

Configurar o AnyConnect Secure Mobility Client com túnel dividido em um ASA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Informações sobre a licença do AnyConnect](#)

[Configurar](#)

[Diagrama de Rede](#)

[Assistente de configuração do ASDM AnyConnect](#)

[Configuração de túnel dividido](#)

[Baixe e instale o AnyConnect Client](#)

[Implantação na Web](#)

[Implantação autônoma](#)

[Configuração de CLI](#)

[Verificar](#)

[Troubleshoot](#)

[Instale o DART](#)

[Execute o DART](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o Cisco AnyConnect Secure Mobility Client por meio do Cisco Adaptive Security Device Manager (ASDM) em um Cisco Adaptive Security Appliance (ASA) que executa a versão de software 9.3(2).

Prerequisites

Requirements

O pacote de implantação na Web do Cisco AnyConnect Secure Mobility Client deve ser baixado no desktop local em que ocorre o acesso do ASDM ao ASA. Para baixar o pacote cliente, consulte a página da Web [Cisco AnyConnect Secure Mobility Client](#). Os pacotes de implantação na Web para vários sistemas operacionais (SOs) podem ser carregados no ASA ao mesmo tempo.

Estes são os nomes dos arquivos de implantação na Web de vários SOs:

- SOs Microsoft Windows – *AnyConnect-win-<version>-k9.pkg*

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA versão 9.3(2)
- ASDM versão 7.3(1)101
- AnyConnect versão 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.

Informações de Apoio

Este documento fornece detalhes passo a passo sobre como usar o assistente de configuração do Cisco AnyConnect por meio do ASDM para configurar o AnyConnect Client e ativar o túnel dividido.

O túnel dividido é usado nos cenários em que apenas o tráfego específico deve ser encapsulado, ao contrário dos cenários em que todo o tráfego gerado pelo computador cliente flui pela VPN, quando conectada. Por padrão, o uso do assistente de configuração do AnyConnect resultará em uma configuração de *tunnel-all* no ASA. O túnel dividido deve ser configurado separadamente, o que é explicado mais detalhadamente na seção deste documento.

O objetivo deste exemplo de configuração é enviar o tráfego para a sub-rede 10.10.10.0/24, que é a sub-rede de LAN atrás do ASA, pelo túnel VPN, e todo o tráfego restante do computador cliente é encaminhado através de seu próprio circuito de Internet.

Informações sobre a licença do AnyConnect

Estes são alguns links para obter informações úteis sobre as licenças do Cisco AnyConnect Secure Mobility Client:

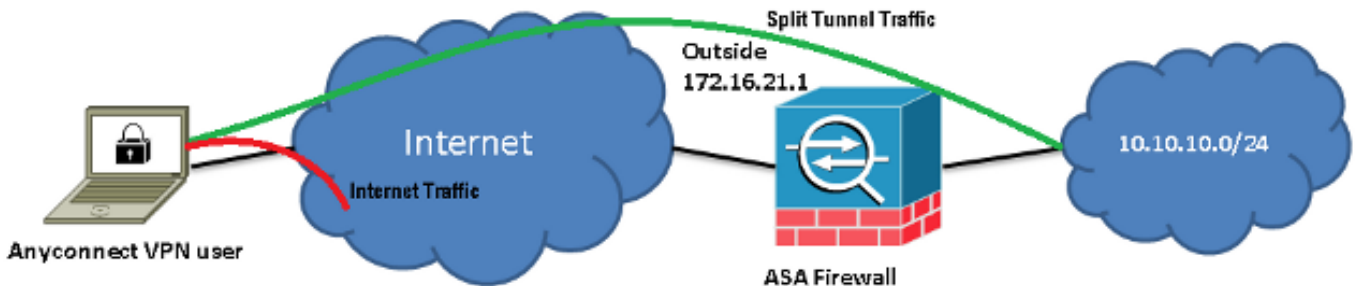
- Consulte o documento [recursos, licenças e SOs do AnyConnect Secure Mobility Client versão 3.1](#) para determinar as licenças necessárias para o AnyConnect Secure Mobility Client e os recursos relacionados.
- Consulte o [guia de pedidos do Cisco AnyConnect](#) para obter informações sobre as licenças Apex e Plus do AnyConnect.
- Consulte o documento [Qual licença do ASA é necessária para conexões de telefone IP e VPN móvel?](#) para obter informações sobre os requisitos adicionais de licença para conexões de telefone IP e dispositivos móveis.

Configurar

Esta seção descreve como configurar o Cisco AnyConnect Secure Mobility Client no ASA.

Diagrama de Rede

Esta é a topologia usada nos exemplos deste documento:

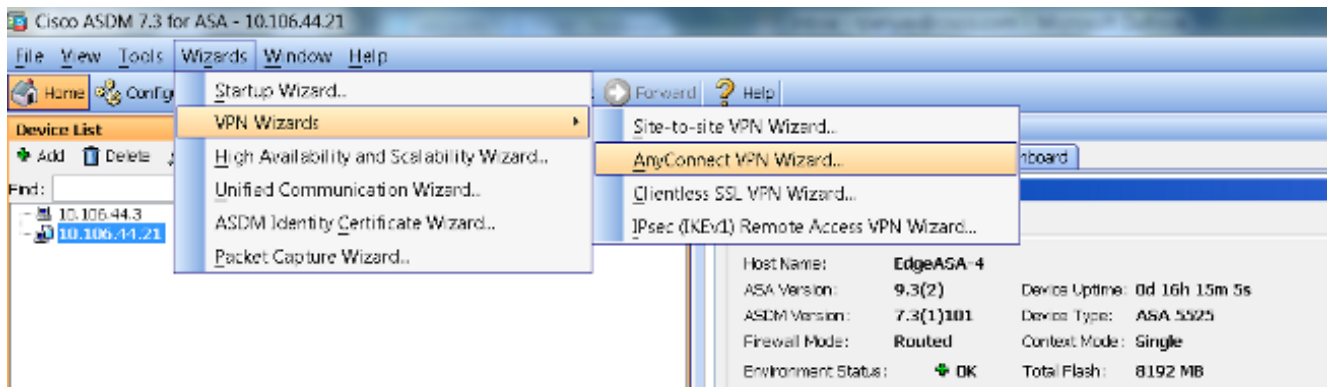


Assistente de configuração do ASDM AnyConnect

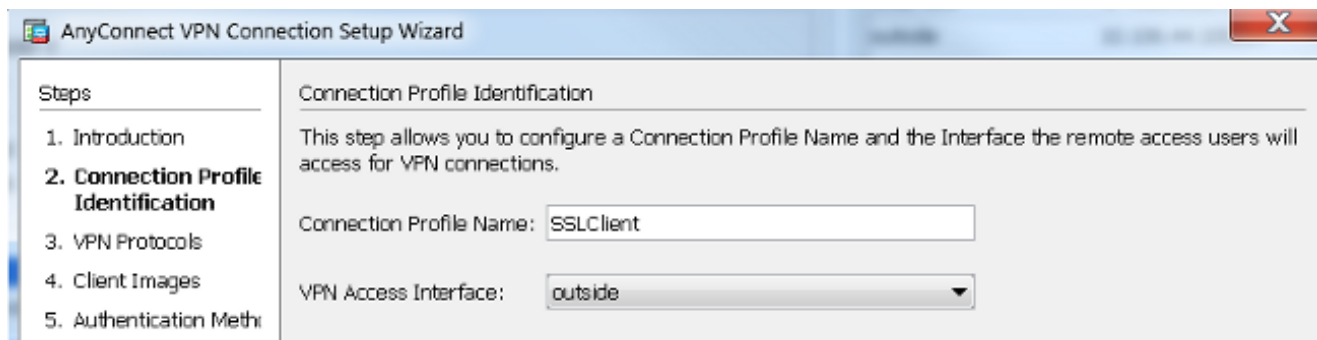
O assistente de configuração do AnyConnect pode ser usado para configurar o AnyConnect Secure Mobility Client. Verifique se um pacote do AnyConnect Client foi carregado no flash/disco do firewall do ASA, antes de continuar.

Siga estas etapas para configurar o AnyConnect Secure Mobility Client usando o assistente de configuração:

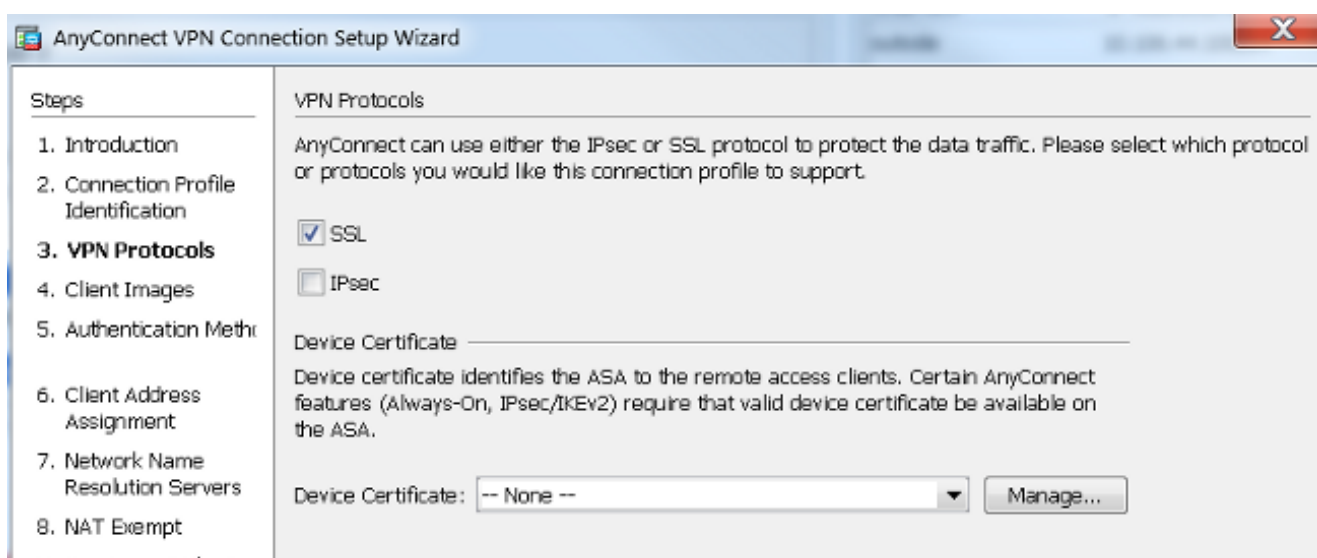
1. Faça login no ASDM, inicie o **assistente de configuração** e clique em **Avançar**:



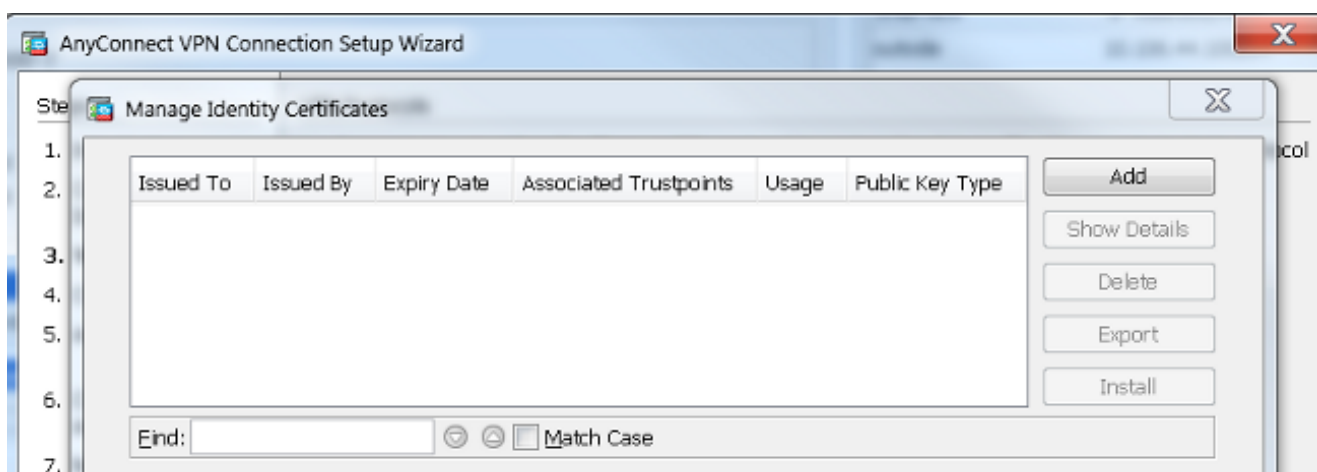
2. Insira o *nome do perfil de conexão*, escolha a interface em que a VPN será encerrada no menu suspenso *Interface de acesso VPN* e clique em **Avançar**:



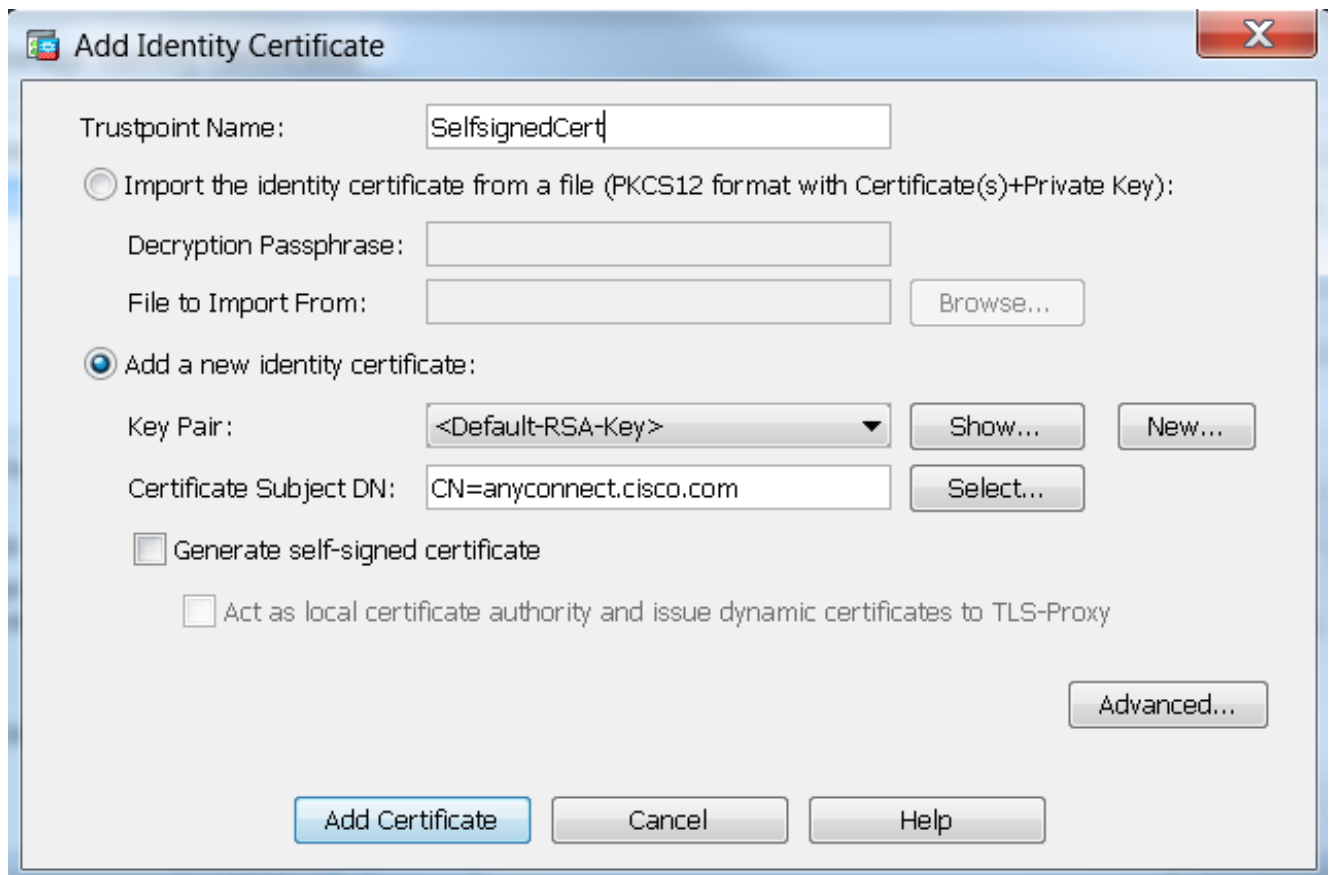
3. Marque a caixa de seleção **SSL** para ativar o Secure Sockets Layer (SSL). O *certificado do dispositivo* pode ser emitido por uma autoridade de certificado (CA) de terceiros confiável (como a Verisign ou a Entrust) ou pode ser um certificado autoassinado. Se o certificado já estiver instalado no ASA, poderá ser escolhido no menu suspenso. **Note:** Este é o certificado do lado do servidor que será fornecido. Se não houver certificados instalados no ASA no momento e for necessário gerar um certificado autoassinado, clique em **Gerenciar**. Para instalar um certificado de terceiros, siga as etapas descritas no documento da Cisco [Instalar manualmente os certificados de fornecedores de terceiros do ASA 8.x para uso com o exemplo de configuração de WebVPN](#).



4. Clique em **Adicionar**.



5. Digite um nome apropriado no campo *Nome de trustpoint* e clique no botão de opção **Adicionar um novo certificado de identidade**. Se não houver pares de chaves Rivest-Shamir-Addleman (RSA) no dispositivo, clique em **Novo** para gerar um:



Add Identity Certificate

Trustpoint Name:

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:

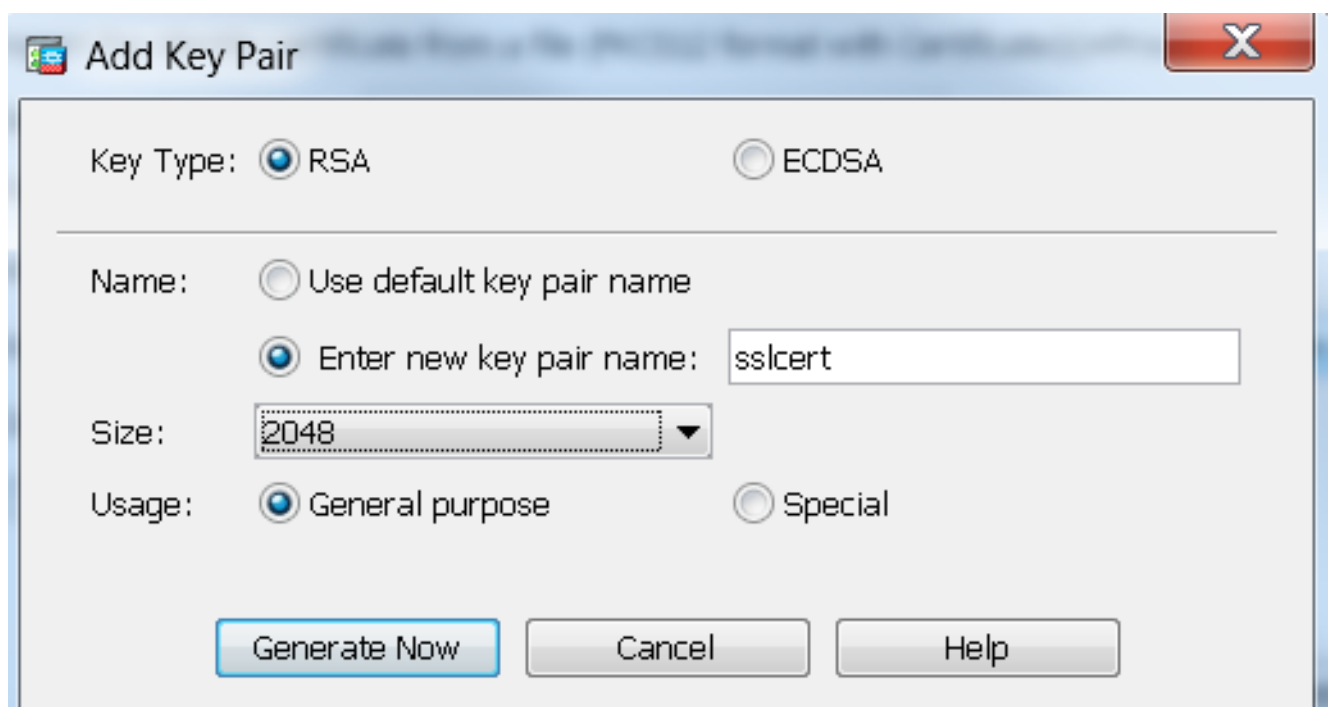
Key Pair:

Certificate Subject DN:

Generate self-signed certificate

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

6. Clique no botão de opção **Usar nome de par de chaves padrão** ou **Inserir novo nome de par de chaves** e insira um novo nome. Selecione o tamanho das chaves e clique em **Gerar agora**:



Add Key Pair

Key Type: RSA ECDSA

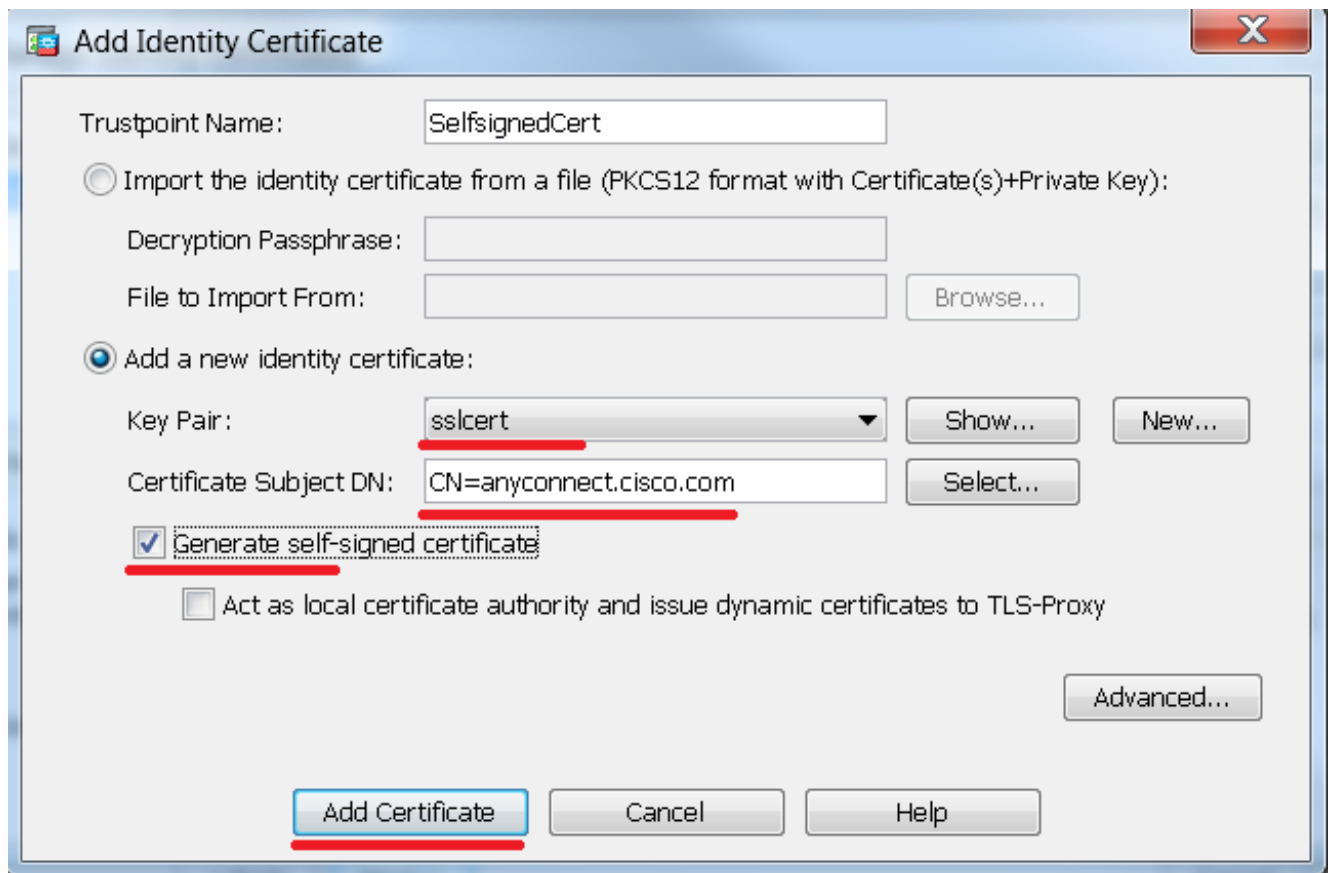
Name: Use default key pair name

Enter new key pair name:

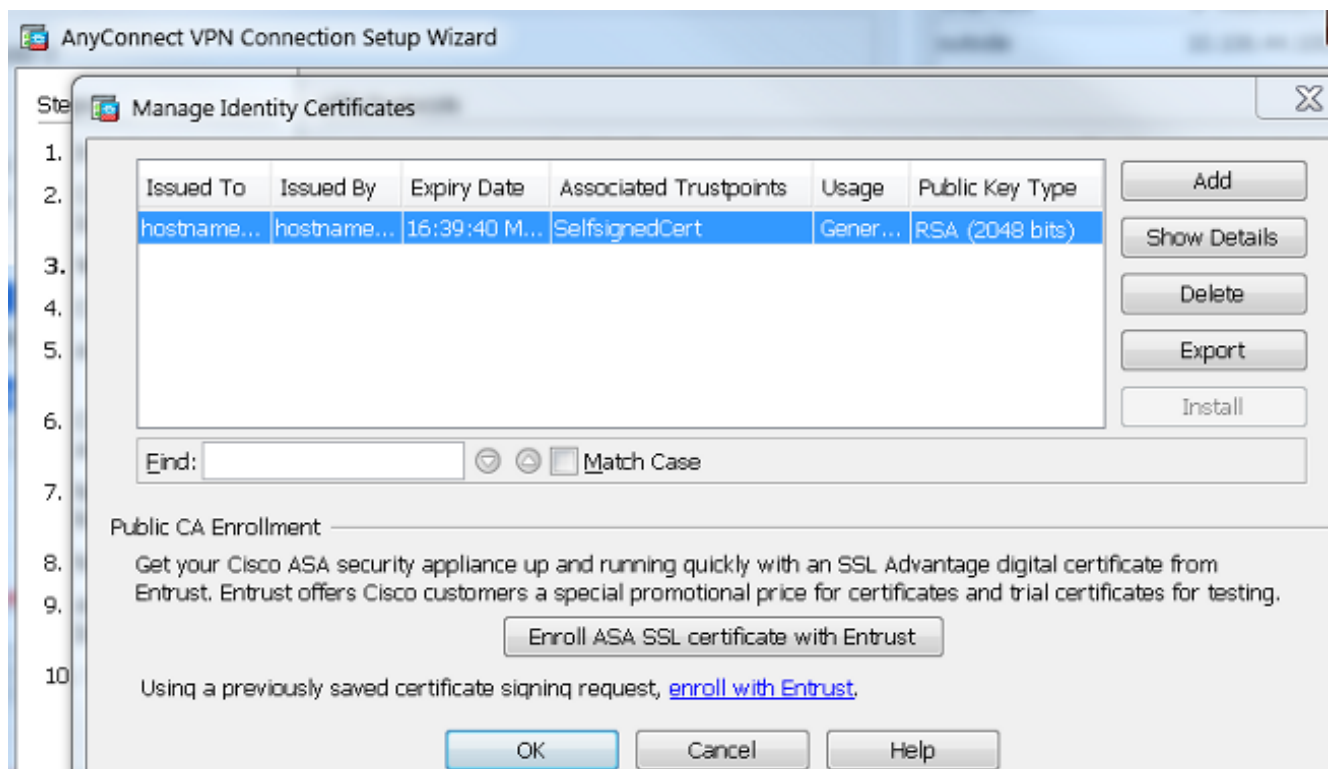
Size: ▼

Usage: General purpose Special

7. Depois que o par de chaves RSA for gerado, escolha a chave e marque a caixa de seleção **Gerar certificado autoassinado**. Insira o nome do domínio (DN) do assunto desejado no campo *DN do assunto do certificado* e clique em **Adicionar certificado**:

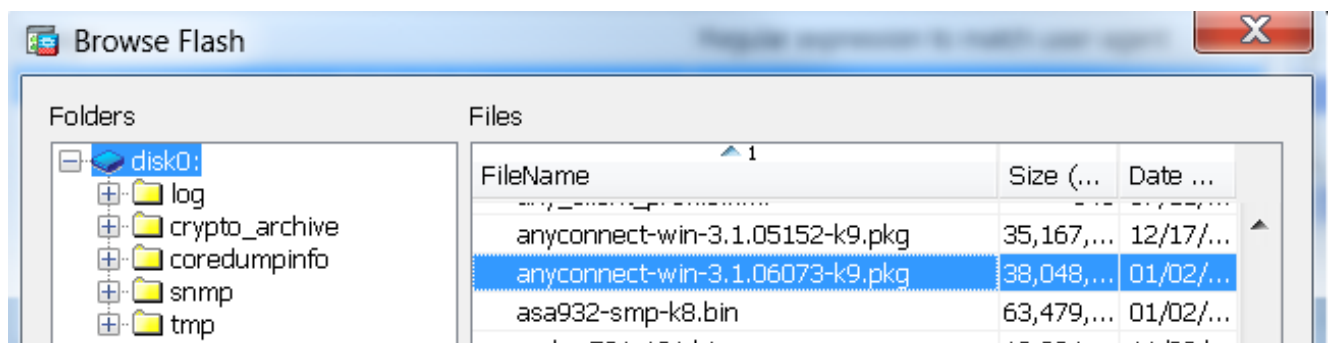
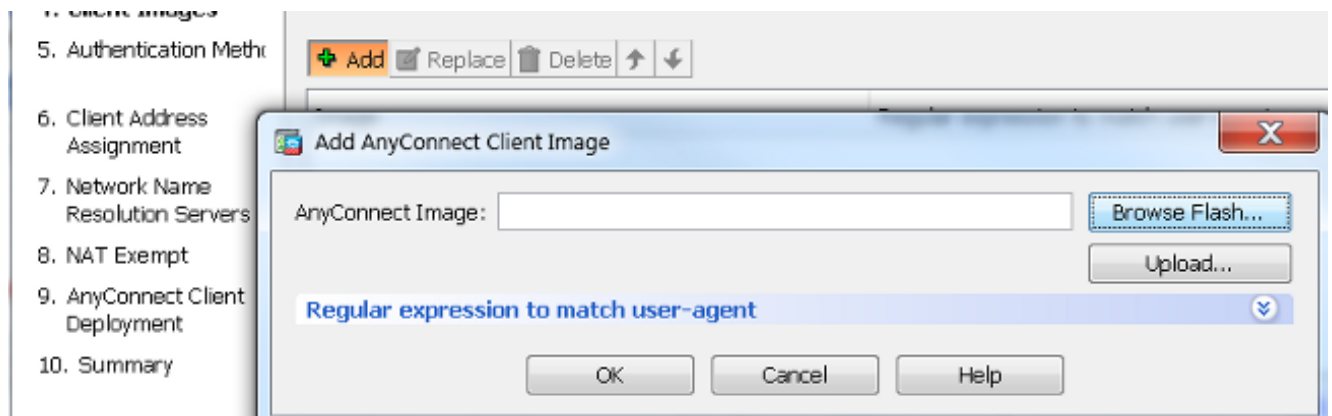


8. Quando a inscrição estiver concluída, clique em **OK**, **OK** e depois em **Avançar**:

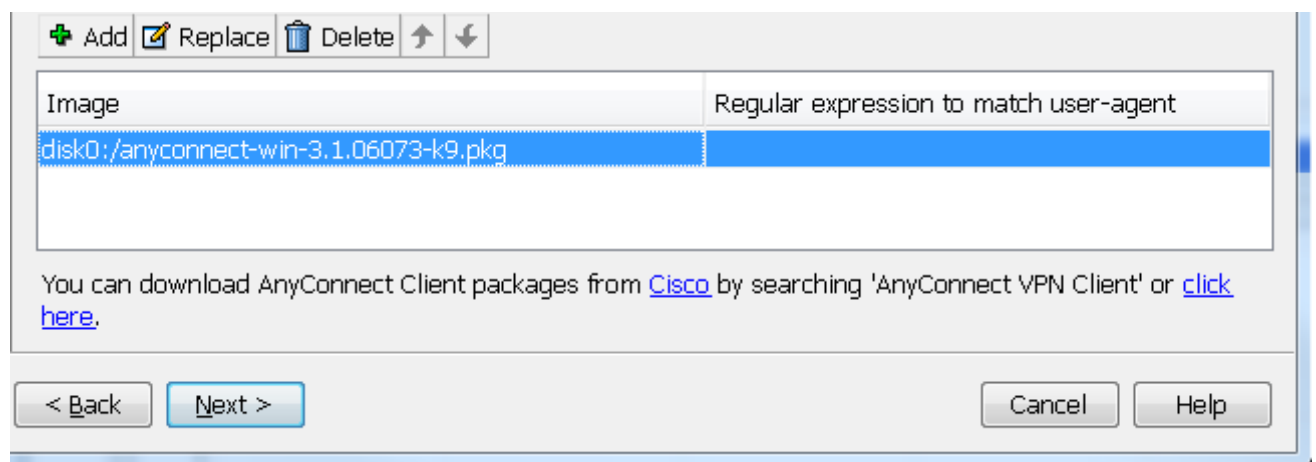


9. Clique em **Adicionar** para adicionar a imagem do AnyConnect Client (o arquivo *.pkg*) no PC

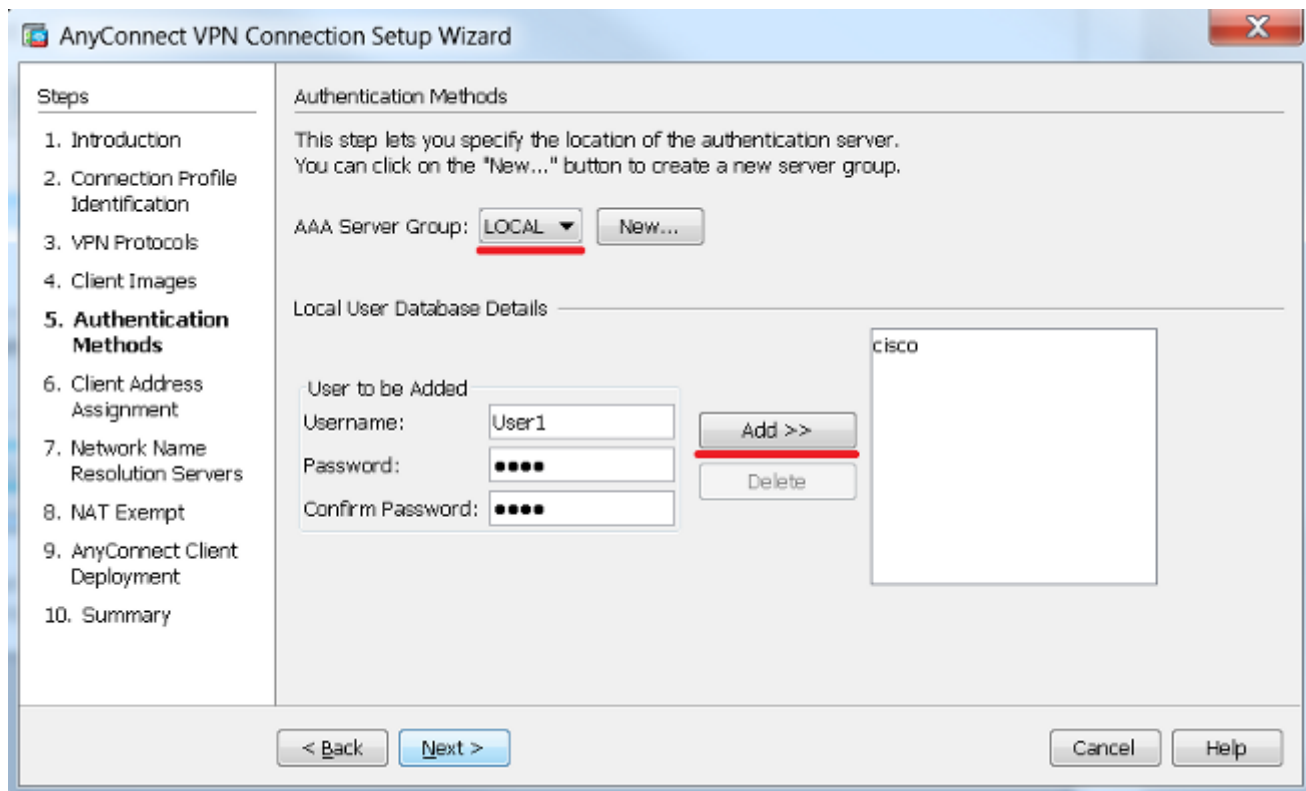
ou no flash. Clique em **Procurar flash** para adicionar a imagem da unidade flash ou clique em **Carregar** para adicionar a imagem diretamente do computador host:



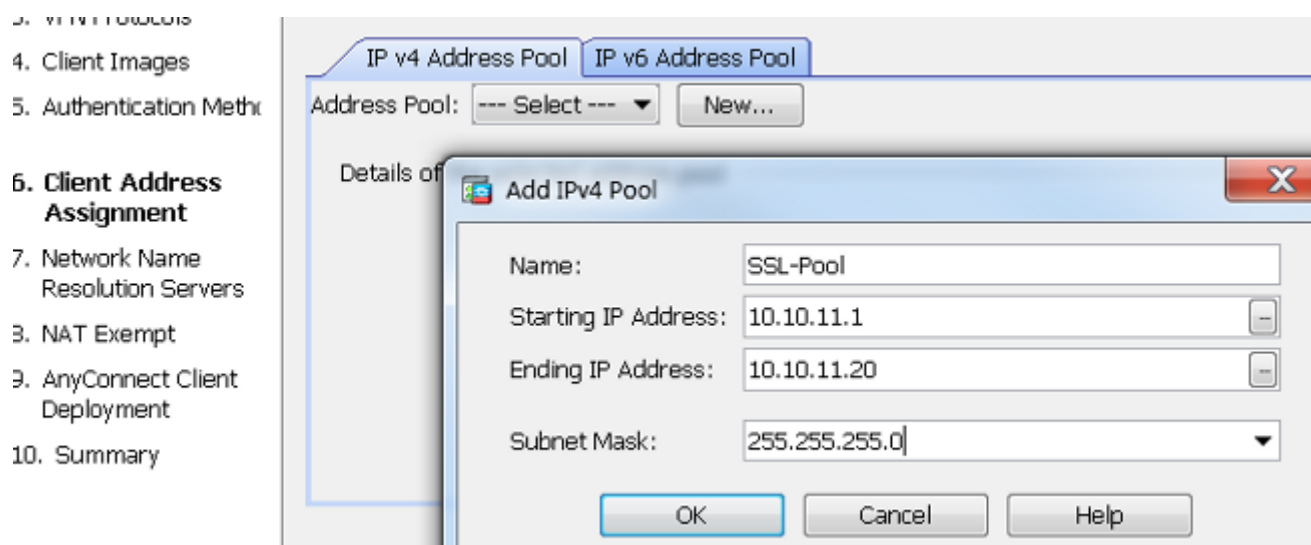
10. Quando a imagem for adicionada, clique em **Avançar**:



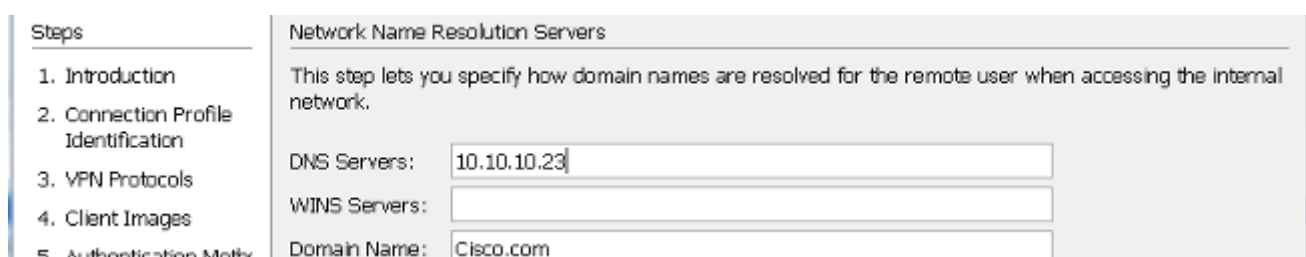
11. A autenticação do usuário pode ser concluída por meio dos grupos de servidores Autenticação, Autorização e Contabilização (AAA). Se os usuários já estiverem configurados, escolha **LOCAL** e clique em **Avançar**. **Note:** Neste exemplo, a autenticação **LOCAL** está configurada e significa que o banco de dados do usuário local no ASA será usado para autenticação.



12. O pool de endereços do cliente VPN deve ser configurado. Se já estiver configurado, selecione-o no menu suspenso. Caso contrário, clique em **Novo** para configurar um novo. Quando terminar, clique em **Avançar**.



13. Insira os servidores DNS (Domain Name System) e os DNS nos campos *DNS* e *Nome de domínio* de forma adequada e clique em **Avançar**:



14. Neste cenário, o objetivo é restringir o acesso pela VPN à rede **10.10.10.0/24** configurada como sub-rede (ou LAN) *interna* atrás do ASA. O tráfego entre o cliente e a sub-rede interna deve ser isento de conversão de endereço de rede (NAT) dinâmica.

Marque a caixa de seleção **Isentar tráfego VPN de conversão de endereço de rede** e configure as interfaces de LAN e WAN que serão usadas para a isenção:

2. Connection Profile Identification

3. VPN Protocols

4. Client Images

5. Authentication Method

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.

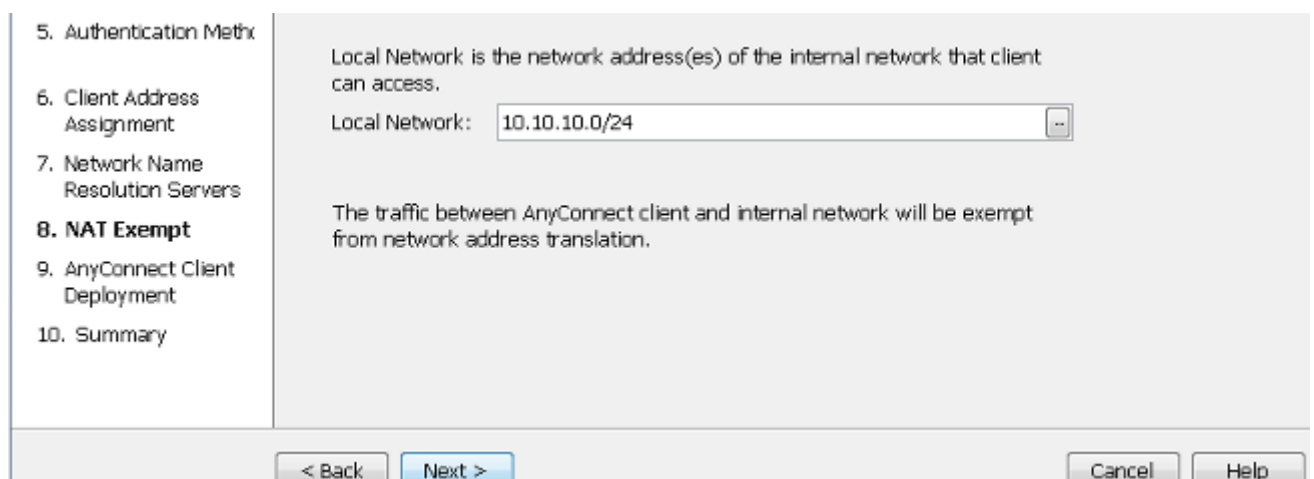
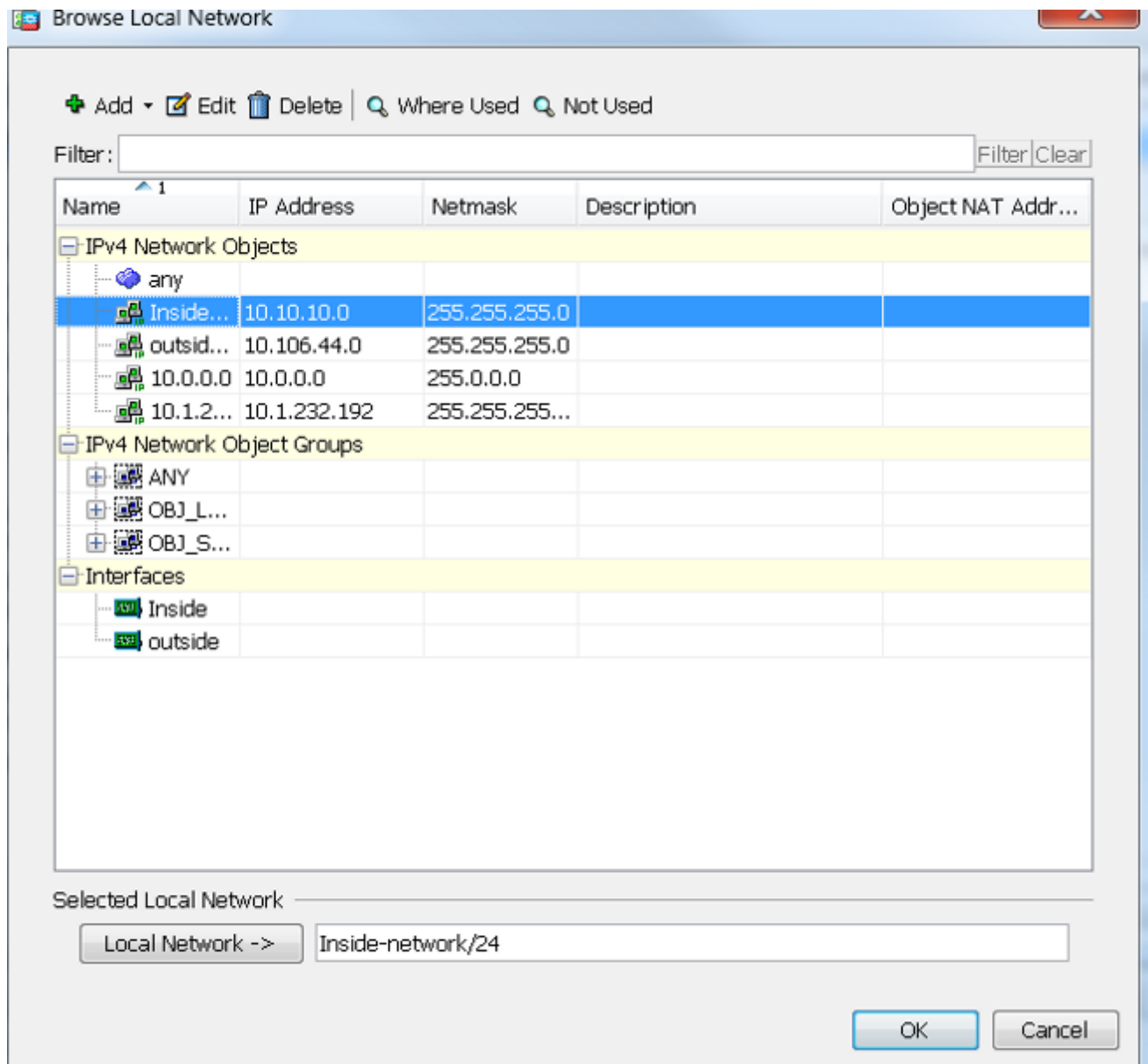
Inside Interface:

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

Local Network:

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

15. Escolha as redes locais que devem ser isentas:



16. Clique em **Avançar**, **Avançar** e, em seguida, **Concluir**.

Agora a configuração do AnyConnect Client está concluída. No entanto, quando você configura o AnyConnect usando o assistente de configuração, ele configura a política de *túnel dividido* como **Tunnelall** por padrão. Para encapsular somente tráfego específico, o *split-tunneling* deve ser implementado.

Note: Se o split-tunneling não estiver configurado, a política de túnel dividido será herdada do group-policy padrão (DfltGrpPolicy), definida por padrão como **Tunnelall**. Isso significa que quando o cliente estiver conectado por VPN, todo o tráfego (incluindo o tráfego para a Web) será enviado pelo túnel.

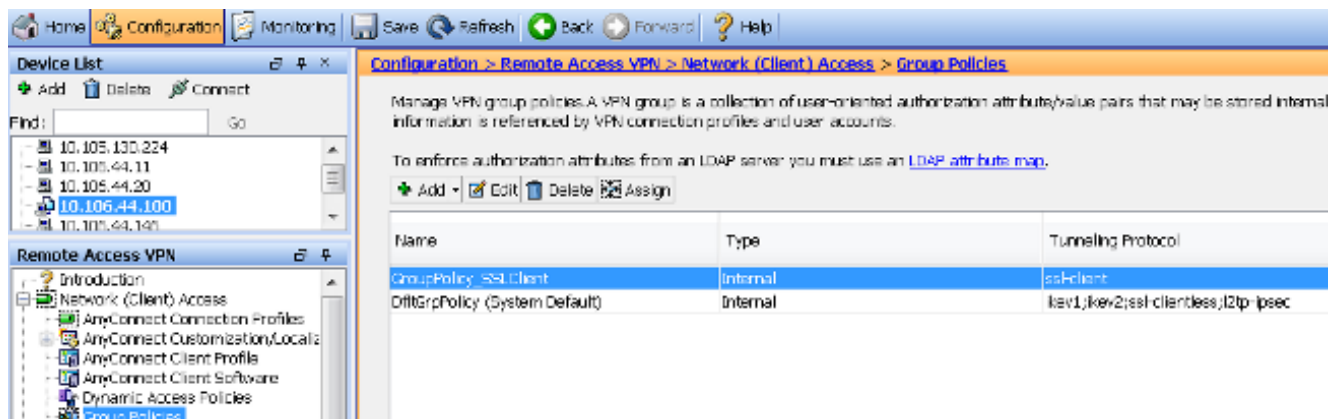
Somente o tráfego destinado ao endereço IP de WAN (ou *externo*) do ASA será desviado do túnel no computador cliente. Isso pode ser observado na saída do comando **route print** nos computadores Microsoft Windows.

Configuração de túnel dividido

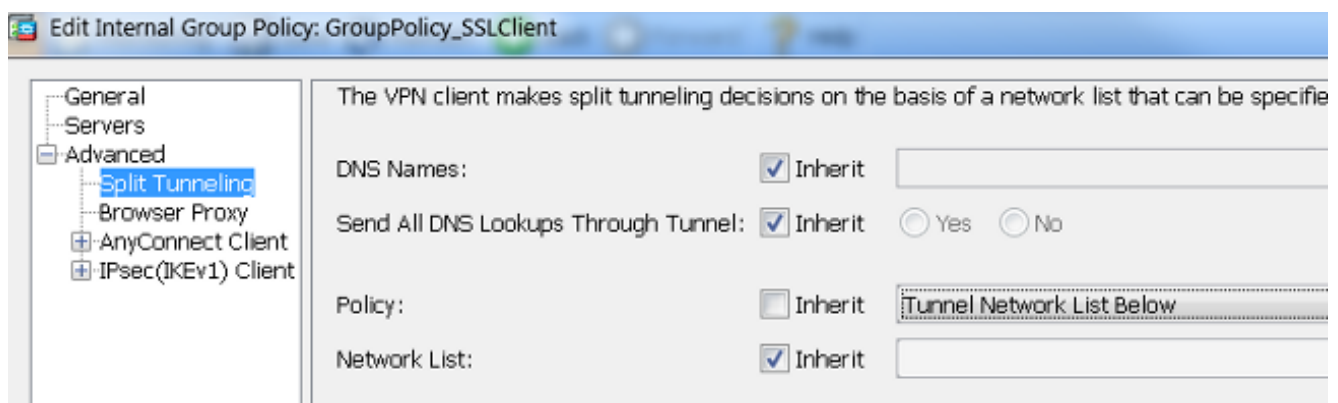
O túnel dividido é um recurso que você pode usar para definir o tráfego para as sub-redes ou os hosts que devem ser criptografados. Isso envolve a configuração de uma lista de controle de acesso (ACL) que será associada a esse recurso. O tráfego para as sub-redes ou os hosts definidos nessa ACL será criptografado pelo túnel do lado do cliente e as rotas para essas sub-redes serão instaladas na tabela de roteamento do PC.

Siga estas etapas para migrar da configuração de *Tunnel-all* para a configuração de *Split-tunnel*:

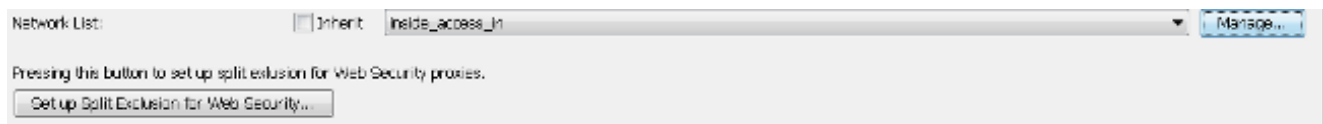
1. Navegue até **Configuração > VPN de acesso remoto > Políticas de grupo**:



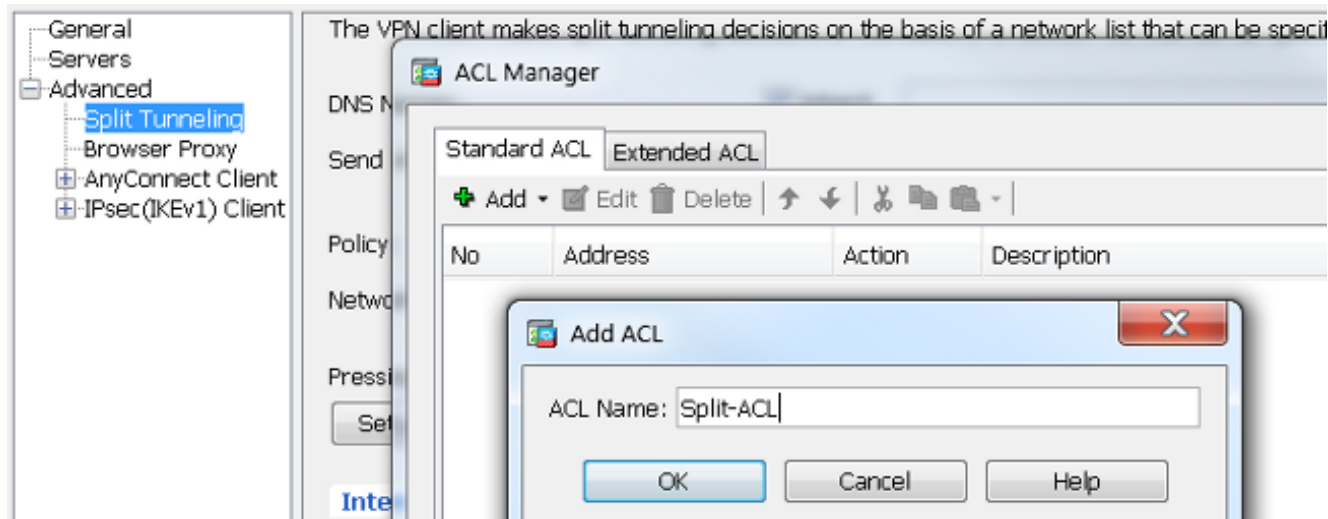
2. Clique em **Editar** e use a árvore de navegação para ir até **Avançado > Túnel dividido**. Desmarque a caixa de seleção **Herdar** na seção *Política* e selecione **Lista de redes de túnel abaixo** no menu suspenso:



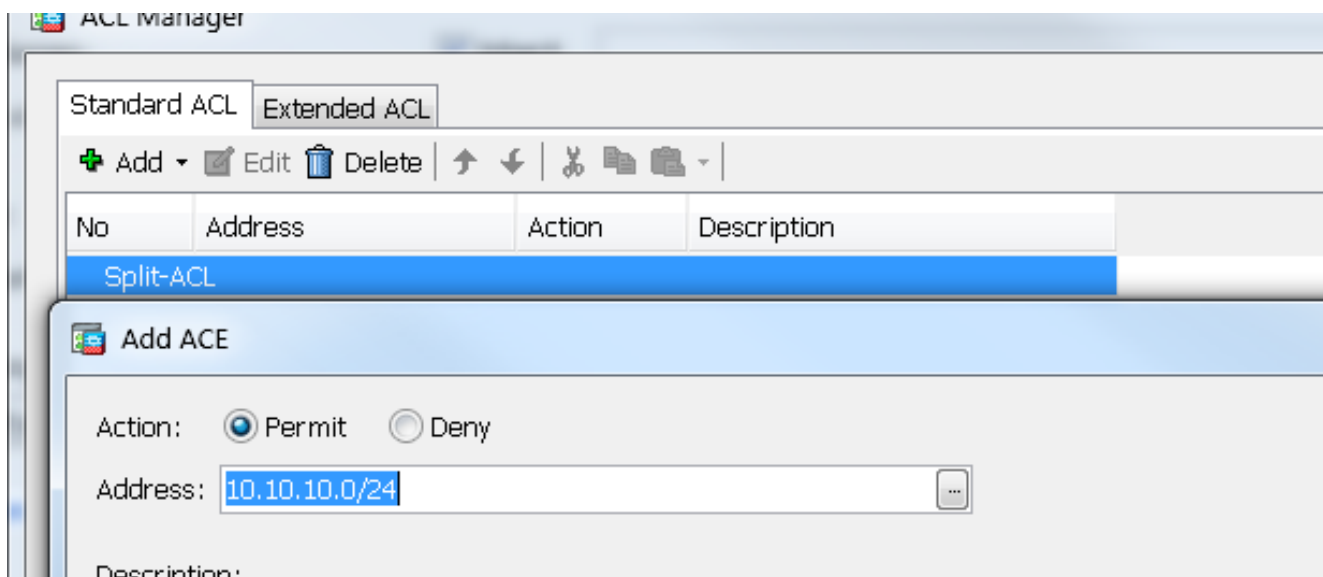
3. Desmarque a caixa de seleção **Herdar** na seção *Lista de redes* e clique em **Gerenciar** para selecionar a ACL que especifica as redes de LAN que o cliente precisa acessar:



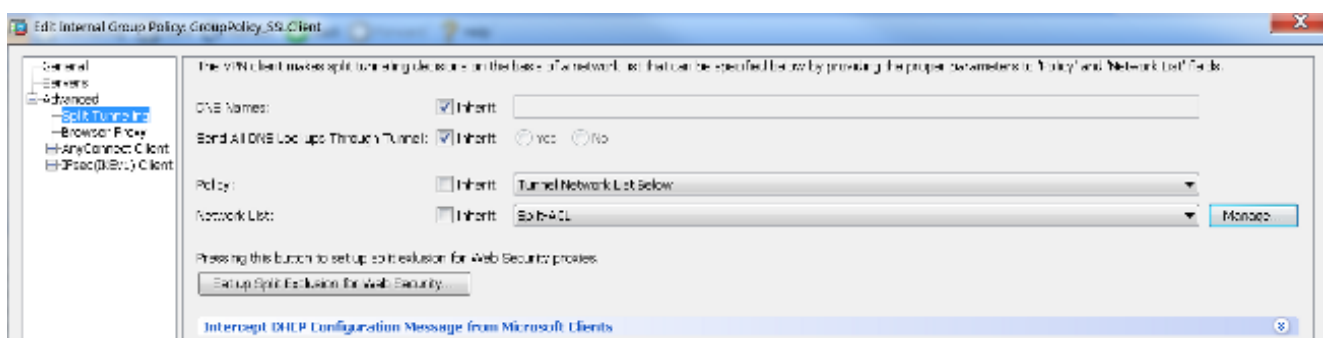
4. Clique em **ACL padrão, Adicionar, Adicionar ACL** e, em seguida, **Nome da ACL**:



5. Clique em **Adicionar ACE** para adicionar a regra:



6. Click **OK**.



7. Clique em Apply.

Depois de conectadas, as rotas para as sub-redes ou os hosts na ACL dividida são adicionadas à tabela de roteamento do computador cliente. Em computadores Microsoft Windows, isso pode ser visualizado na saída do comando **route print**. O próximo salto para essas rotas será um endereço IP da sub-rede do pool IP do cliente (geralmente o primeiro endereço IP da sub-rede):

```
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.
```

Em computadores com o SO MAC, insira o comando **netstat -r** para visualizar a tabela de roteamento do 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.
```

Baixe e instale o AnyConnect Client

Há dois métodos que podem ser usados para implantar o Cisco AnyConnect Secure Mobility Client no computador do usuário:

- Implantação na Web
- Implantação autônoma

Esses dois métodos são explicados com mais detalhes nas seções a seguir.

Implantação na Web

Para usar o método de implantação na Web, insira o **https://<ASA's FQDN>** ou o **<ASA's IP>URL** em um navegador no computador cliente, o que leva você para a página do portal *WebVPN*.

Note: Se o Internet Explorer (IE) for usado, a instalação será concluída principalmente por meio do ActiveX, a menos que você seja obrigado a usar o Java. Todos os outros

navegadores usam o Java.

Depois de fazer login na página, a instalação deve começar no computador cliente e o cliente deve se conectar ao ASA após a conclusão da instalação.

Note: Você pode ser solicitado a fornecer permissão para executar o ActiveX ou o Java. Você deve fornecer a permissão para continuar a instalação.

Logon	
Group	SSLClient ▼
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Logon"/>	



CISCO AnyConnect Secure Mobility Client

WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Java
- Download
- Connected

Attempting to use Java for Installation

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

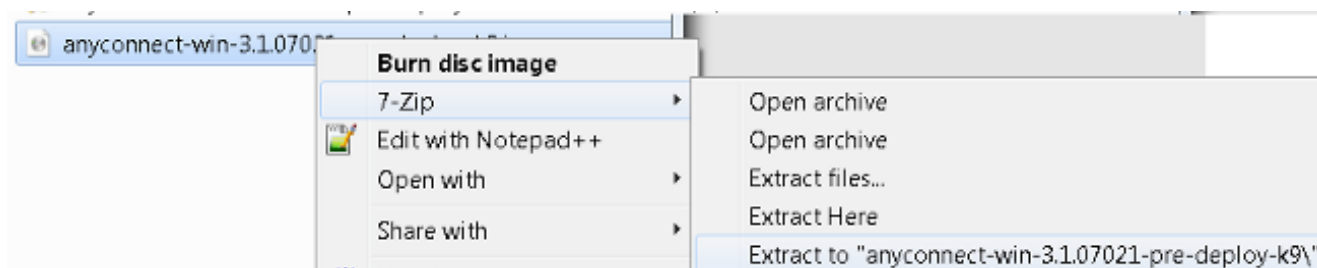
Implantação autônoma

Siga estas etapas para usar o método de implantação autônomo:

1. Baixe a imagem do AnyConnect Client no site da Cisco. Para escolher a imagem correta para download, consulte a página da Web [Cisco AnyConnect Secure Mobility Client](#). Um link

de download é fornecido nesta página. Navegue até a página de download e selecione a versão apropriada. Pesquise o **pacote de instalação Completo - Windows / Instalador Autônomo (ISO)**. **Note:** Uma imagem do instalador ISO é baixada (como *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).

2. Use o *WinRar* ou o *7-Zip* para extrair o conteúdo do pacote ISO:



3. Depois que o conteúdo for extraído, execute o arquivo **Setup.exe** e escolha os módulos que devem ser instalados em conjunto com o Cisco AnyConnect Secure Mobility Client.

Tip: Para definir as configurações adicionais da VPN, consulte a seção [Configuração das conexões do cliente VPN do AnyConnect](#) do *Guia de configuração do Cisco ASA 5500 Series usando a CLI, 8.4 e 8.6*.

Configuração de CLI

Essa seção fornece a configuração de CLI para o Cisco AnyConnect Secure Mobility Client para fins de referência.

```
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*****
!Generate the key pair and then configure the trustpoint
!Enroll the trustpoint generate 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 dl32a360 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 bala5541 ed719680 ee49abe8
```

quit

telnet timeout 5

ssh timeout 5

ssh key-exchange group dh-group1-shal

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-shal 3des-shal aes128-shal aes256-shal

*!***** 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, Split 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

```

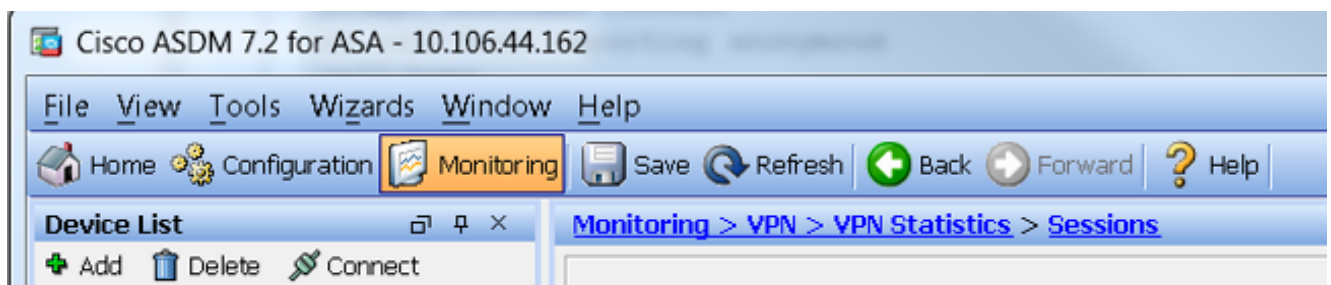
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum: 8d492b10911d1a8fbcc93aa4405930a0
: end

```

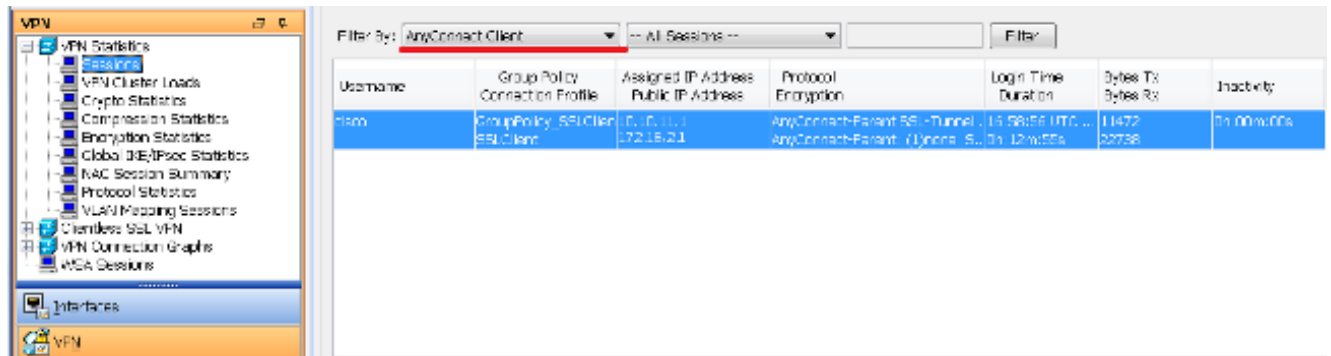
Verificar

Siga estas etapas para verificar a conexão do cliente e os vários parâmetros associados a essa conexão:

1. Navegue até **Monitoramento > VPN** no ASDM:



2. Você pode usar a opção **Filtrar por** para filtrar o tipo de VPN. Selecione **AnyConnect Client** no menu suspenso e em todas as sessões do AnyConnect Client. **Tip:** As sessões podem ser filtradas ainda mais com outros critérios, como *nome do usuário* e *endereço IP*.



3. Clique duas vezes em uma sessão para obter mais detalhes sobre essa sessão específica:

Username	Group Policy Connection Profile	Assigned IP Address	Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Inactivity
cisco	GroupPolicy_SSLClient	10.10.11.1	172.16.21.1	AnyConnect-Parent SSL-Tunnel	16:58:56 UTC ...	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. Insira o comando **show vpn-sessiondb anyconnect** na CLI para obter os detalhes da sessão:

```
# 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. Você pode usar as outras opções de filtro para refinar os 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

Você pode usar o AnyConnect Diagnostics and Reporting Tool (DART) para coletar os dados que são úteis para solucionar problemas de instalação e conexão do AnyConnect. O Assistente DART é usado no computador que executa o AnyConnect. O DART reúne os registros, o status e as informações de diagnóstico para a análise do Cisco Technical Assistance Center (TAC) e não exige os privilégios de administrador para ser executado no computador cliente.

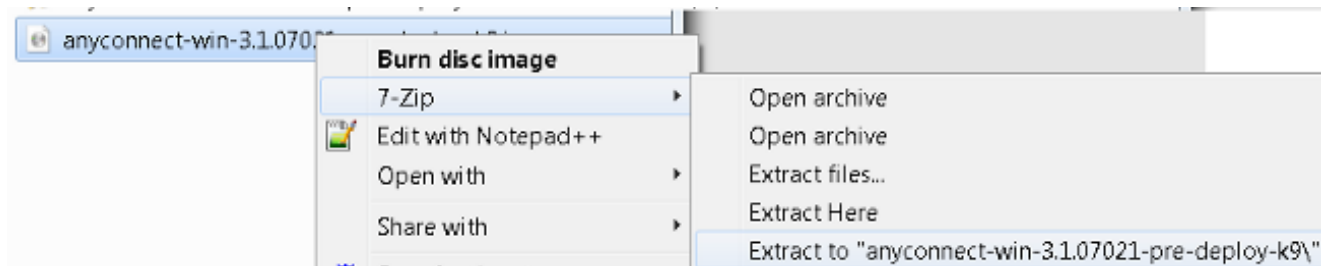
Instale o DART

Siga estas etapas para instalar o DART:

1. Baixe a imagem do AnyConnect Client no site da Cisco. Para escolher a imagem correta para download, consulte a página da Web [Cisco AnyConnect Secure Mobility Client](#). Um link de download é fornecido nesta página. Navegue até a página de download e selecione a

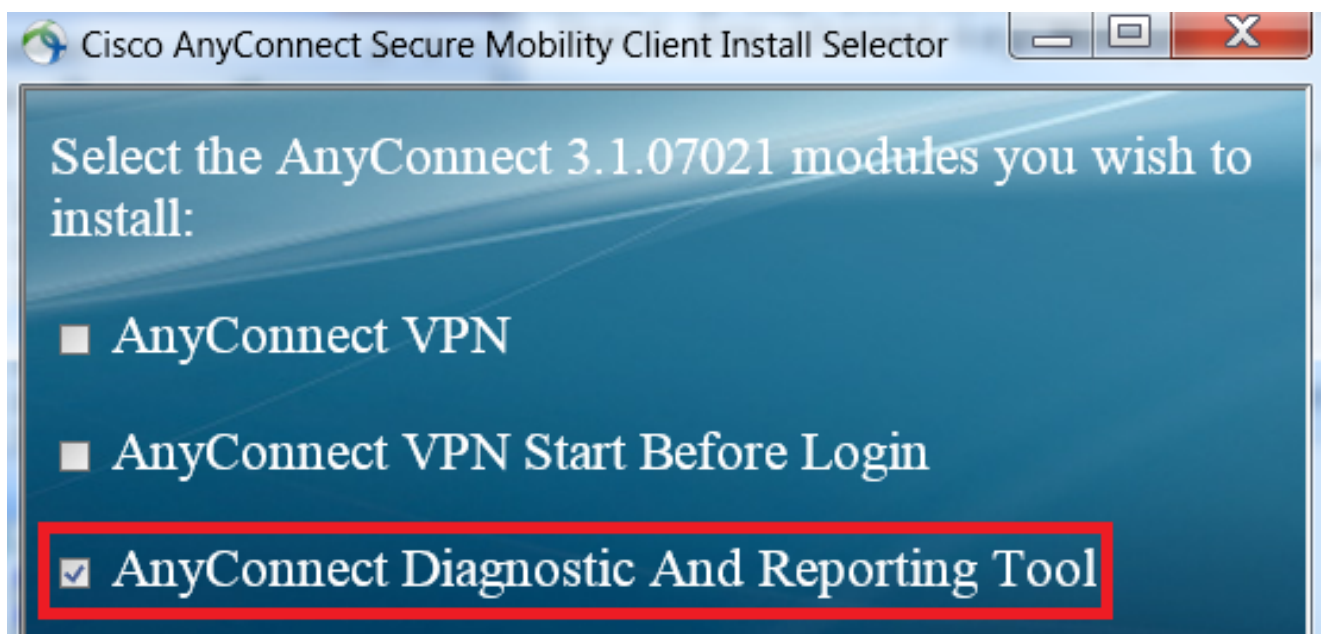
versão apropriada. Pesquise o **pacote de instalação Completo - Windows / Instalador Autônomo (ISO)**. **Note:** Uma imagem do instalador ISO é baixada (como *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).

2. Use o *WinRar* ou o *7-Zip* para extrair o conteúdo do pacote ISO:



3. Navegue até a pasta para a qual o conteúdo foi extraído.

4. Execute o arquivo **Setup.exe** e selecione apenas a **ferramenta de diagnóstico e relatório do Anyconnect**:

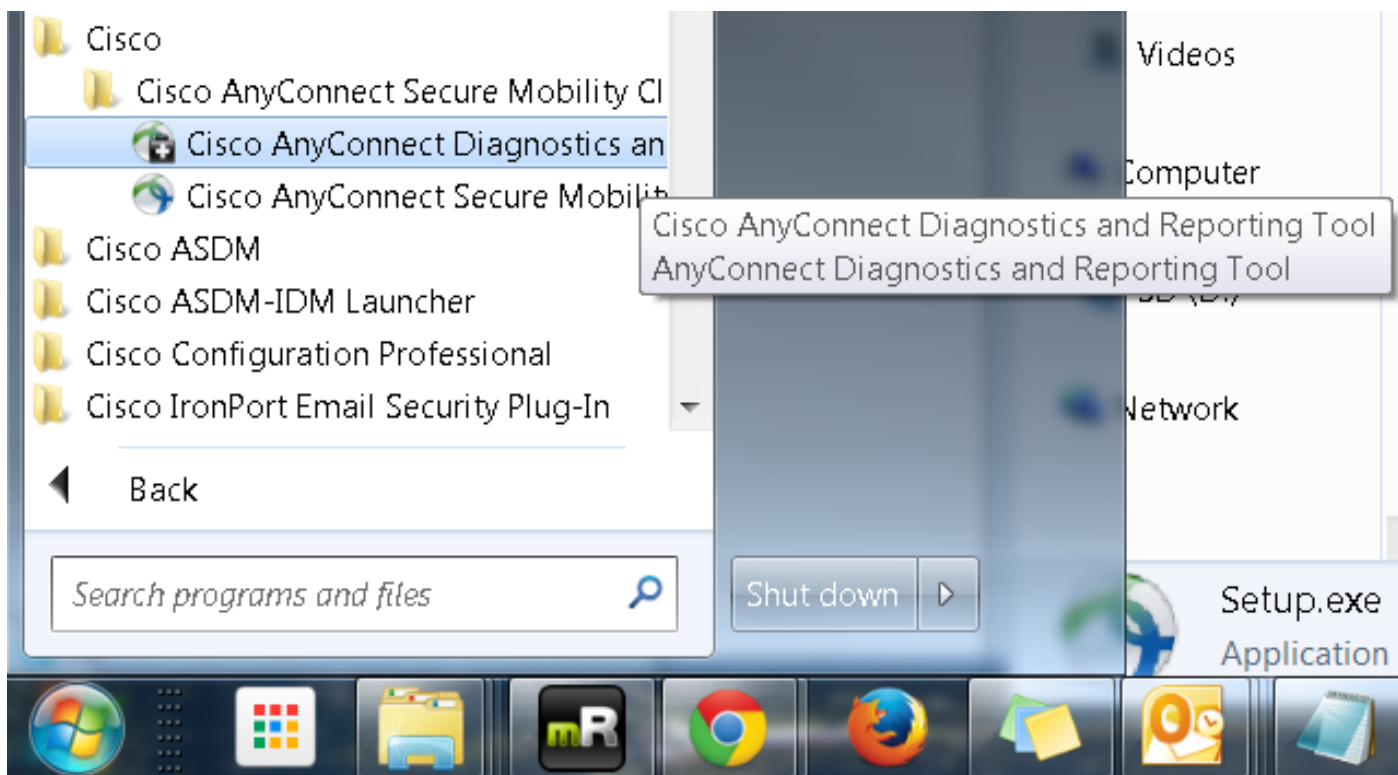


Execute o DART

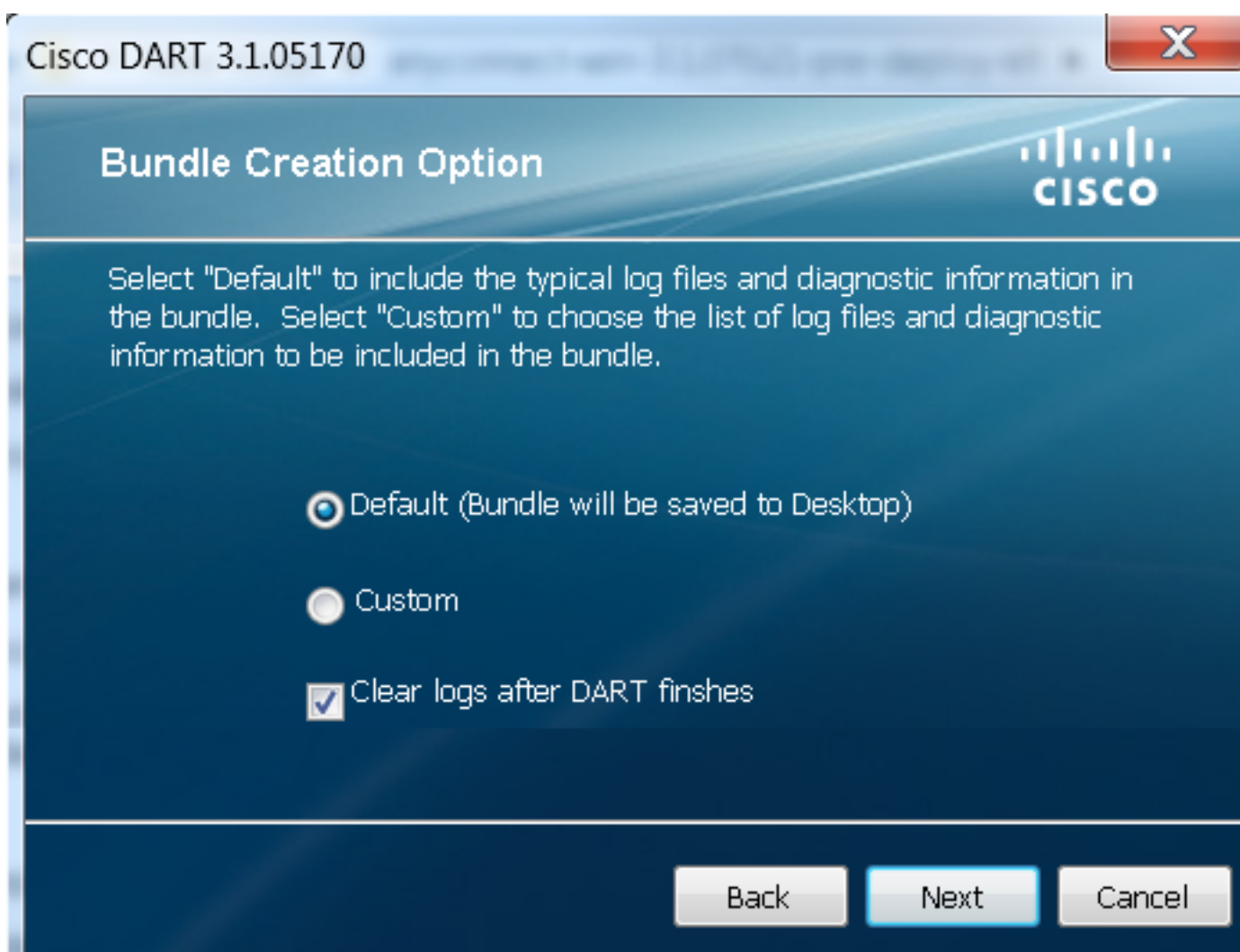
Estas são algumas informações importantes a serem consideradas antes de executar o DART:

- O problema deve ser recriado pelo menos uma vez antes de você executar o DART.
- A data e a hora no computador do usuário devem ser observadas quando o problema for recriado.

Execute o DART no *menu Iniciar* no computador cliente:



O modo *Padrão* ou *Personalizado* pode ser selecionado. A Cisco recomenda que você execute o DART no modo *Padrão* para que todas as informações possam ser capturadas de uma só vez.



Depois de concluída, a ferramenta salva o arquivo *.zip* do pacote do DART no desktop cliente. O

pacote pode ser enviado por e-mail para o TAC (depois que você abrir um caso de TAC) para uma análise posterior.

Informações Relacionadas

- [Guia de solução de problemas do cliente AnyConnect VPN - Problemas comuns](#)
- [Problemas do Java 7 com AnyConnect, CSD/Hostscan e WebVPN – Guia de solução de problemas](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.