ASA 8.X : Acheminement du trafic de VPN SSL par l'exemple percé un tunnel de configuration de passerelle par défaut

Contenu

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptable (ASA) pour router le trafic VPN SSL via la passerelle tunnelisée par défaut (TDG). Quand vous créez un default route avec l'option percée un tunnel, tout le trafic d'un tunnel se terminant sur l'ASA qui ne peut pas être conduite utilisant les artères instruites ou statiques est envoyé à cette artère. Pour l'émergeant du trafic d'un tunnel, cette artère ignore tous les default route configurés ou appris d'autre.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- ASA qui fonctionne sur la version 8.x
- Client VPN SSL Cisco (SVC) 1.x**Remarque:** Téléchargez le module de client de VPN SSL (sslclient-win*.package) du téléchargement logiciel de Cisco (clients enregistrés seulement). Copiez le SVC sur la mémoire flash sur l'ASA. Le SVC doit être téléchargé aux ordinateurs d'utilisateur distant afin d'établir la connexion de VPN SSL avec l'ASA.

Composants utilisés

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

- Gamme Cisco 5500 ASA qui exécute la version de logiciel 8.x
- Version de Client VPN SSL Cisco pour Windows 1.1.4.179
- PC qui exécute le Windows 2000 Professional ou le Windows XP
- Version 6.1(5) du Cisco Adaptive Security Device Manager (ASDM)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Le client de VPN SSL (SVC) est une technologie de tunnellisation VPN qui donne à des utilisateurs distants les avantages d'un client vpn d'IPSec sans besoin des administrateurs réseau d'installer et configurer des clients vpn d'IPSec sur des ordinateurs distants. Le SVC utilise le ssl encryption qui est déjà présent sur l'ordinateur distant aussi bien que la procédure de connexion de webvpn et l'authentification des dispositifs de sécurité.

Dans le scénario en cours, il y a un client de VPN SSL se connectant aux ressources internes derrière l'ASA par le tunnel de VPN SSL. Le tunnel partagé n'est pas activé. Quand le client de VPN SSL est connecté à l'ASA, toutes les données seront percées un tunnel. Sans compter qu'accéder aux ressources internes, le critère principal est de conduire ce trafic percé un tunnel par la passerelle percée un tunnel par par défaut (DTG).

Vous pouvez définir un default route distinct pour le trafic percé un tunnel avec le default route standard. Le trafic décrypté reçu par l'ASA, pour laquelle il n'y a pas statique ou route apprise, est conduit par le default route standard. Le trafic chiffré reçu par l'ASA, pour laquelle il n'y a pas statique ou route apprise, sera passé au DTG défini par le default route percé un tunnel.

Afin de définir un default route percé un tunnel, utilisez cette commande :

```
route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled
```

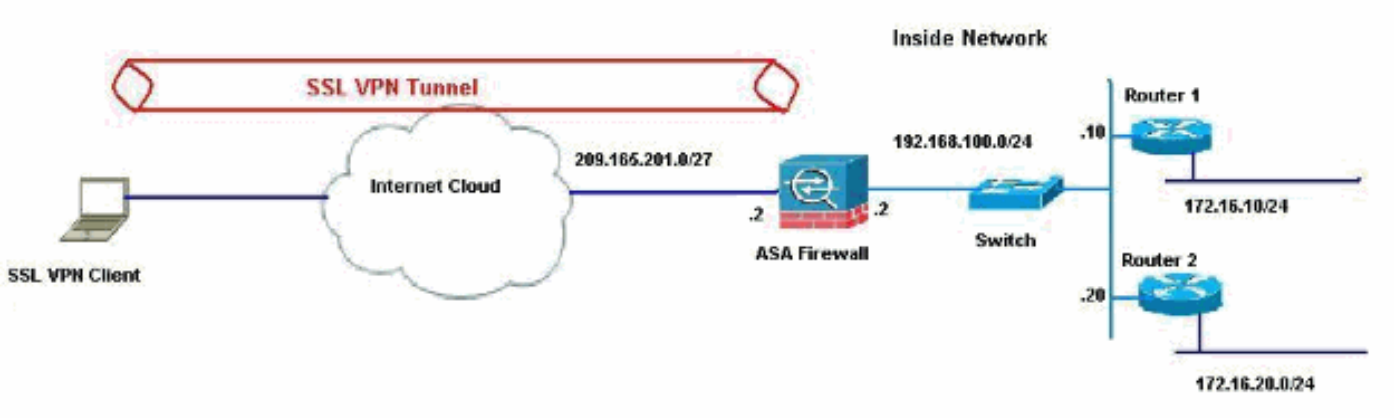
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans cet exemple, les accès client de VPN SSL le réseau intérieur de l'ASA par le tunnel. Le trafic signifié pour des destinations autres que le réseau intérieur sont également percés un tunnel, car il n'y a aucun tunnel partagé configuré, et sont conduits par le TDG (192.168.100.20).

Après que les paquets soient conduits au TDG, qui est Router2 dans ce cas, il exécute la traduction d'adresses pour conduire ces paquets en avant à l'Internet. Pour plus d'informations sur configurer un routeur comme passerelle internet, référez-vous à comment configurer un routeur de Cisco derrière un modem câble de Non-Cisco.

Configuration ASA utilisant l'ASDM 6.1(5)

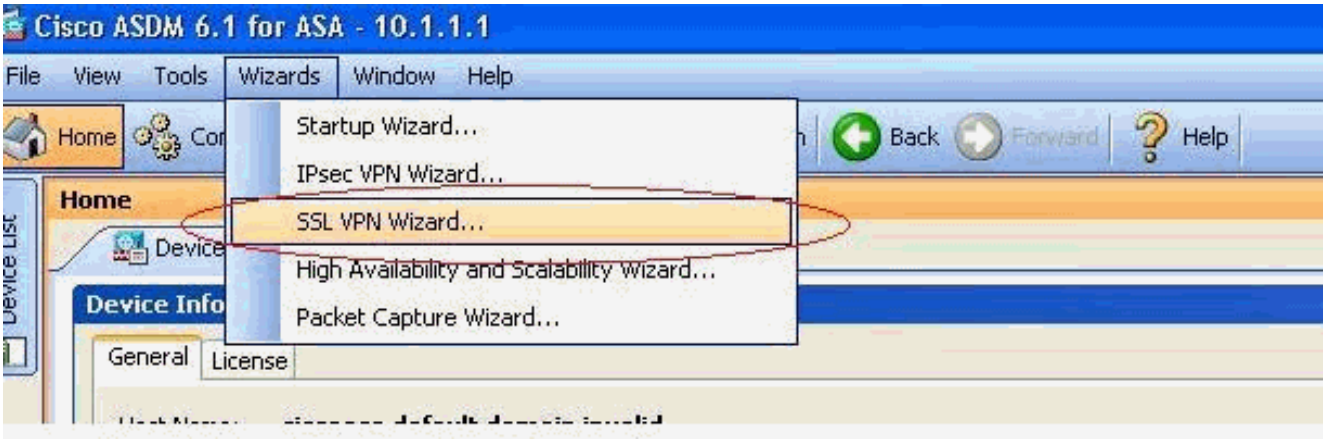
Ce document suppose les configurations de base, telles que la configuration d'interface, est complet et travail correctement.

Remarque: Référez-vous à permettre HTTPS Access pour l'ASDM pour les informations sur la façon dont permettre l'ASA à configurer par l'ASDM.

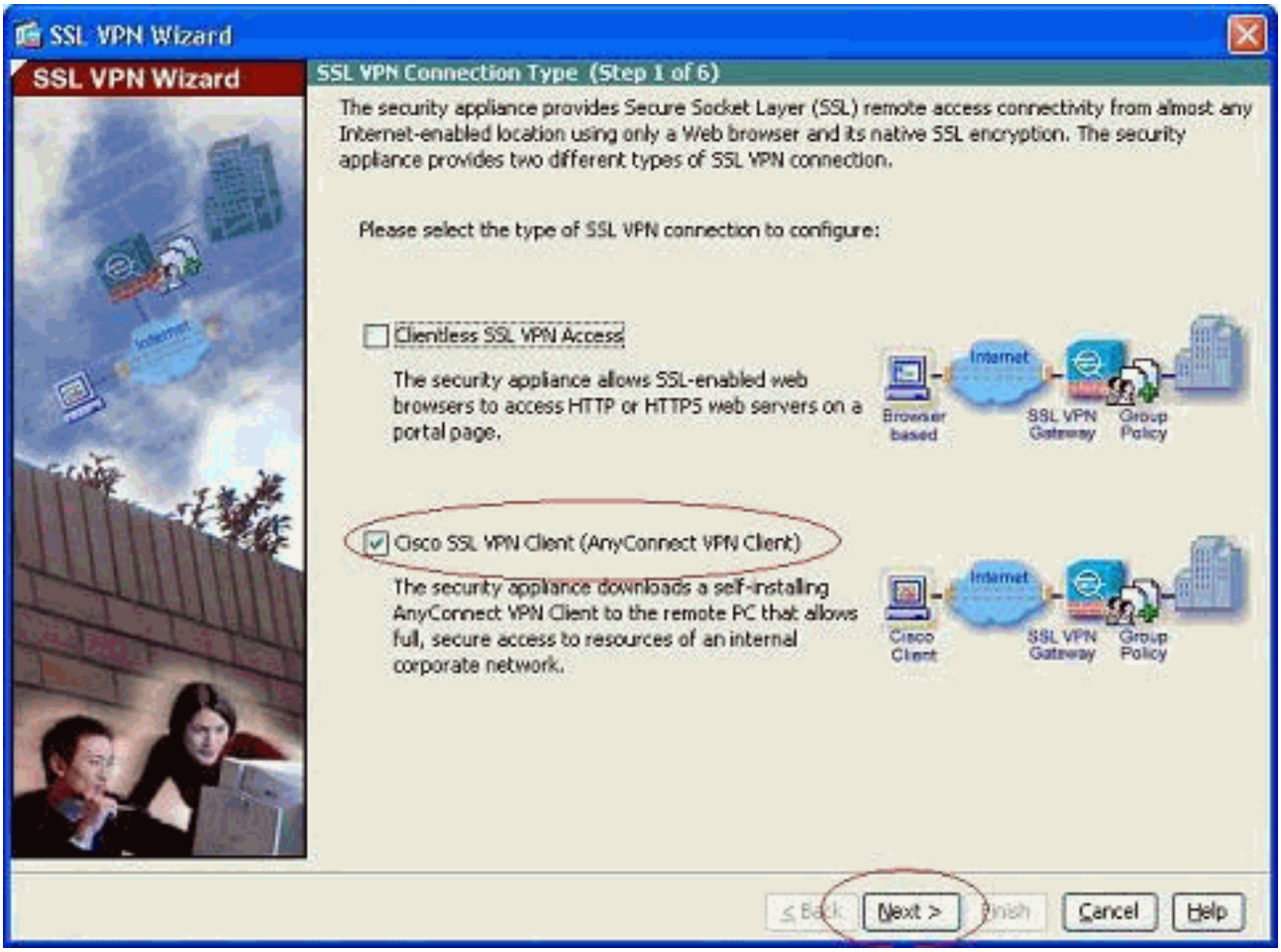
Remarque: Le WebVPN et l'ASDM ne peuvent pas être activés sur la même interface ASA à moins que vous changiez les numéros de port. Référez-vous à ASDM et WebVPN activés sur la même interface d'ASA pour plus d'informations.

Terminez-vous ces étapes afin de configurer le VPN SSL à l'aide de l'assistant de VPN SSL.

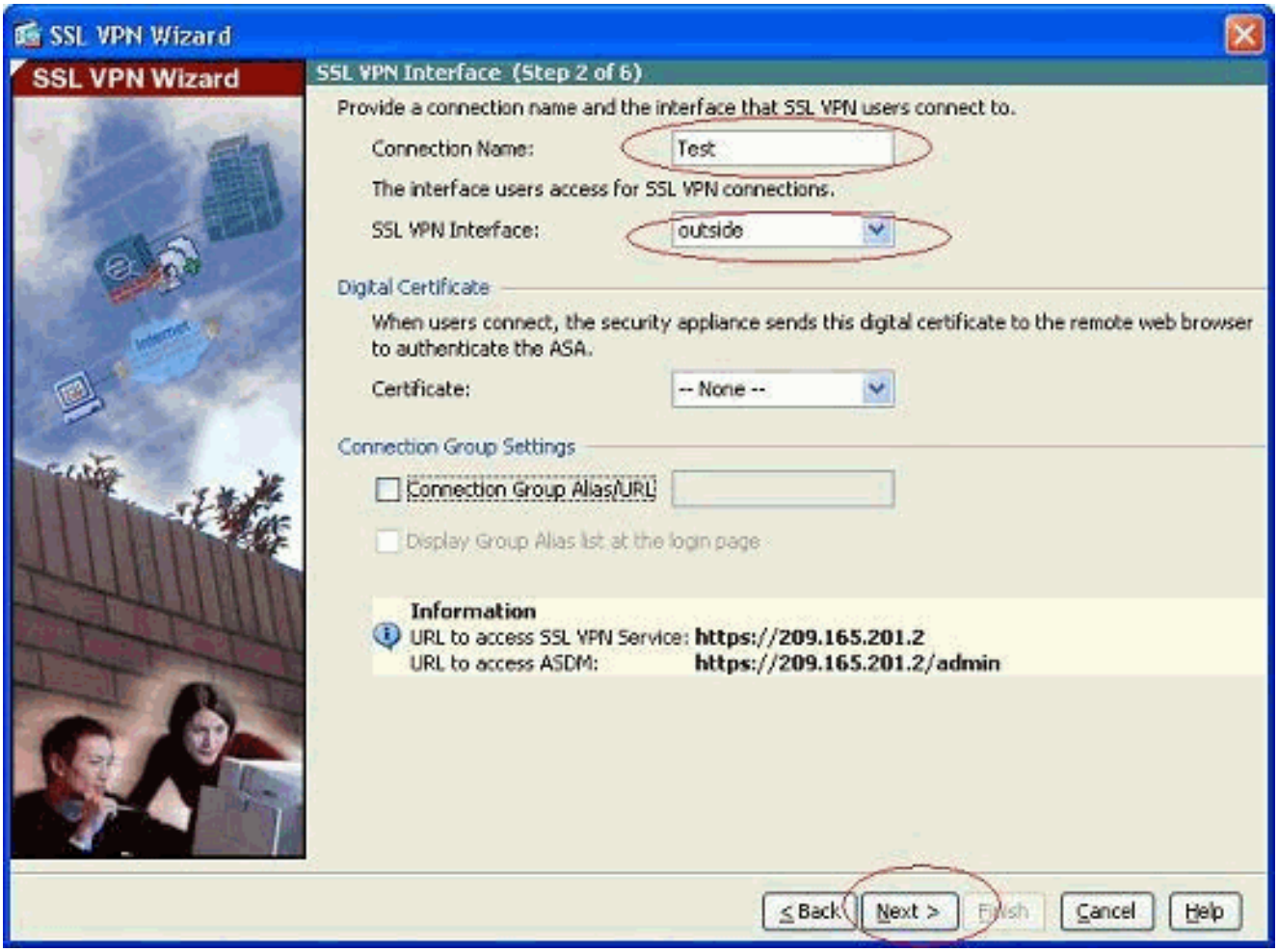
1. Du menu d'assistants, choisissez l'**assistant de VPN SSL**.



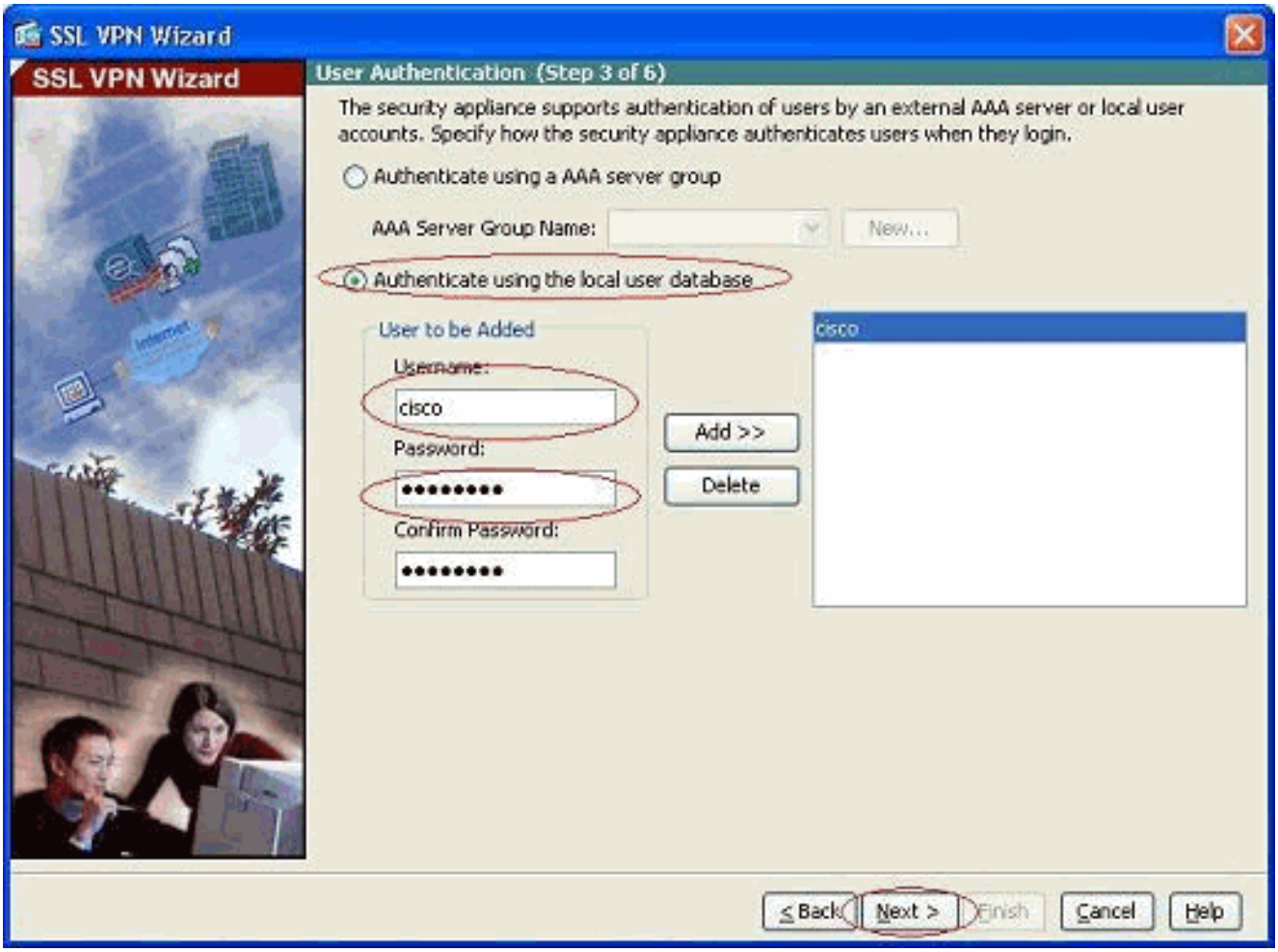
2. Cliquez sur la case de **Client VPN SSL Cisco**, et cliquez sur Next.



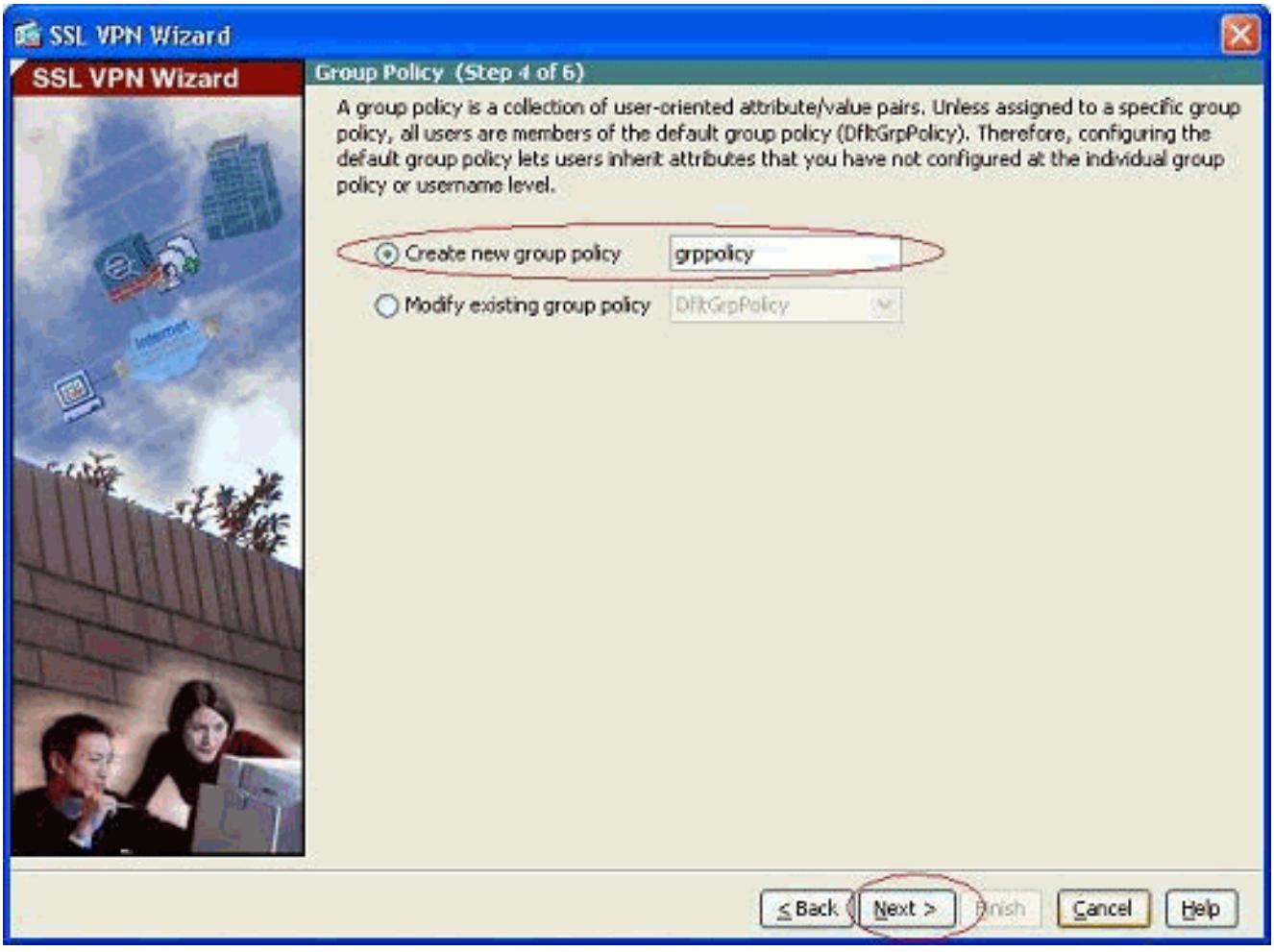
3. Écrivez un nom pour la connexion dans le domaine de nom de la connexion, et puis choisissez l'interface qui est utilisée par l'utilisateur pour accéder au VPN SSL de la liste déroulante d'interface de VPN
   SSL.



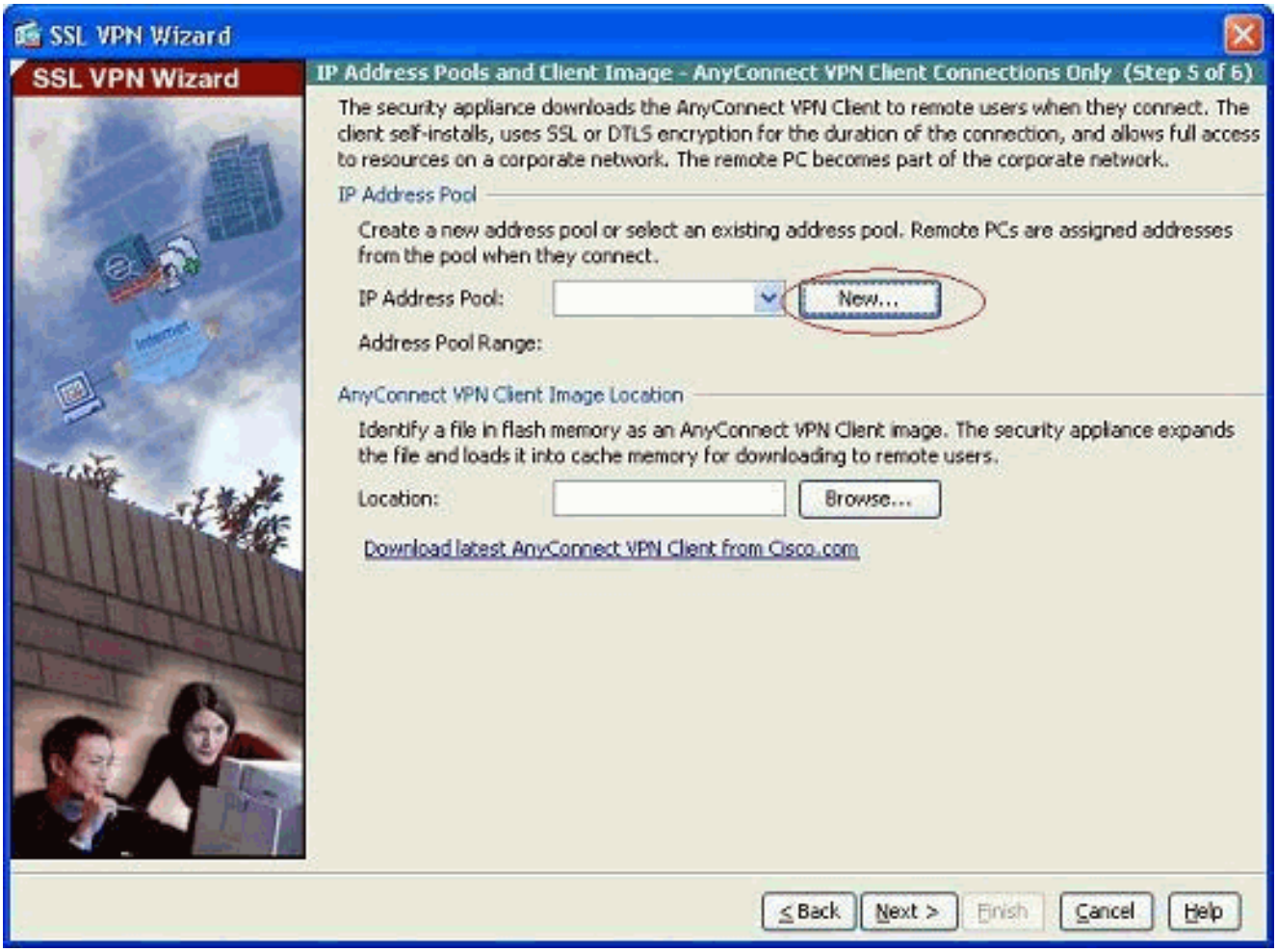
4. Cliquez sur **Next** (Suivant).
5. Choisissez une authentication mode, et cliquez sur Next. (Cet exemple utilise l'authentification
   locale.)



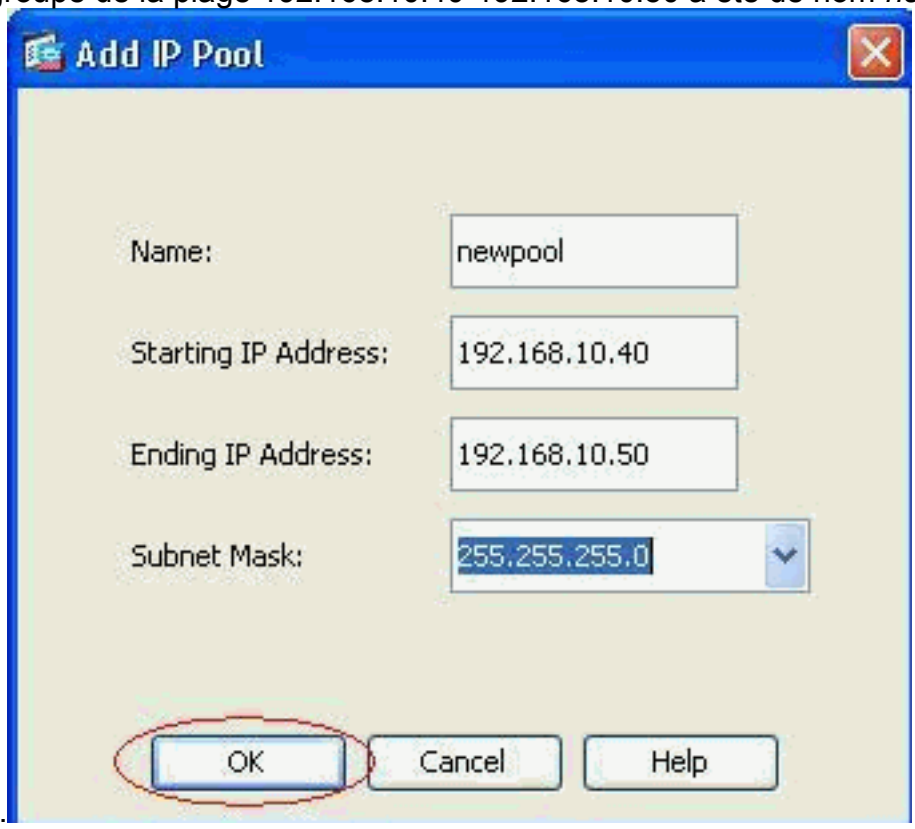
6. Créez une nouvelle stratégie de groupe autre que la stratégie existante de groupe par défaut.



7. Créez un nouveau groupe d'adresses qui seront assignées aux PC de client de VPN SSL une fois qu'elles obtiennent
connecté.

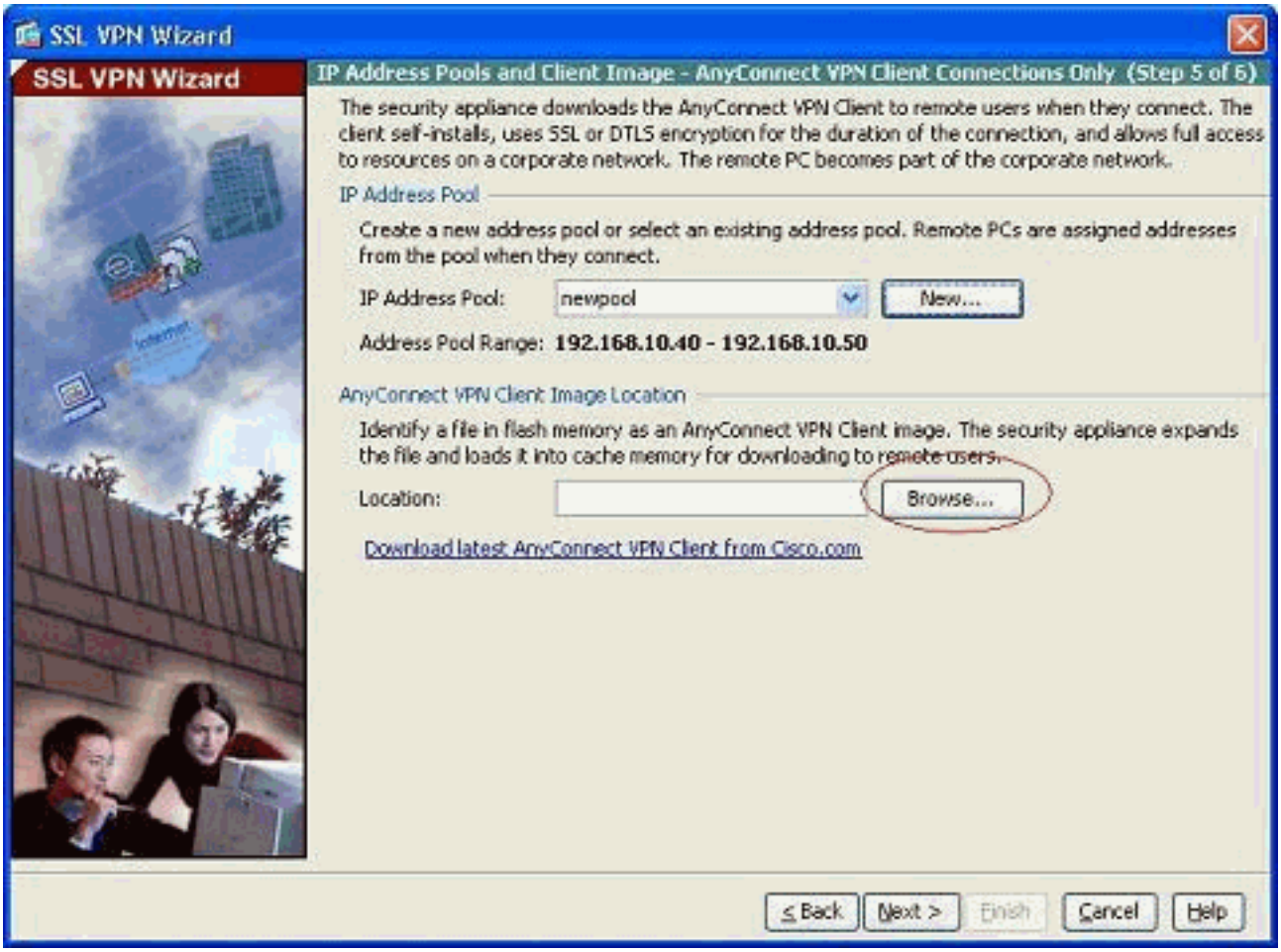


Un groupe de la plage 192.168.10.40-192.168.10.50 a été de nom *newpool*
créé.

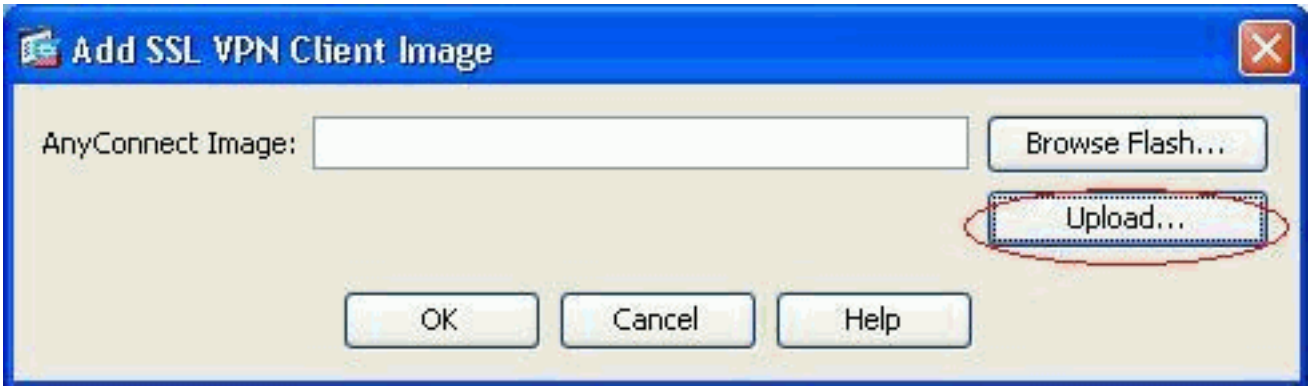


8. Cliquez sur **parcourent** afin de choisir et télécharger l'image de client de VPN SSL à la

mémoire flash de
l'ASA.

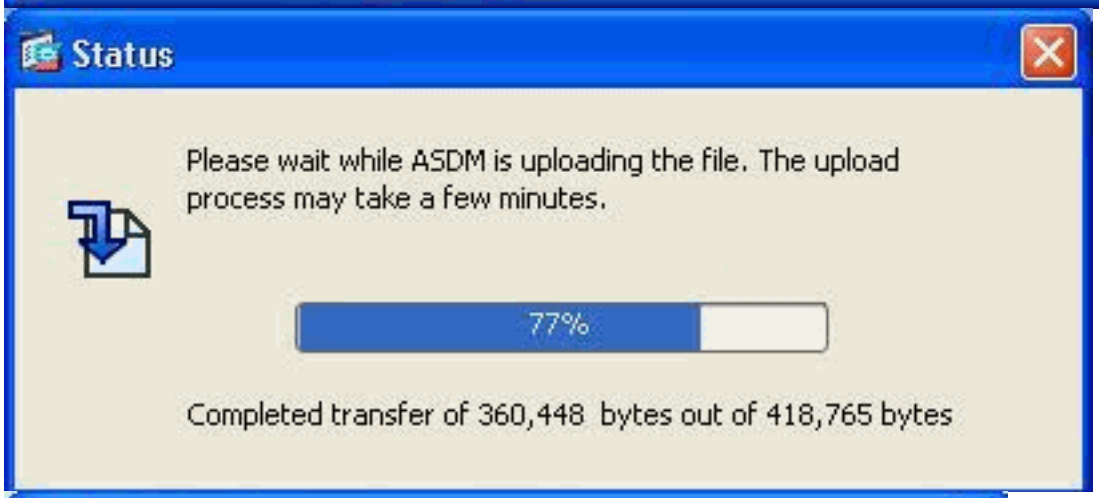


9. Cliquez sur Upload afin de placer le chemin de fichier à partir du répertoire local de l'ordinateur.



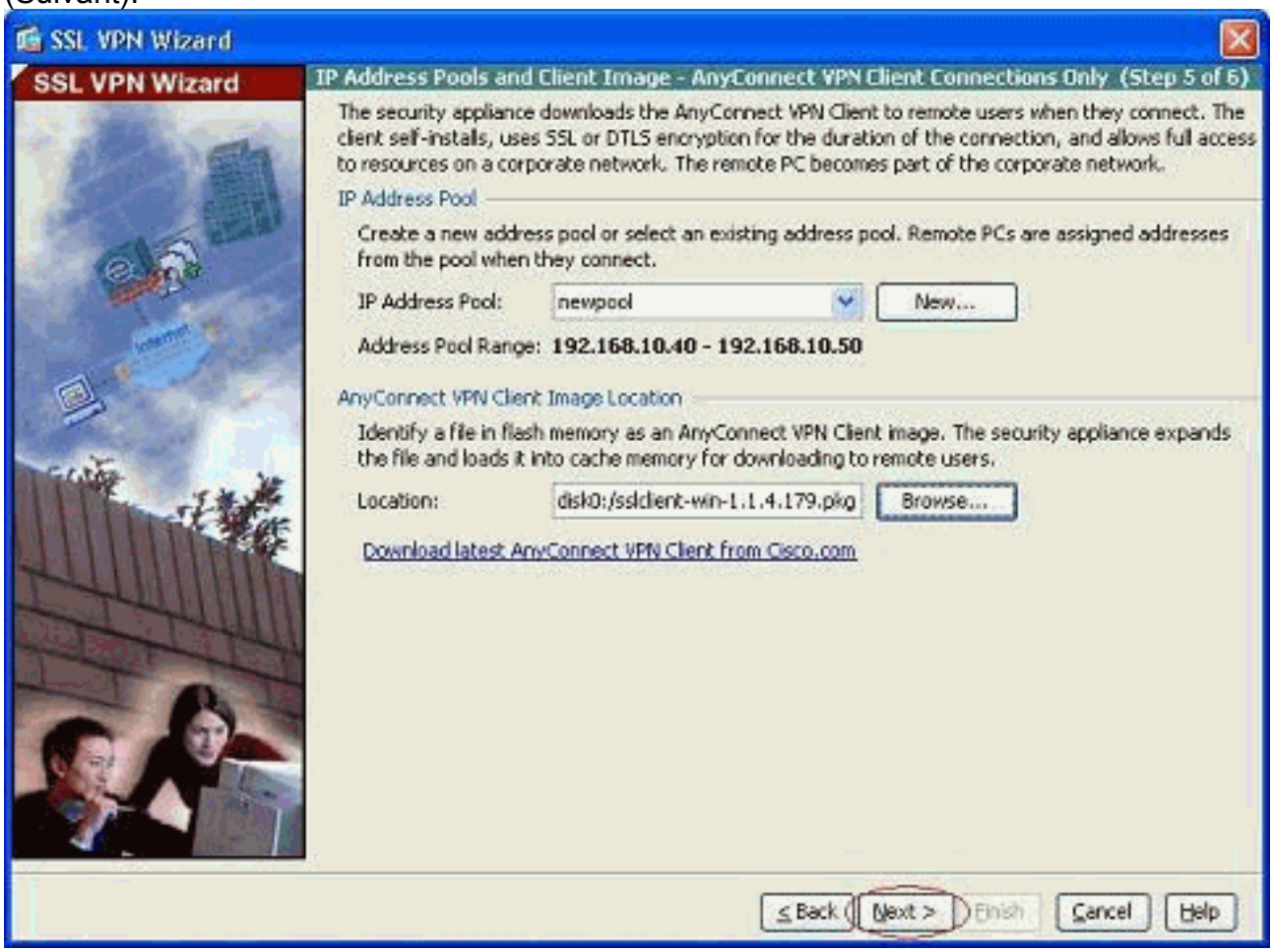
10. Le clic **parcourent des fichiers locaux** afin de sélectionner le répertoire où le fichier sslclient.pkg
existe.

11. Cliquez sur Upload le **fichier** afin de télécharger le fichier sélectionné à l'éclair de l'ASA.

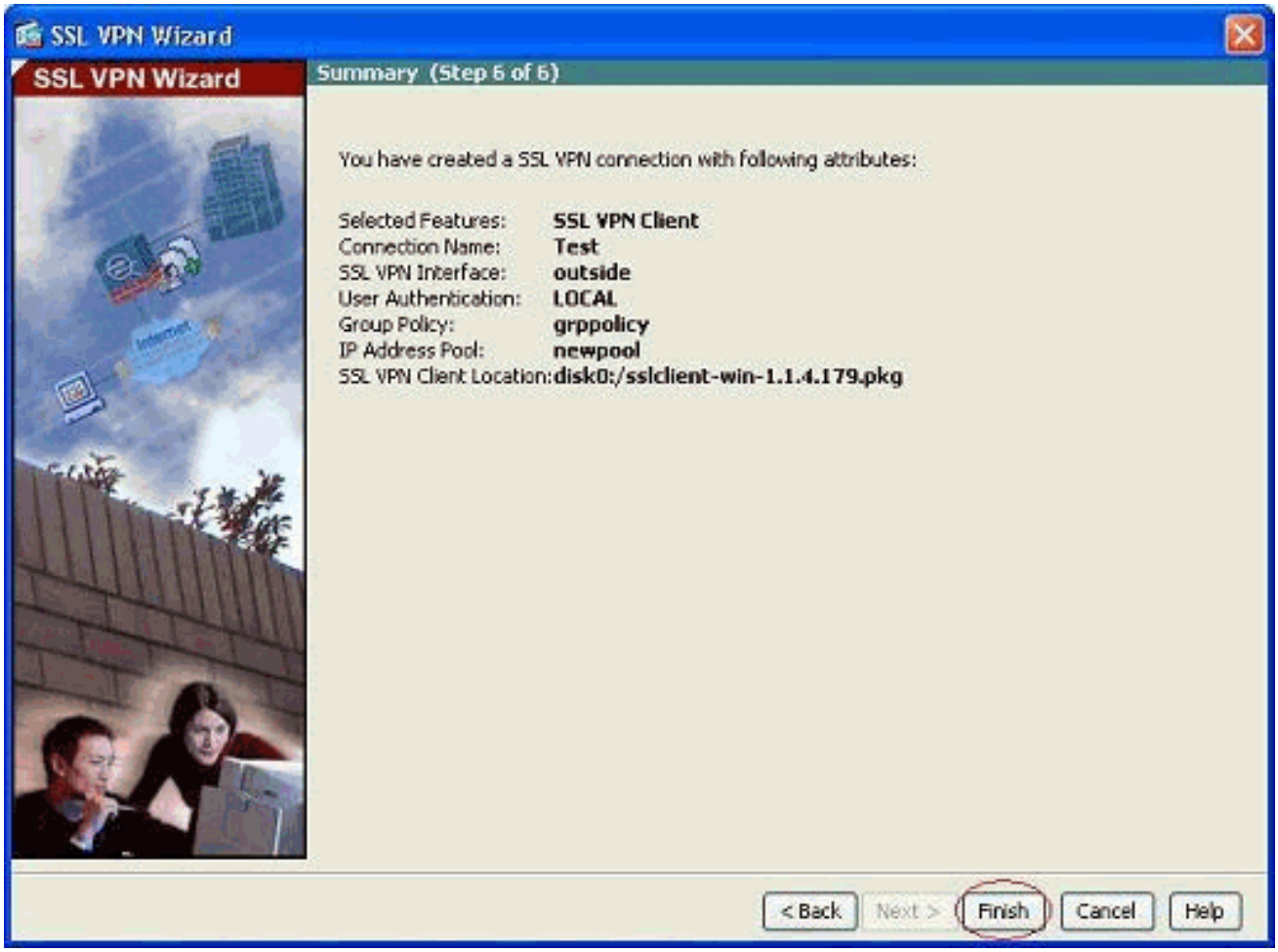


12. Une fois le fichier est téléchargé en fonction à l'éclair de l'ASA, cliquent sur OK pour se terminer cette
tâche.

13. Maintenant il affiche le dernier fichier de package d'anyconnect téléchargé en fonction à l'éclair de l'ASA. Cliquez sur **Next**
(Suivant).



14. Le résumé de la configuration de client de VPN SSL est affiché. Cliquez sur Finish pour se terminer
l'assistant.



La configuration illustrée dans l'ASDM concerne principalement la configuration d'assistant de client de VPN SSL.

Dans le CLI, vous pouvez observer une certaine configuration supplémentaire. La configuration complète CLI est affichée ci-dessous et d'importantes commandes ont été mises en valeur.

ciscoasa

```
ciscoasa#show running-config : Saved : ASA Version
8.0(4) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 209.165.201.2
255.255.255.224 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.100.2
255.255.255.0 ! interface Ethernet0/2 nameif manage
security-level 0 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/3 shutdown no nameif no security-
level no ip address ! interface Ethernet0/4 shutdown no
nameif no security-level no ip address ! interface
Ethernet0/5 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive access-list nonat extended permit ip
192.168.100.0 255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0 !--- ACL to
define the traffic to be exempted from NAT. no pager
logging enable logging asdm informational mtu outside
1500 mtu inside 1500 mtu manage 1500 !--- Creating IP
address block to be assigned for the VPN clients ip
local pool newpool 192.168.10.40-192.168.10.50 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-615.bin no asdm
history enable arp timeout 14400 global (outside) 1
```

```
interface nat (inside) 0 access-list nonat !--- The
traffic permitted in "nonat" ACL is exempted from NAT.
nat (inside) 1 192.168.100.0 255.255.255.0 route outside
0.0.0.0 0.0.0.0 209.165.201.1 1 !--- Default route is
configured through "inside" interface for normal
traffic. route inside 0.0.0.0 0.0.0.0 192.168.100.20
tunneled !--- Tunneled Default route is configured
through "inside" interface for encrypted traffic !
timeout xlate 3:00:00 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 uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable !--- Configuring the ASA as HTTP server.
http 10.1.1.0 255.255.255.0 manage !--- Configuring the
network to be allowed for ASDM access. ! !--- Output is
suppressed ! telnet timeout 5 ssh timeout 5 console
timeout 0 threat-detection basic-threat threat-detection
statistics access-list ! class-map inspection_default
match default-inspection-traffic ! ! policy-map type
inspect dns preset_dns_map parameters message-length
maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map inspect
ftp inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
inspect xdmcp ! service-policy global_policy global ! !-
-- Output suppressed ! webvpn enable outside !--- Enable
WebVPN on the outside interface svc image
disk0:/sslclient-win-1.1.4.179.pkg 1 !--- Assign the
AnyConnect SSL VPN Client image to be used svc enable !-
-- Enable the ASA to download SVC images to remote
computers group-policy grppolicy internal !--- Create an
internal group policy "grppolicy" group-policy grppolicy
attributes VPN-tunnel-protocol svc !--- Specify SSL as a
permitted VPN tunneling protocol ! username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 15 !---
Create a user account "cisco" tunnel-group Test type
remote-access !--- Create a tunnel group "Test" with
type as remote access tunnel-group Test general-
attributes address-pool newpool !--- Associate the
address pool vpnpool created default-group-policy
grppolicy !--- Associate the group policy "clientgroup"
created prompt hostname context
Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
ciscoasa#
```

Vérifiez

Les instructions données dans cette section peuvent être utilisées pour vérifier cette configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **affichez que svc de webvpn** — — affiche les images de SVC enregistrées dans la mémoire flash ASA.
- **show vpn-sessiondb svc** — Affiche les informations sur les connexions SSL actuelles.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support d'appliance de sécurité adaptable de gamme Cisco 5500
- Exemple de configuration de PIX/ASA et d'un client VPN pour un VPN Internet public sur un stick
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- Support et documentation techniques - Cisco Systems