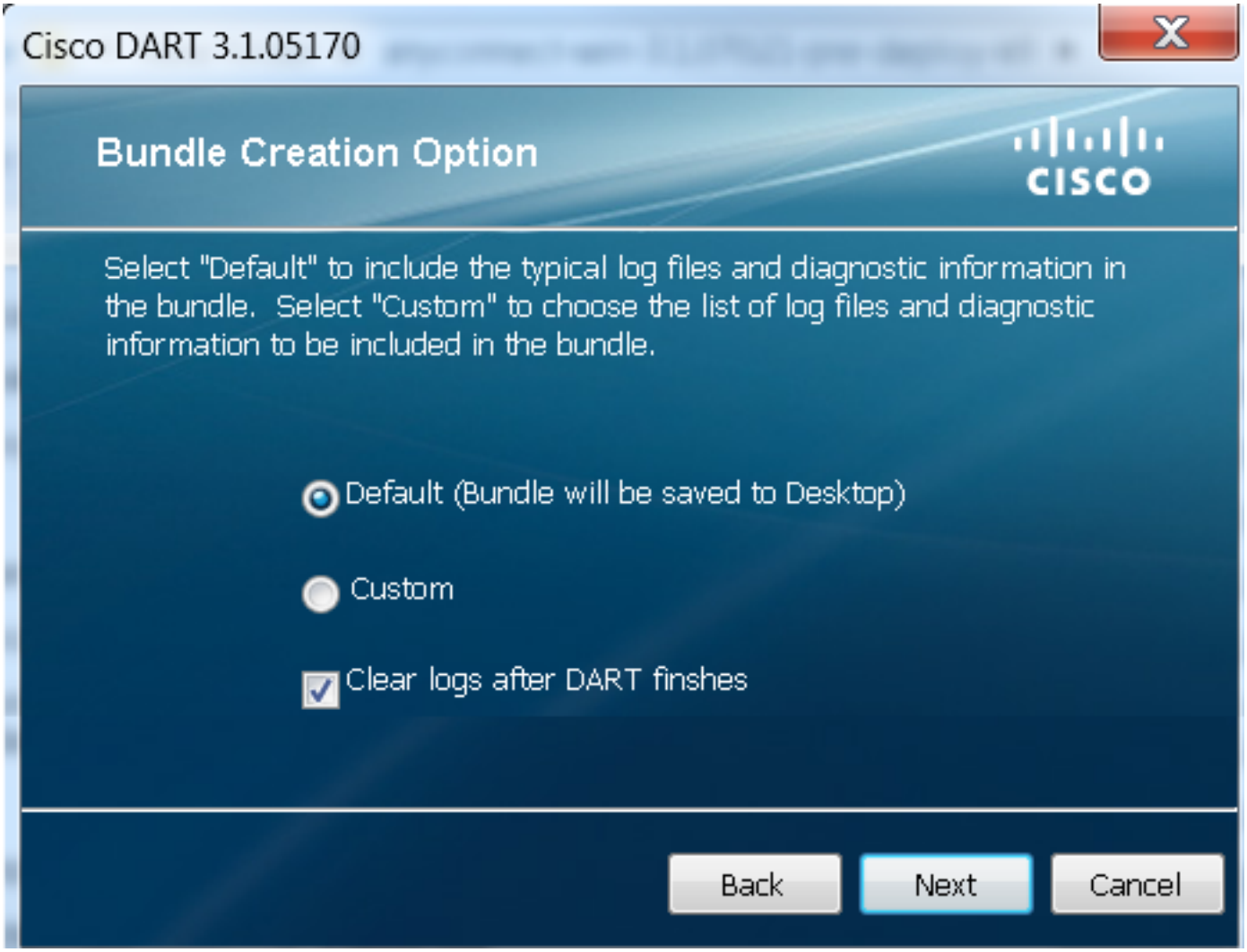
Aquí hay información importante que debe tener en cuenta antes de ejecutar la DART:

- El problema se debe recrear al menos una vez antes de ejecutar la DART.
- La fecha y hora en la máquina del usuario deben tenerse en cuenta cuando se vuelve a crear el problema.

Ejecute la DART desde el menú *Inicio* en la máquina del cliente:



Se puede seleccionar el modo *Predeterminado* o *Personalizado*. Cisco recomienda ejecutar la DART en el modo predeterminado para que toda la información se pueda capturar en una sola toma.



Una vez completada, la herramienta guarda el archivo *.zip* del paquete de la DART en el escritorio del cliente. El paquete se puede enviar por correo electrónico a TAC (después de abrir un caso en TAC) para su posterior análisis.

Información Relacionada

- Guía de solución de problemas de AnyConnect VPN Client: problemas comunes
- Problemas de Java 7 con AnyConnect, CSD/Hostscan y WebVPN: guía de solución de problemas
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).