

Configurer le client sécurisé avec le split tunneling sur un ASA

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Renseignements sur la licence AnyConnect](#)

[Configurer](#)

[Diagramme du réseau](#)

[Assistant de configuration AnyConnect par ASDM](#)

[Configuration du tunnel fractionné](#)

[Télécharger et installer le client AnyConnect](#)

[Déploiement sur le Web](#)

[Déploiement autonome](#)

[Configuration CLI](#)

[Vérifier](#)

[Dépannage](#)

[Installer DART](#)

[Exécuter DART](#)

Introduction

Ce document décrit comment configurer le client Cisco AnyConnect Secure Mobility via l'ASDM sur un Cisco ASA qui exécute la version 9.16.1 du logiciel.

Conditions préalables

Exigences

Le package de déploiement Web du client Cisco AnyConnect Secure Mobility peut être téléchargé sur le bureau local à partir duquel l'accès Cisco Adaptive Security Device Manager (ASDM) à l'appliance Cisco Adaptive Security (ASA) est disponible. Pour télécharger l'ensemble client, consultez la page Web du [client pour la mobilité sécurisée Cisco AnyConnect](#). Les packages de déploiement Web pour différents systèmes d'exploitation (OS) peuvent être téléchargés vers l'ASA en même temps.

Voici les noms de fichier du déploiement sur le Web pour les divers systèmes d'exploitation :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document fournit des détails étape par étape sur la façon d'utiliser l'Assistant de configuration Cisco AnyConnect via l'ASDM afin de configurer le client AnyConnect et d'activer la tunnellation partagée.

Le tunnel fractionné est utilisé dans les scénarios où seul un trafic bien précis doit faire l'objet de la tunnellation, contrairement aux scénarios où tout le trafic généré par la machine cliente transite par le VPN au moment de la connexion.

L'utilisation de l'assistant de configuration AnyConnect peut par défaut entraîner une configuration tunnel-all sur l'ASA. La tunnellation fractionnée doit être configurée séparément, ce qui est expliqué plus en détail dans le présent document, dans la section qui traite de la tunnellation fractionnée.

Dans cet exemple de configuration, l'objectif consiste à acheminer du trafic pour le sous-réseau 10.10.10.0/24, qui est le sous-réseau LAN derrière l'ASA, sur le tunnel VPN. De plus, tout autre trafic provenant de la machine cliente est acheminé par son propre circuit Internet.

Renseignements sur la licence AnyConnect

Voici des liens vers des renseignements utiles sur les licences du client pour la mobilité sécurisée Cisco AnyConnect :

- Reportez-vous au document [Cisco AnyConnect Licensing Frequently Asked Questions \(FAQ\)](#) afin de déterminer les licences requises pour AnyConnect Secure Mobility Client et

les fonctionnalités associées.

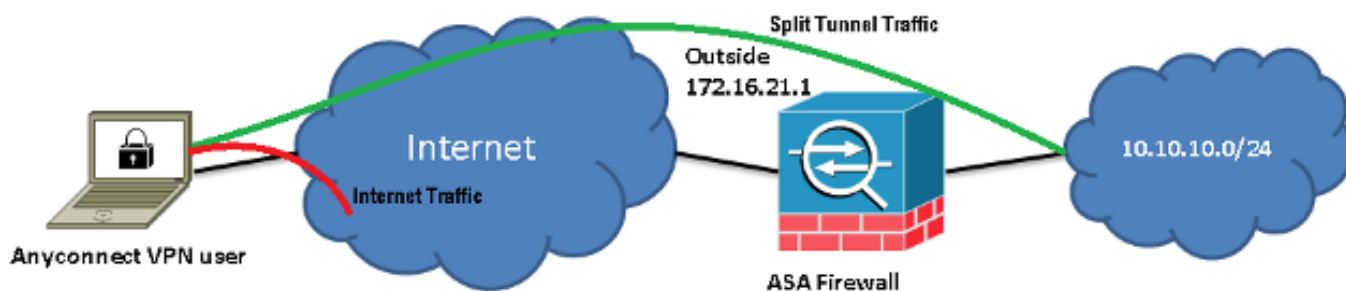
- Reportez-vous au [Guide de commande Cisco Secure Client](#) pour obtenir des informations sur les licences.

Configurer

Cette section décrit comment configurer le client sécurisé Cisco sur l'ASA.

Diagramme du réseau

Voici la topologie utilisée dans les exemples du présent document :

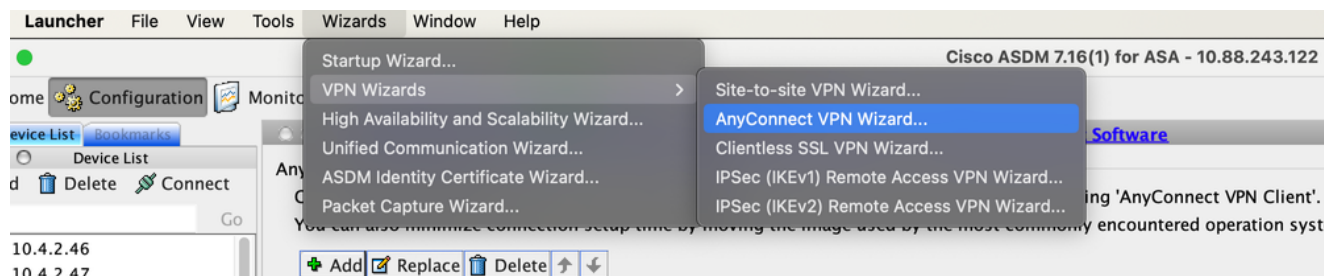


Assistant de configuration AnyConnect par ASDM

L'assistant de configuration AnyConnect peut être utilisé pour configurer le client pour la mobilité sécurisée Cisco AnyConnect. Assurez-vous qu'un paquet client AnyConnect a été chargé sur le disque ou la mémoire flash du pare-feu ASA avant de poursuivre.

Suivez ces étapes pour configurer le client pour la mobilité sécurisée AnyConnect avec l'aide de l'assistant de configuration :

1. Connectez-vous à l'ASDM, lancez ensuite l'assistant de configuration, puis cliquez sur Next [suivant] :



2. Saisissez le nom du profil de connexion, choisissez l'interface sur laquelle le VPN est terminé dans le menu déroulant VPN Access Interface, et cliquez sur Next :

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. **Connection Profile Identification**
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuratic
7. Client Address Assignment
8. Network Name Resolution Servers
9. NAT Exempt
10. AnyConnect Clie Deployment
11. Summary

Connection Profile Identification

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

Connection Profile Name:

VPN Access Interface:

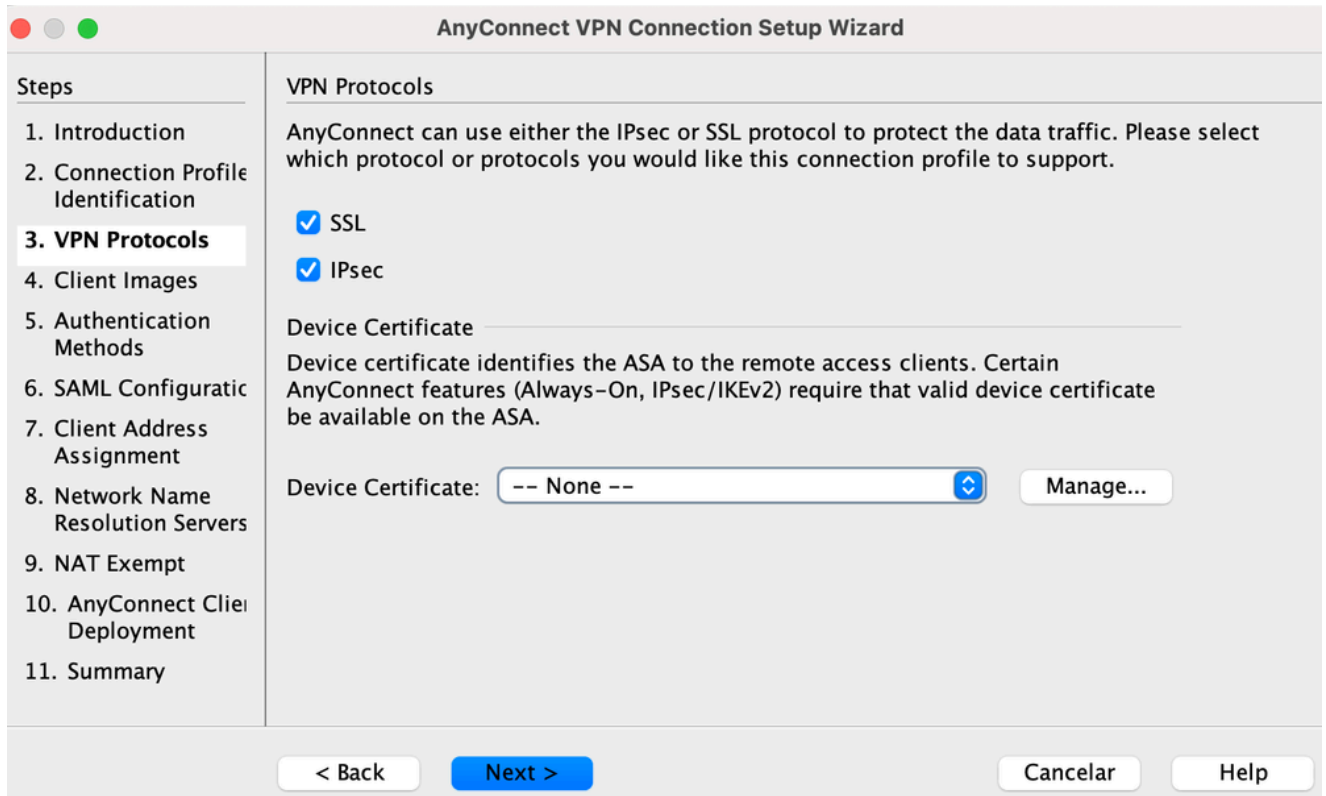
< Back Next > Cancelar Help

3. Cochez la case SSL pour activer le protocole SSL (Secure Sockets Layer). Le certificat de périphérique peut être un certificat émis par une autorité de certification (CA) tierce de confiance (p. ex., Verisign ou Entrust) ou un certificat autosigné. Si le certificat est déjà installé sur l'ASA, vous pouvez alors le sélectionner dans le menu déroulant.



Remarque : ce certificat est le certificat côté serveur qui est fourni. Si aucun certificat n'est actuellement installé sur l'ASA et qu'un certificat autosigné doit être généré, cliquez sur Manage [gérer].

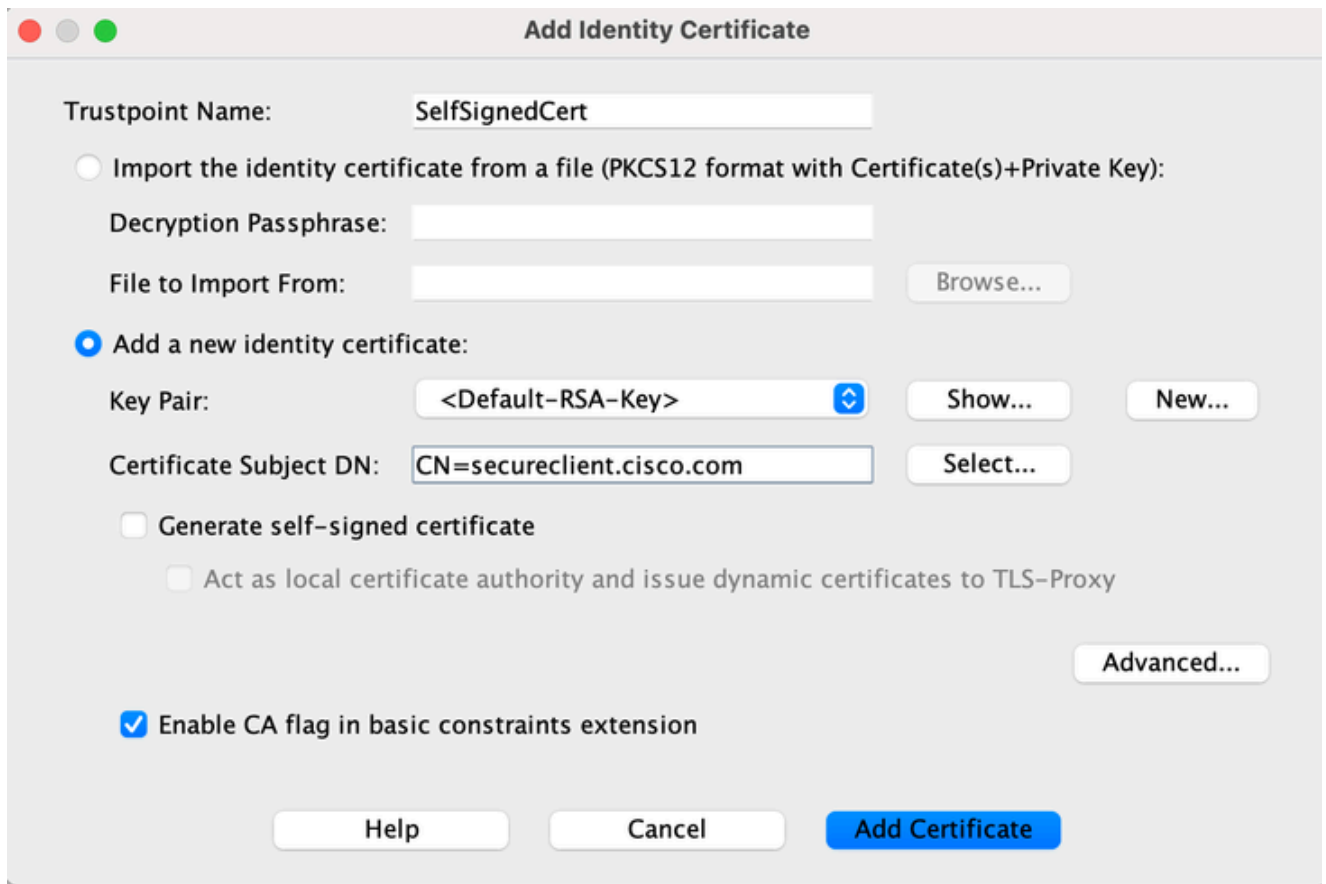
Afin d'installer un certificat tiers, complétez les étapes qui sont décrites dans le document [Configurer ASA : SSL Digital Certificate Installation and Renewal](#) Cisco.



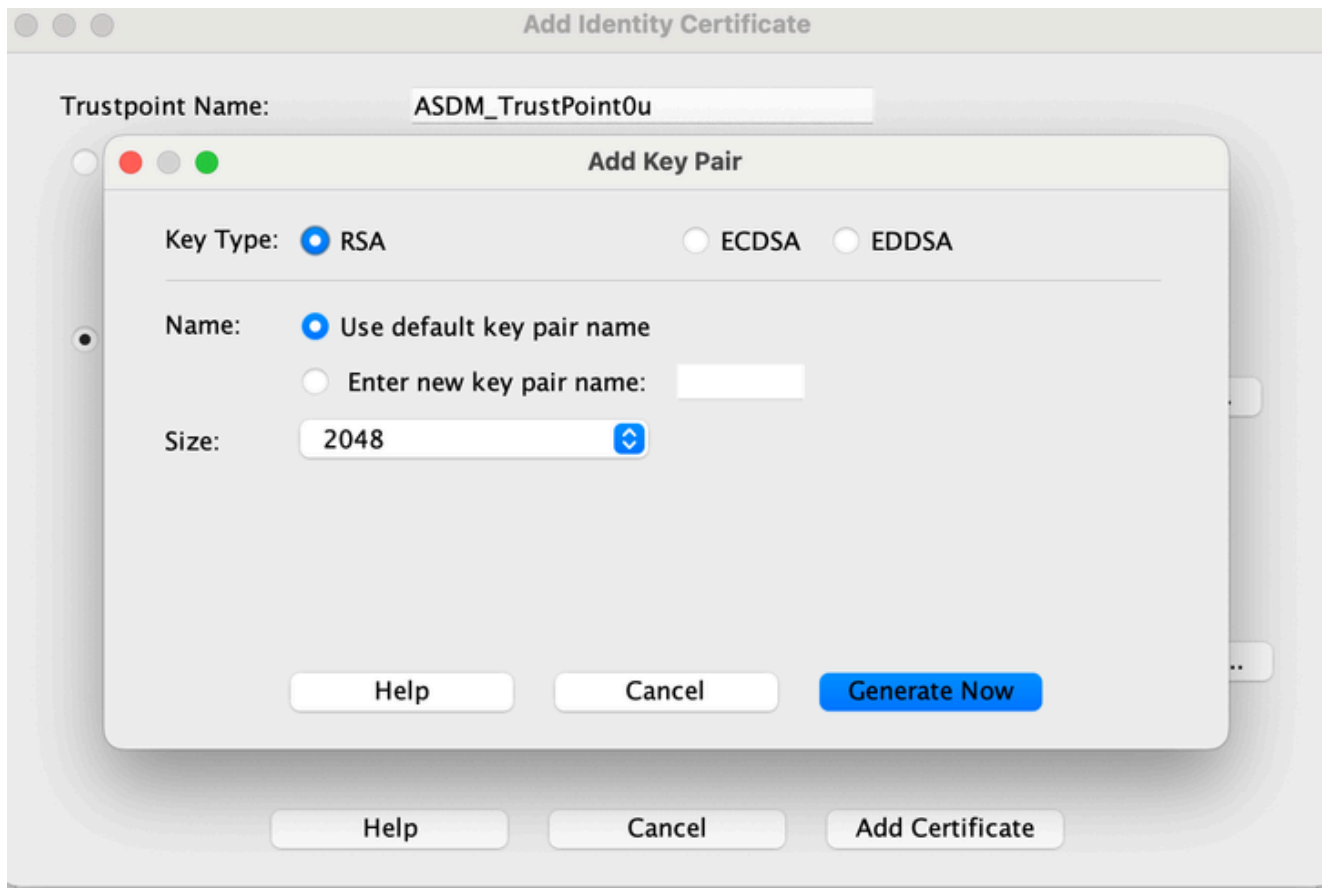
4. Cliquez sur Add [ajouter] :



5. Saisissez un nom approprié dans le champ Trustpoint Name [nom du point de confiance], puis cliquez sur le bouton radio Add a new identity certificate [ajouter un nouveau certificat d'identité]. Si aucune paire de clés Rivest-Shamir-Addleman (RSA) n'est présente sur l'appareil, cliquez sur New [nouveau] pour en générer une :



6. Activez la case d'option Utiliser le nom de la paire de clés par défaut ou cliquez sur la case d'option Entrer un nouveau nom de paire de clés, puis entrez un nouveau nom. Sélectionnez la taille des clés, puis cliquez sur Generate Now [générer maintenant] :



7. Lorsque la paire de clés RSA a été générée, sélectionnez la clé, puis cochez la case Generate self-signed certificate [générer un certificat autosigné]. Saisissez le nom de domaine (DN) du sujet souhaité dans le champ Certificate Subject DN [DN du sujet du certificat], puis cliquez sur Add Certificate [ajouter le certificat] :
8. Une fois l'inscription terminée, cliquez sur OK, encore sur OK, puis sur Next [suivant] :

Public CA Enrollment

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

[Enroll ASA SSL certificate with Entrust](#)

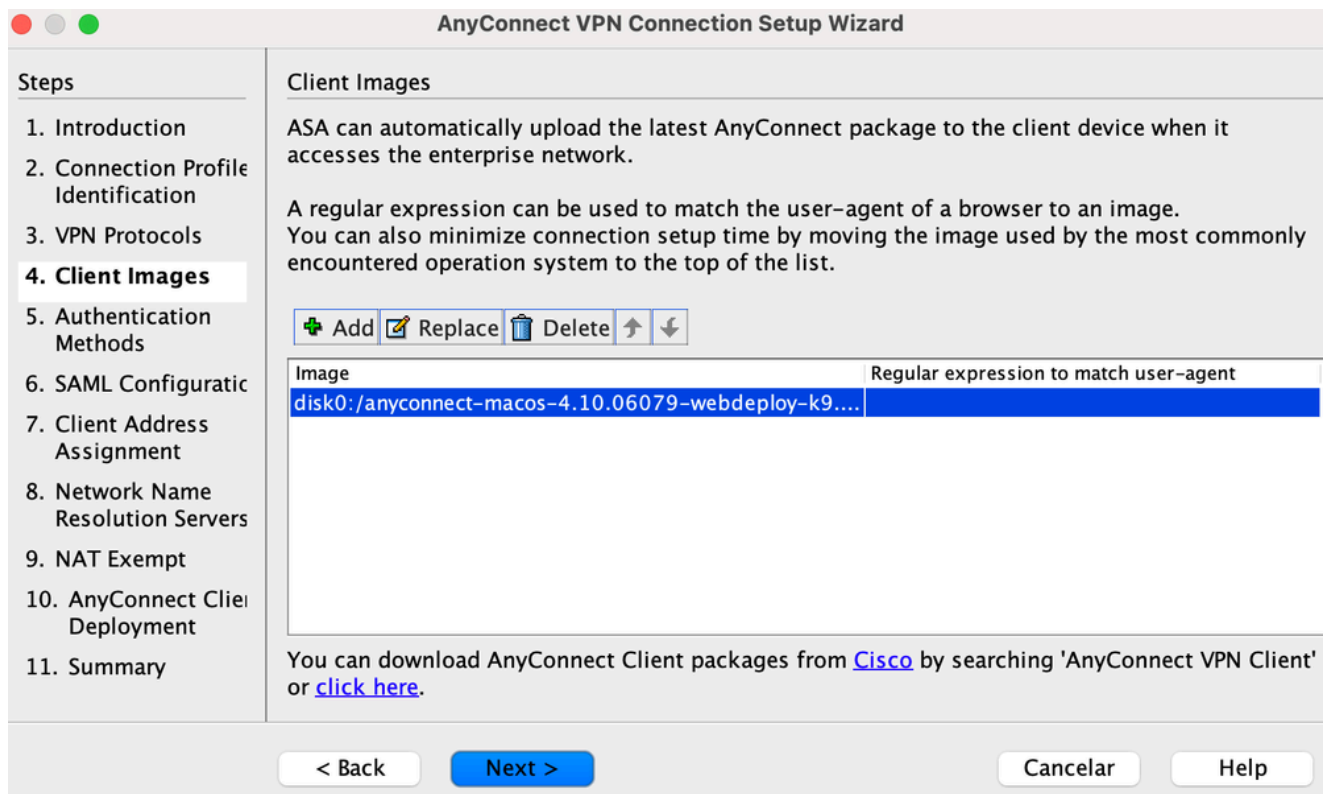
Using a previously saved certificate signing request, [enroll with Entrust](#).

ASDM Identity Certificate Wizard

The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.


[Launch ASDM Identity Certificate Wizard](#)

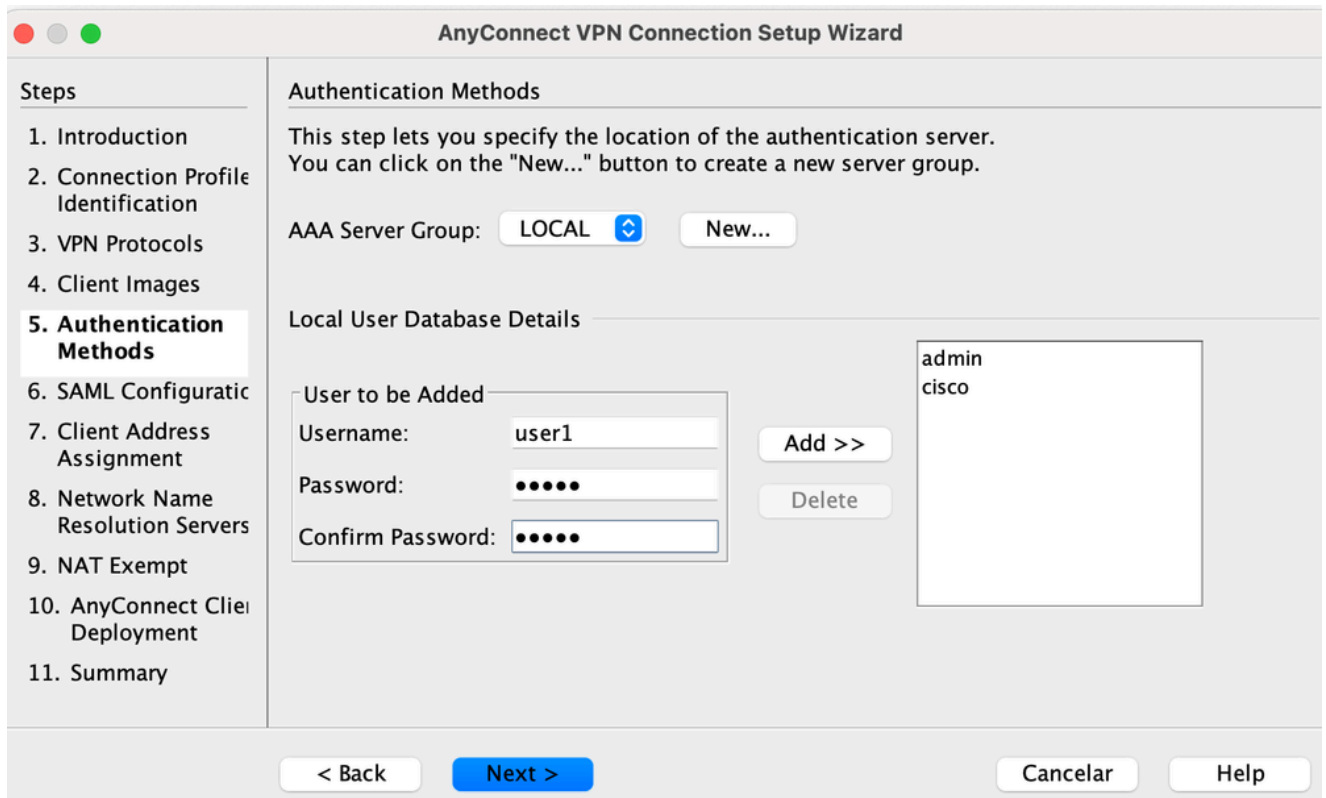
9. Cliquez sur Add [ajouter] pour ajouter l'image du client AnyConnect (le fichier .pkg) à partir de l'ordinateur ou du flash. Cliquez sur Browse Flash [parcourir le flash] pour ajouter l'image à partir du lecteur flash, ou cliquez sur Upload [charger] pour ajouter l'image directement à partir de la machine hôte :



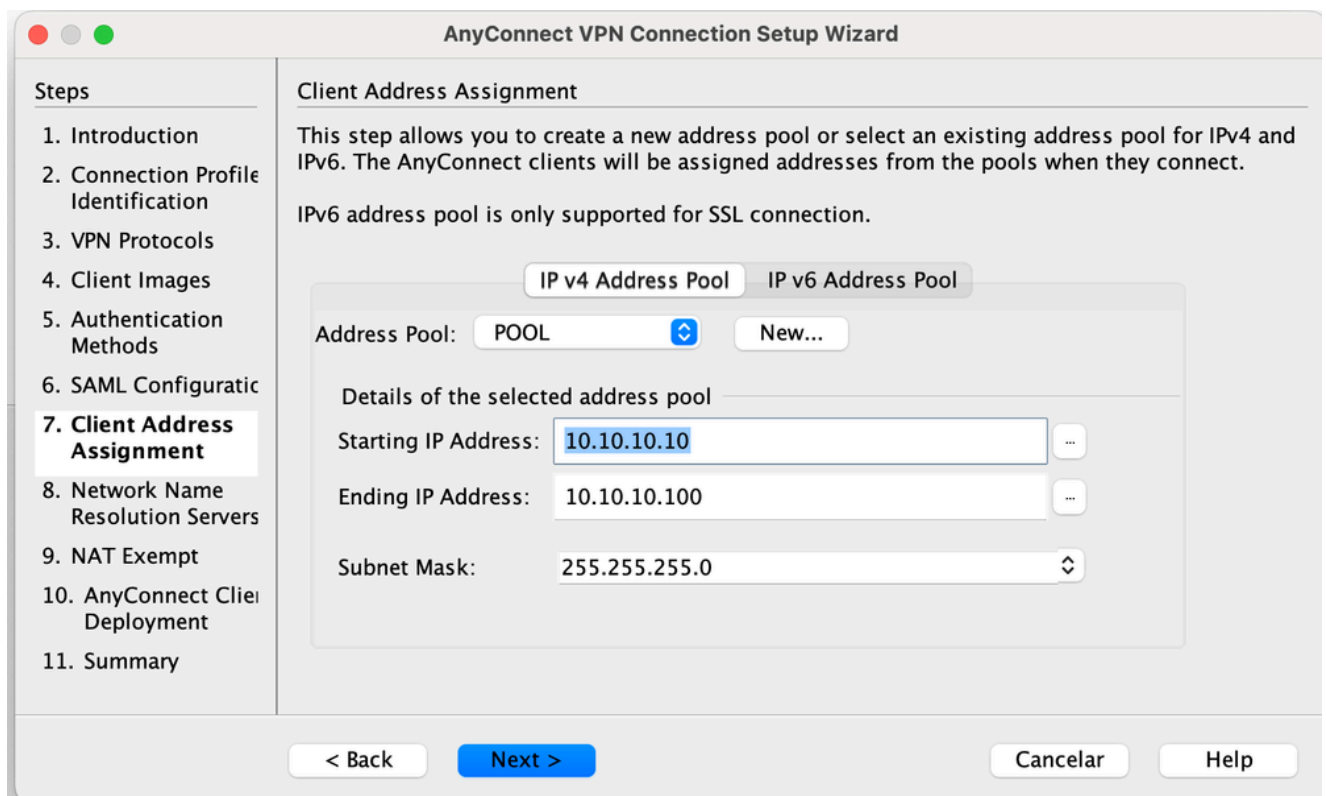
10. Une fois l'image ajoutée, cliquez sur Next [suivant] :

11. L'authentification de l'utilisateur peut être effectuée par les groupes de serveurs AAA (authentification, autorisation et administration). Si les utilisateurs sont déjà configurés, choisissez LOCA, puis cliquez sur Next (suivant).

 **Remarque :** dans cet exemple, l'authentification LOCAL est configurée, ce qui signifie que la base de données d'utilisateurs locaux sur l'ASA peut être utilisée pour l'authentification.



12. L'ensemble des adresses du client VPN doit être configuré. Si un élément est déjà configuré, sélectionnez-le dans le menu déroulant. Sinon, cliquez sur New [nouveau] pour en configurer un nouveau. Une fois terminé, cliquez sur Next [suivant] :

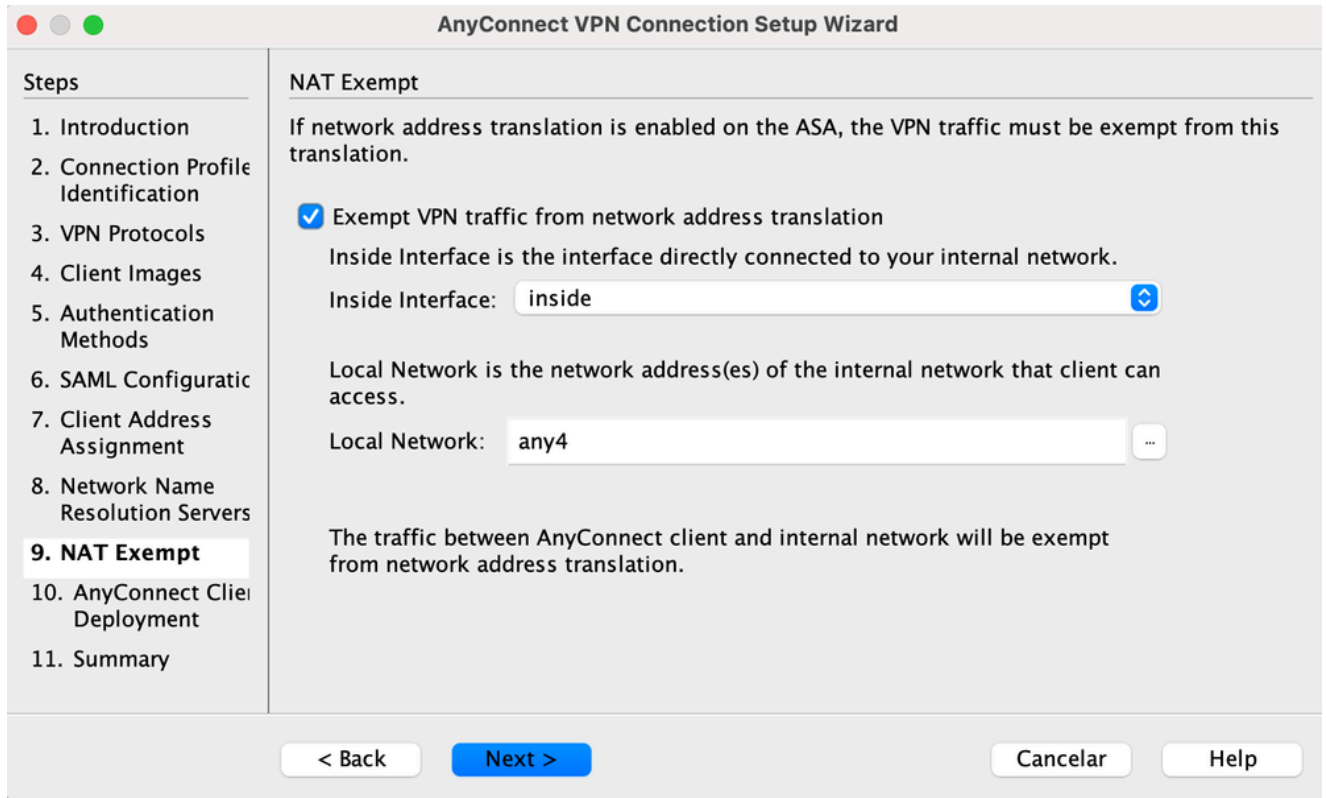


13. Saisissez les serveurs DNS et les noms de domaines dans les champs DNS et Domain Name [nom de domaine] correspondants, puis cliquez sur Next [suivant] :

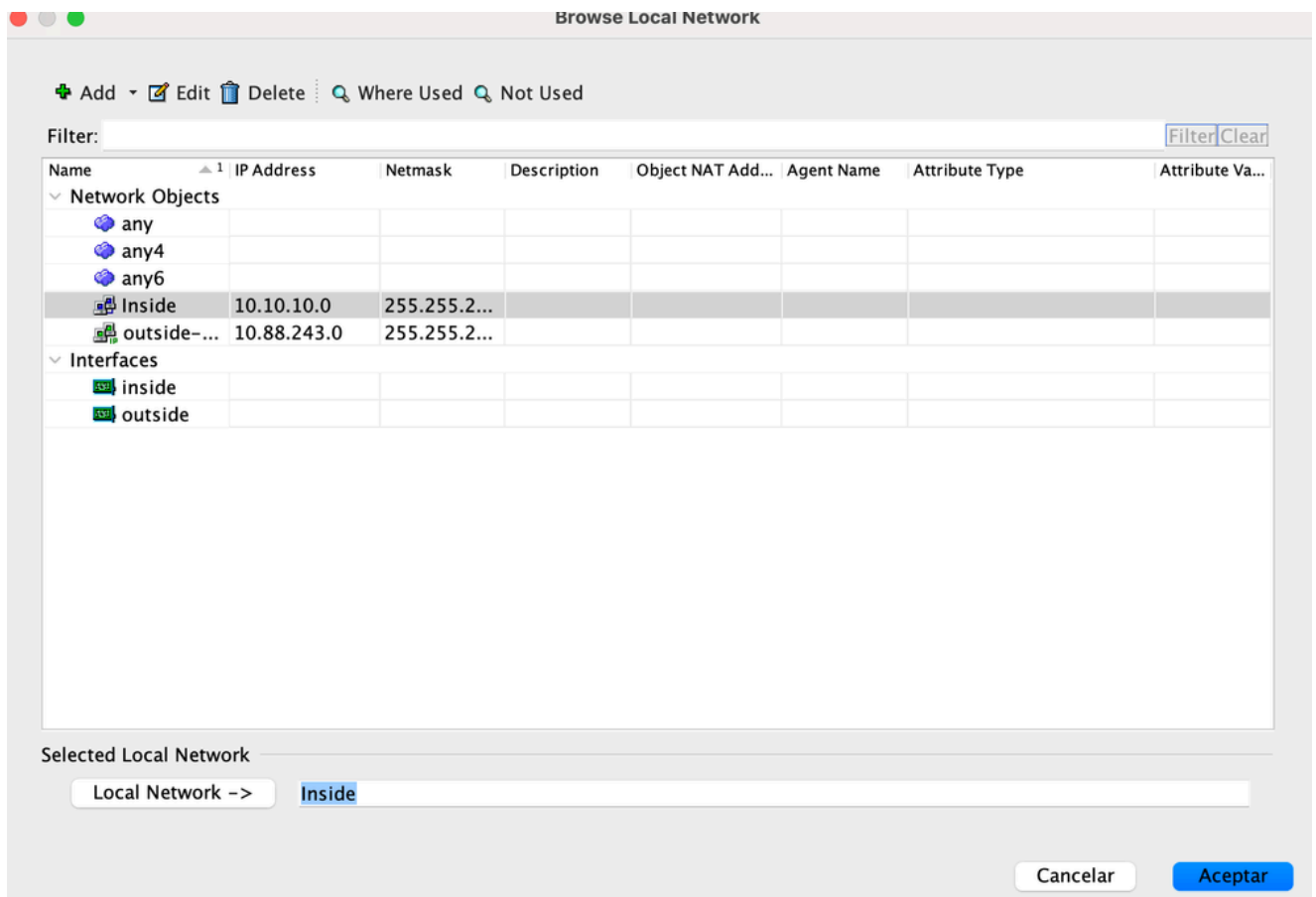
The screenshot shows a window titled "AnyConnect VPN Connection Setup Wizard". On the left, a "Steps" sidebar lists 11 steps, with step 8, "Network Name Resolution Servers", highlighted. The main area is titled "Network Name Resolution Servers" and contains the following text: "This step lets you specify how domain names are resolved for the remote user when accessing the internal network." Below this text are three input fields: "DNS Servers:" with the value "10.10.10.23", "WINS Servers:" which is empty, and "Domain Name:" with the value "Cisco.com". At the bottom of the window, there are four buttons: "< Back", "Next >" (highlighted in blue), "Cancelar", and "Help".

14. Dans ce scénario, l'objectif est de limiter l'accès par le VPN au réseau 10.10.10.0/24 configuré comme sous-réseau interne (ou LAN) derrière l'ASA. Le trafic entre le client et le sous-réseau interne doit être exempté de toute traduction d'adresse réseau (NAT) dynamique.

Cochez la case Exempt VPN traffic from network address translation et configurez les interfaces LAN et WAN qui peuvent être utilisées pour l'exemption :




15. Choisissez les réseaux locaux à exempter :



16. Cliquez sur Next [suivant], encore sur Next [suivant], puis sur Finish [terminer].

Vous avez terminé la configuration du client AnyConnect. Toutefois, lorsque vous configurez AnyConnect à l'aide de l'Assistant de configuration, il configure la politique tunnel fractionné, comme Tunnelall, par défaut. Afin que seul un trafic précis fasse l'objet d'une tunnellation, il faut mettre en œuvre le tunnel fractionné.

 Remarque : si la transmission tunnel partagée n'est pas configurée, la stratégie de tunnel partagé peut être héritée de la stratégie de groupe par défaut (DfltGrpPolicy), qui est par défaut définie sur TunnelAll. Ainsi, lorsque le client est connecté par VPN, tout le trafic (y compris le trafic Web) est transmis par le tunnel.

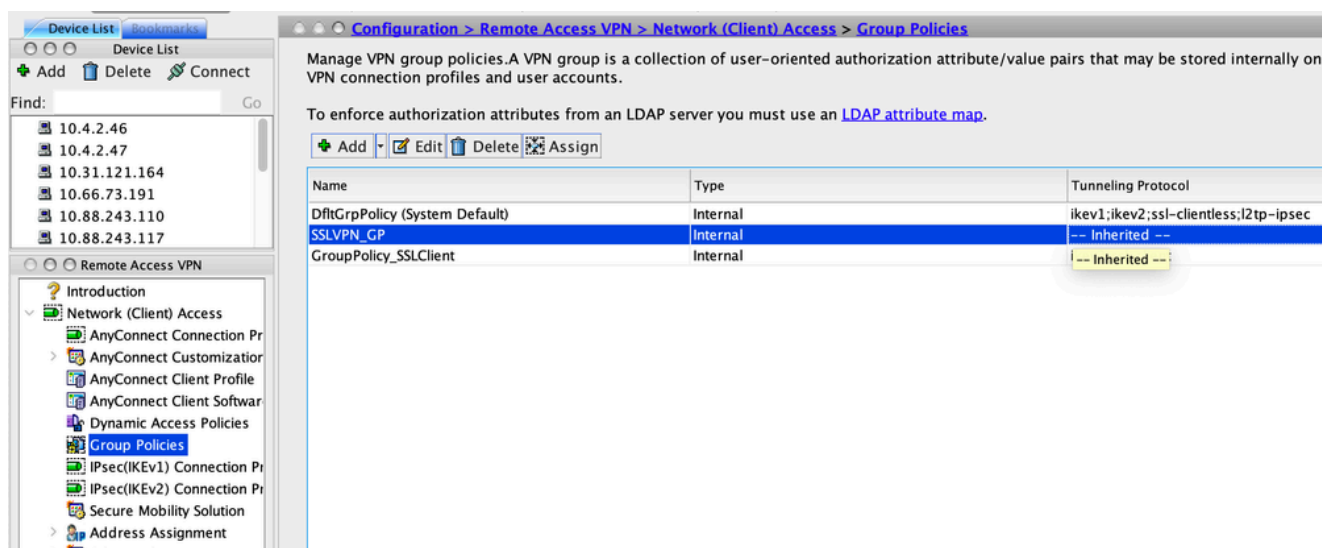
Seul le trafic destiné à l'adresse IP WAN (ou externe) ASA peut contourner la transmission tunnel sur l'ordinateur client. On peut observer cela dans le résultat de la commande route print sur les machines Microsoft Windows.

Configuration du tunnel fractionné

La tunnellation fractionnée est une fonction que vous pouvez utiliser pour définir le trafic des sous-réseaux ou des hôtes à chiffrer. Cela implique la configuration d'une liste de contrôle d'accès (ACL) qui peut être associée à cette fonctionnalité. Le trafic des sous-réseaux ou des hôtes qui est défini sur cette liste de contrôle d'accès peut être chiffré sur le tunnel à partir du client-end, et les routes pour ces sous-réseaux sont installées sur la table de routage du PC.

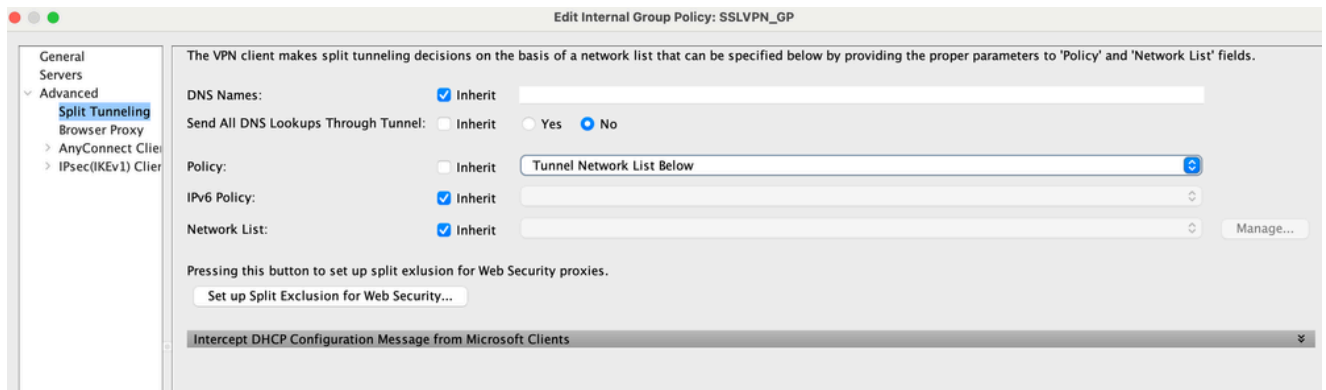
Suivez ces étapes pour passer de la configuration Tunnel-all [tunnel-tout] à la configuration Split-tunnel [tunnel-fractionné] :

1. Allez à Configuration > Remote Access VPN > Group Policies [configuration > VPN d'accès à distance > politiques de groupe] :

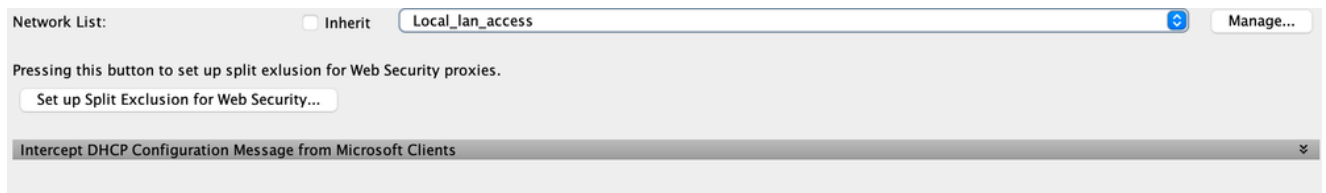


Name	Type	Tunneling Protocol
DfltGrpPolicy (System Default)	Internal	ikev1,ikev2,ssl-clientless,l2tp-ipsec
SSLVPN_GP	Internal	-- Inherited --
GroupPolicy_SSLClient	Internal	-- Inherited --

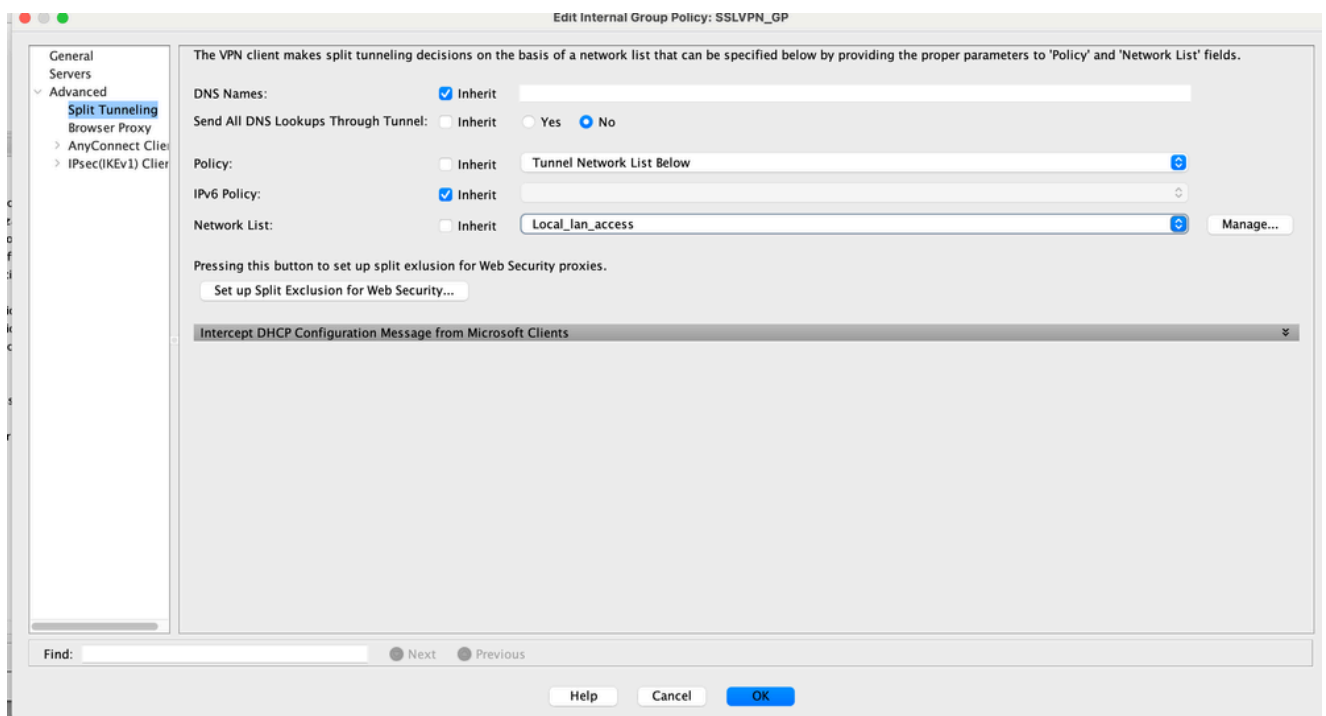
2. Cliquez sur Edit [modifier] et utilisez l'arborescence de navigation pour aller à Advanced > Split Tunneling [avancé > tunnellation fractionnée]. Décochez la case Inherit [hériter] dans la section Policy [politique], puis sélectionnez Tunnel Network List Below [liste des réseaux de tunnels ci-dessous] dans le menu déroulant :



3. Décochez la case Inherit [hériter] dans la section Network List [liste des réseaux], puis cliquez sur Manage [gérer] pour sélectionner l'ACL qui précise les réseaux LAN auxquels le client doit accéder :



4. Cliquez sur ACL standard, Ajouter, Ajouter ACL, puis sur ACL name.
5. Cliquez sur Add ACE afin d'ajouter la règle.
6. Click OK.



7. Cliquez sur Apply.

Une fois la connexion établie, les itinéraires des sous-réseaux ou des hôtes de l'ACL fractionnée sont ajoutés à la table de routage de la machine du client. On peut observer cela dans le résultat de la commande route print sur les machines Microsoft Windows. Le saut suivant pour ces routes peut être une adresse IP du sous-réseau du pool d'adresses IP client (généralement la première adresse IP du sous-réseau) :

<#root>

C:\Users\admin>

route print

IPv4 Route Table

=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	10.106.44.1	10.106.44.243	261

10.10.10.0	255.255.255.0	10.10.11.2	10.10.11.1	2
------------	---------------	------------	------------	---

!! This is the split tunnel route

10.106.44.0	255.255.255.0	On-link	10.106.44.243	261
-------------	---------------	---------	---------------	-----

172.16.21.1	255.255.255.255	On-link	10.106.44.243	6
-------------	-----------------	---------	---------------	---

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

Sur les machines MAC OS, entrez la commande netstat -r pour afficher la table de routage de l'ordinateur :

<#root>

\$

netstat -r

Routing tables

Internet:

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	hsrp-64-103-236-1.	UGSc	34	0	en1	
10.10.10/24	10.10.11.2	UGSc	0	44	utun1	

!! This is the split tunnel route

.

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

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

Télécharger et installer le client AnyConnect


Il existe deux méthodes pour déployer le client pour la mobilité sécurisée Cisco AnyConnect sur la machine de l'utilisateur :

- Déploiement sur le Web
- Déploiement autonome


Ces méthodes sont expliquées plus en détail dans les sections qui suivent.

Déploiement sur le Web

Si vous optez pour le déploiement sur le Web, saisissez l'adresse `https://<ASA's FQDN>ou<ASA's IP>` l'URL dans un navigateur sur la machine du client pour vous rendre à la page du portail WebVPN.

 Remarque : si Internet Explorer (IE) est utilisé, l'installation s'effectue principalement via ActiveX, sauf si vous êtes forcé d'utiliser Java. Tous les autres navigateurs utilisent Java.

Une fois connecté à la page, l'installation peut commencer sur l'ordinateur client et le client peut se connecter à l'ASA une fois l'installation terminée.

 Remarque : vous pouvez être invité à demander l'autorisation d'exécuter ActiveX ou Java. Il faut avoir l'autorisation pour procéder à l'installation.



Déploiement autonome

Voici la marche à suivre pour utiliser le déploiement autonome :

1. Téléchargez l'image du client AnyConnect sur le site Web de Cisco. Pour télécharger la bonne image, consultez la page Web [Cisco AnyConnect Secure Mobility Client](#). Un lien de téléchargement est fourni sur cette page. Accédez à la page de téléchargement, puis sélectionnez la version appropriée. Effectuez une recherche pour trouver l'intégralité du programme d'installation – programme d'installation autonome/Windows (ISO).

 Remarque : une image d'installation ISO est ensuite téléchargée (par exemple anyconnect-win-4.10.06079-pre-deploy-k9.iso).

2. Utilisez WinRar ou 7-Zip pour extraire le contenu du programme ISO :

3. Une fois le contenu extrait, exécutez le fichier Setup.exe et choisissez les modules à installer avec le client de mobilité sécurisée Cisco AnyConnect.

Configuration CLI

Cette section fournit la configuration de la CLI affectée au client pour la mobilité sécurisée Cisco AnyConnect à des fins de référence.

```
<#root>
```

```
ASA Version 9.16(1)
```

```
!
```

```
hostname PeerASA-29
```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
```

```
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
```



```
!  
interface GigabitEthernet0/0  
nameif outside  
security-level 0  
ip address 172.16.21.1 255.255.255.0  
!  
interface GigabitEthernet0/1  
nameif inside  
security-level 100  
ip address 10.10.10.1 255.255.255.0  
!  
boot system disk0:/asa916-smp-k8.bin  
ftp mode passive  
object network NETWORK_OBJ_10.10.10.0_24  
subnet 10.10.10.0 255.255.255.0  
object network NETWORK_OBJ_10.10.11.0_27  
subnet 10.10.11.0 255.255.255.224  
  
access-list all extended permit ip any any  
  
!*****Split ACL configuration*****  
  
access-list Split-ACL standard permit 10.10.10.0 255.255.255.0  
  
no pager  
logging enable  
logging buffered debugging  
mtu outside 1500  
mtu inside 1500  
mtu dmz 1500  
no failover  
icmp unreachable rate-limit 1 burst-size 1  
asdm image disk0:/asdm-7161.bin  
no asdm history enable  
arp timeout 14400  
no arp permit-nonconnected  
  
!***** NAT exemption Configuration *****  
!This can exempt traffic from Local LAN(s) to the  
!Remote LAN(s) from getting NATted on any dynamic NAT rule.  
  
nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24  
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp  
route-lookup  
  
access-group all in interface outside  
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1  
timeout xlate 3:00:00  
timeout pat-xlate 0:00:30  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00  
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00  
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute  
timeout tcp-proxy-reassembly 0:01:00  
timeout floating-conn 0:00:00  
dynamic-access-policy-record DfltAccessPolicy  
user-identity default-domain LOCAL  
aaa authentication ssh console LOCAL
```

```
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
```

```
!***** Trustpoint for Selfsigned certificate*****
!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 e2ddea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7
53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34
03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8
```

```
quit
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1-only
ssl encryption des-sha1 3des-sha1 aes128-sha1 aes256-sha1
```

```
!***** Bind the certificate to the outside interface*****
```

```
ssl trust-point SelfsignedCert outside
```

```
!*****Configure the Anyconnect Image and enable Anyconnect***
```

```
webvpn
```

```
enable outside
```

```
anyconnect image disk0:/anyconnect-win-4.10.06079-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

```
!*****Group Policy configuration*****
!Tunnel protocol, 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 3USUcOPFUiMC04Jk encrypted privilege 15
```

```
!*****Tunnel-Group (Connection Profile) Configuraiton*****
```

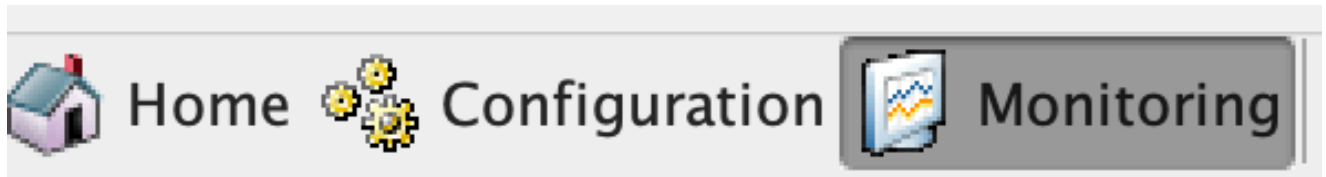
```
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
```

```
!
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
```

Vérifier

Suivez ces étapes pour vérifier la connexion du client et les paramètres connexes :

1. Allez à Monitoring > VPN [surveillance > VPN] sur l'ASDM :



2. Vous pouvez utiliser l'option Filter By [filtrer par] pour filtrer le type de VPN. Sélectionnez AnyConnect Client [client AnyConnect] dans le menu déroulant et toutes les sessions du client AnyConnect.



Conseil : les sessions peuvent être filtrées en fonction d'autres critères, tels que le nom d'utilisateur et l'adresse IP.

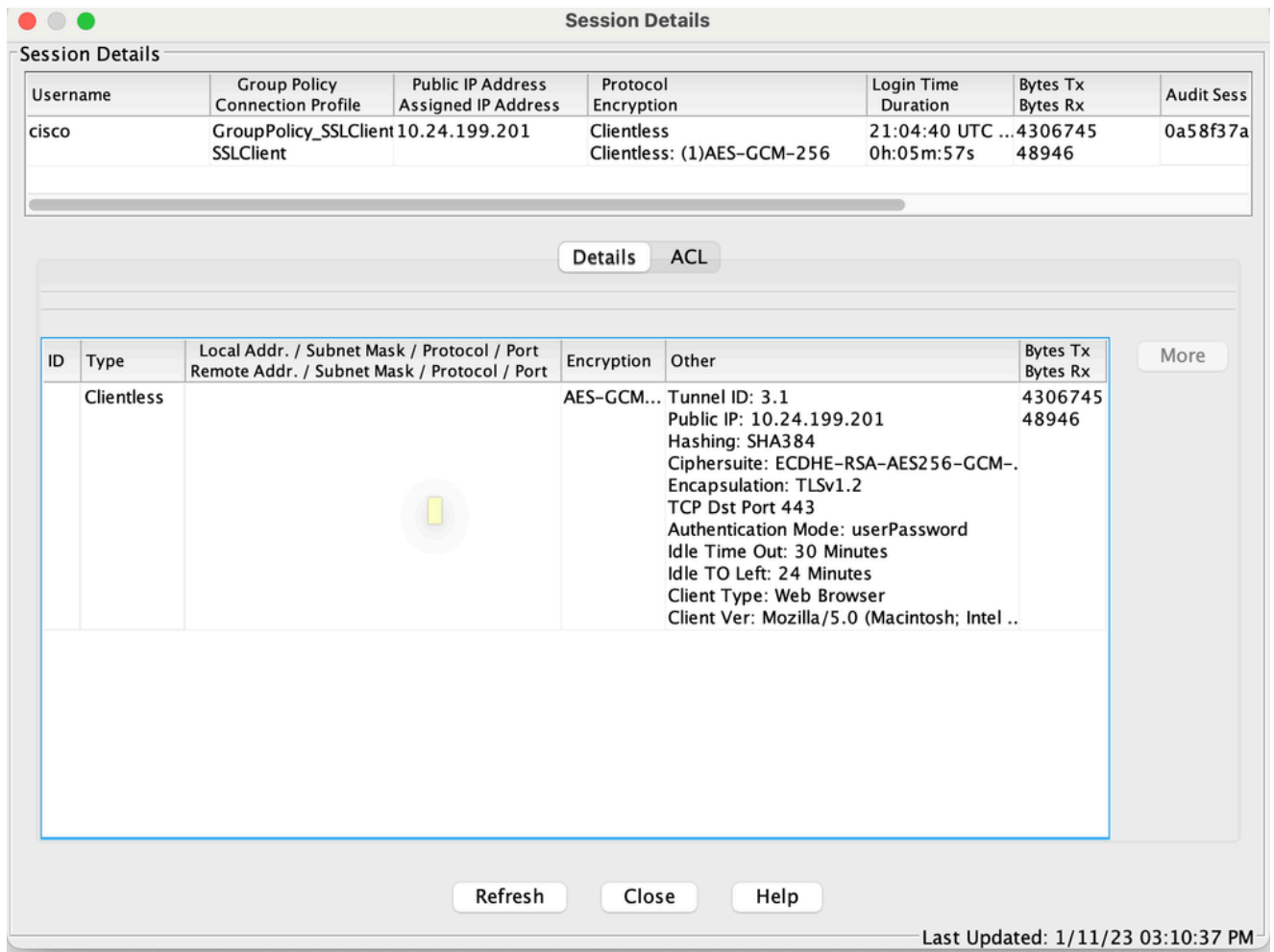
The screenshot shows the ASDM interface for monitoring VPN sessions. The breadcrumb trail is 'Monitoring > VPN > VPN Statistics > Sessions'. On the left, there is a 'Device List' and a 'VPN' tree view with 'Sessions' selected. The main area contains a summary table and a detailed session table.

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN	1	1	1	1
Browser	1	1	1	1

Filter By: All Remote Access -- All Sessions -- Filter

Username	Group Policy	Public IP Address	Protocol	Login Time	Bytes Tx	Audit Session ID	Security Group Tag	Cer Auth Int	Cer Auth Left
cisco	GroupPolicy_SSLClient	10.24.199.201	Clientless	21-04-40 UTC	4306745	0a58f37a000...	none		
	SSLClient		Clientless: (1)AES-GCM-256	0h:05m:29s	48946				

3. Double-cliquez sur une session pour en savoir plus à son sujet :



4. Saisissez la commande `show vpn-sessiondb anyconnect` dans la CLI pour afficher le détail de la session :

<#root>

#

`show vpn-sessiondb anyconnect`

Session Type : AnyConnect

Username : cisco Index : 14

Assigned IP :

10.10.11.1

Public IP :

172.16.21.1

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1

Bytes Tx : 11472 Bytes Rx : 39712

Group Policy :

GroupPolicy_SSLClient

Tunnel Group :

SSLClient

Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

5. Vous pouvez utiliser les autres options de filtrage pour affiner les résultats :

<#root>

#

show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19
Assigned IP :

10.10.11.1

Public IP :

10.106.44.243

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11036 Bytes Rx : 4977
Pkts Tx : 8 Pkts Rx : 60
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy :

GroupPolicy_SSLClient

Tunnel Group :

SSLClient

Login Time

: 20:33:34 UTC Mon Apr 6 2015
Duration : 0h:01m:19s

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

AnyConnect-Parent:

Tunnel ID : 19.1
Public IP : 10.106.44.243

Encryption : none Hashing : none
TCP Src Port : 58311 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073

Bytes Tx : 5518 Bytes Rx : 772
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

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

DTLS-Tunnel:

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

3.1.06073

Bytes Tx : 0 Bytes Rx : 4150
Pkts Tx : 0 Pkts Rx : 59
Pkts

Tx Drop

: 0 Pkts

Rx Drop

: 0

Dépannage

Vous pouvez utiliser l'outil DART (AnyConnect Diagnostics and Reporting Tool) afin de collecter les données utiles pour résoudre les problèmes d'installation et de connexion d'AnyConnect. L'assistant DART est utilisé sur l'ordinateur qui utilise AnyConnect. L'outil DART regroupe les journaux, l'état et les renseignements de diagnostic pour l'analyse du Centre d'assistance technique de Cisco et n'exige aucun privilège administrateur pour fonctionner sur la machine du client.

Installer DART

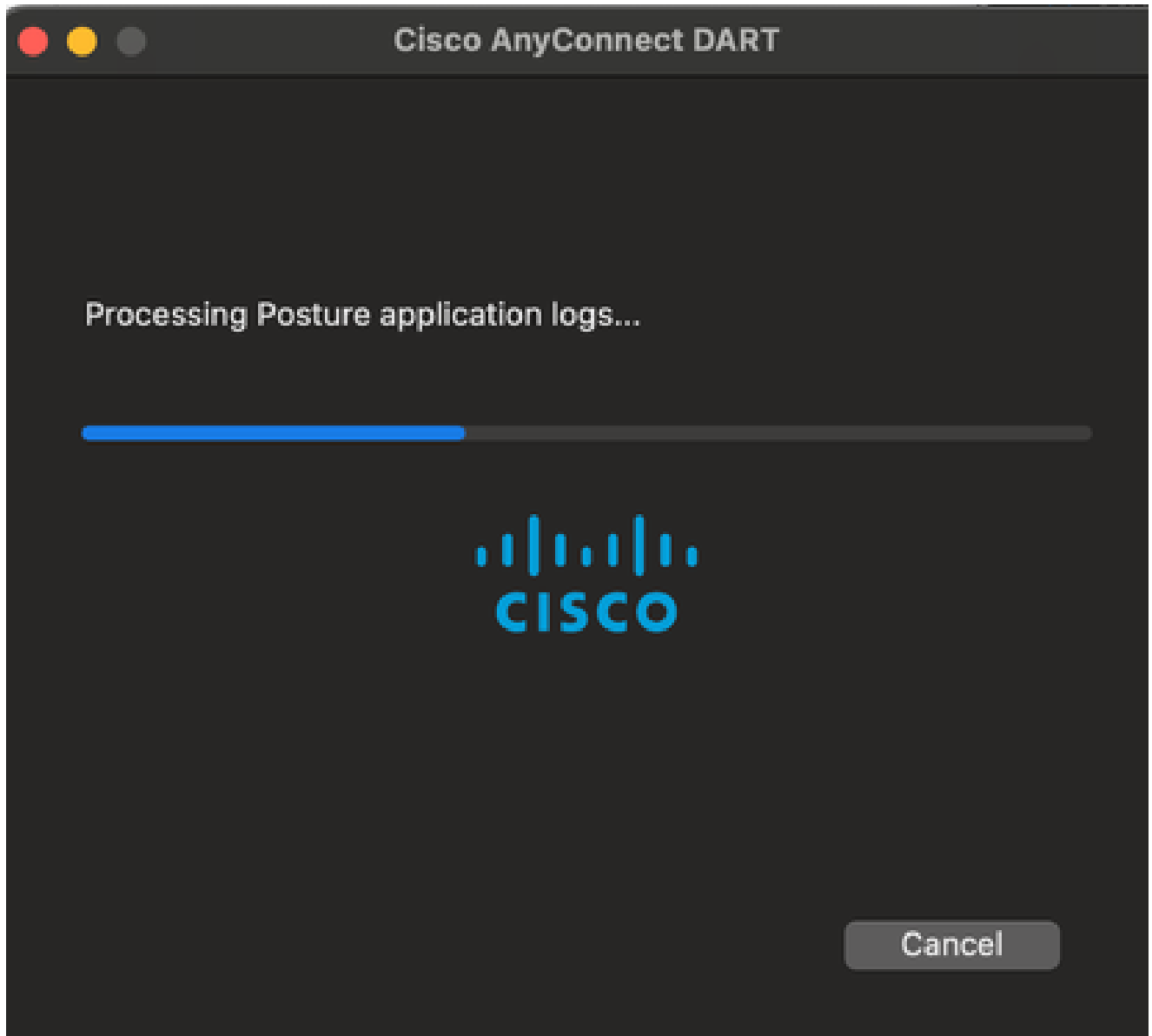
Pour installer le DART, procédez comme suit :

1. Téléchargez l'image du client AnyConnect sur le site Web de Cisco. Pour télécharger la bonne image, consultez la page Web [Cisco AnyConnect Secure Mobility Client](#). Un lien de téléchargement est fourni sur cette page. Accédez à la page de téléchargement, puis sélectionnez la version appropriée. Effectuez une recherche pour trouver l'intégralité du programme d'installation – programme d'installation autonome/Windows (ISO).



Remarque : une image d'installation ISO est ensuite téléchargée (par exemple anyconnect-win-4.10.06079-pre-deploy-k9.iso).

2. Utilisez WinRar ou 7-Zip pour extraire le contenu du programme ISO :
3. Accédez au dossier duquel le contenu a été extrait.
4. Exécutez le fichier Setup.exe et sélectionnez seulement l'outil DART d'Anyconnect :

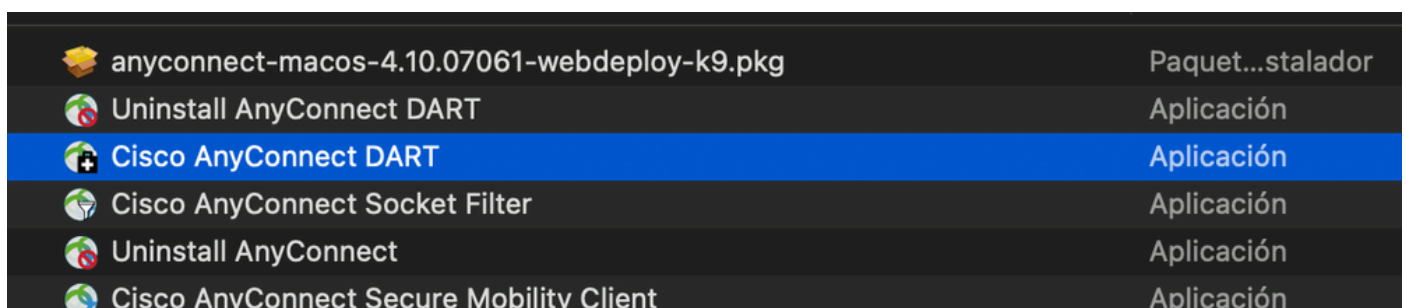


Exécuter DART

Voici quelques renseignements importants à prendre en compte avant le démarrage de DART :

- Le problème doit d'abord être recréé au moins une fois.
- Vous devez indiquer la date et l'heure sur la machine de l'utilisateur lorsque vous recréez le problème.

Lancez DART à partir du menu Start [démarrer] sur la machine du client :



Vous pouvez sélectionner le mode Default [par défaut] ou Custom [personnalisé]. Cisco vous recommande d'exécuter DART en mode Default [par défaut] pour que les renseignements puissent tous être saisis en une fois.

Par la suite, l'outil enregistre le fichier .zip de DART sur le bureau du client. Ce fichier peut ensuite être envoyé par courriel au Centre d'assistance technique de Cisco (après l'ouverture d'un dossier auprès du Centre) pour une analyse plus approfondie.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.