

ASA 8.X : Exemple de configuration de routage du trafic VPN SSL via la passerelle par défaut tunnelisée

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration d'ASA utilisant l'ASDM 6.1\(5\)](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'apppliance de sécurité adaptable (ASA) pour router le trafic VPN SSL via la passerelle tunnelisée par défaut (TDG). Lorsque vous créez une route par défaut avec l'option tunnel, tout le trafic d'un tunnel se terminant sur l'ASA qui ne peut pas être routé à l'aide de routes apprises ou statiques est envoyé à cette route. Pour le trafic sortant d'un tunnel, cette route remplace toute autre route par défaut configurée ou apprise.

Conditions préalables

Conditions requises

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

- ASA qui s'exécute sur la version 8.x
- Client VPN SSL Cisco (SVC) 1.x**Remarque** : Téléchargez le package client VPN SSL (sslclient-win*.pkg) à partir du [téléchargement de logiciels Cisco](#) (clients [enregistrés](#) uniquement). Copiez le SVC dans la mémoire flash de l'ASA. Le SVC doit être téléchargé sur les ordinateurs des utilisateurs distants afin d'établir la connexion VPN SSL avec l'ASA.

Components Used

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

- ASA de la gamme Cisco 5500 qui exécute la version logicielle 8.x
- Version du client VPN SSL Cisco pour Windows 1.1.4.179
- PC exécutant Windows 2000 Professionnel ou Windows XP
- Cisco Adaptive Security Device Manager (ASDM) version 6.1(5)

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.

[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 VPN SSL (SVC) est une technologie de tunnellation VPN qui offre aux utilisateurs distants les avantages d'un client VPN IPSec sans que les administrateurs réseau aient besoin d'installer et de configurer des clients VPN IPSec sur des ordinateurs distants. Le SVC utilise le chiffrement SSL qui est déjà présent sur l'ordinateur distant, ainsi que la connexion WebVPN et l'authentification de l'appliance de sécurité.

Dans le scénario actuel, un client VPN SSL se connecte aux ressources internes derrière l'ASA via le tunnel VPN SSL. Le split-tunnel n'est pas activé. Lorsque le client VPN SSL est connecté à l'ASA, toutes les données sont tunnelisées. Outre l'accès aux ressources internes, le principal critère est d'acheminer ce trafic tunnelisé via la passerelle tunnelée par défaut (DTG).

Vous pouvez définir une route par défaut distincte pour le trafic tunnelisé avec la route par défaut standard. Le trafic non chiffré reçu par l'ASA, pour lequel il n'existe aucune route statique ou apprise, est acheminé par la route par défaut standard. Le trafic crypté reçu par l'ASA, pour lequel il n'existe aucune route statique ou apprise, sera transmis au DTG défini par la route par défaut tunnelisée.

Afin de définir une route par défaut avec tunnel, utilisez cette commande :

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

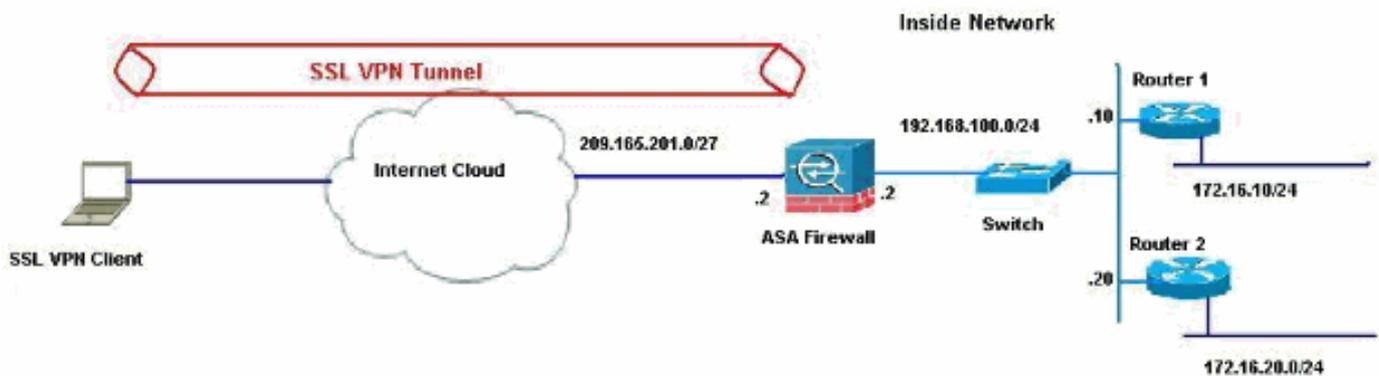
[Configuration](#)

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

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) 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, le client VPN SSL accède au réseau interne de l'ASA via le tunnel. Le trafic destiné à des destinations autres que le réseau interne est également tunnelisé, car aucun tunnel partagé n'est configuré et est acheminé via le TDG (192.168.100.20).

Une fois que les paquets sont routés vers le TDG, qui est le routeur 2 dans ce cas, il effectue la traduction d'adresses pour acheminer ces paquets vers Internet. Pour plus d'informations sur la configuration d'un routeur en tant que passerelle Internet, référez-vous à [Comment configurer un routeur Cisco derrière un modem câble non Cisco](#).

[Configuration d'ASA utilisant l'ASDM 6.1\(5\)](#)

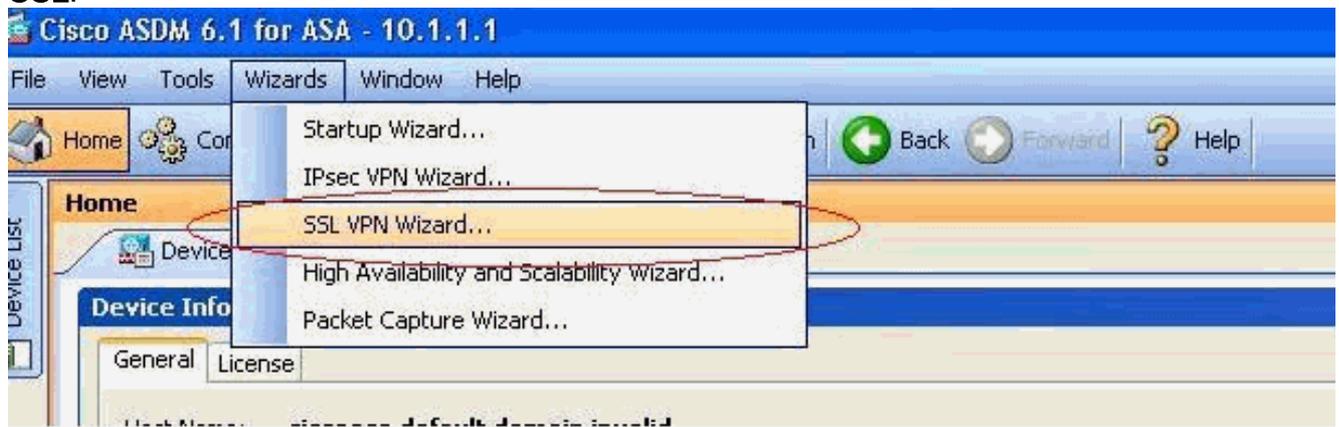
Ce document suppose que les configurations de base, telles que la configuration d'interface, sont complètes et fonctionnent correctement.

Remarque : référez-vous à [Autoriser l'accès HTTPS pour ASDM](#) pour plus d'informations sur la façon de permettre à l'ASA d'être configuré par l'ASDM.

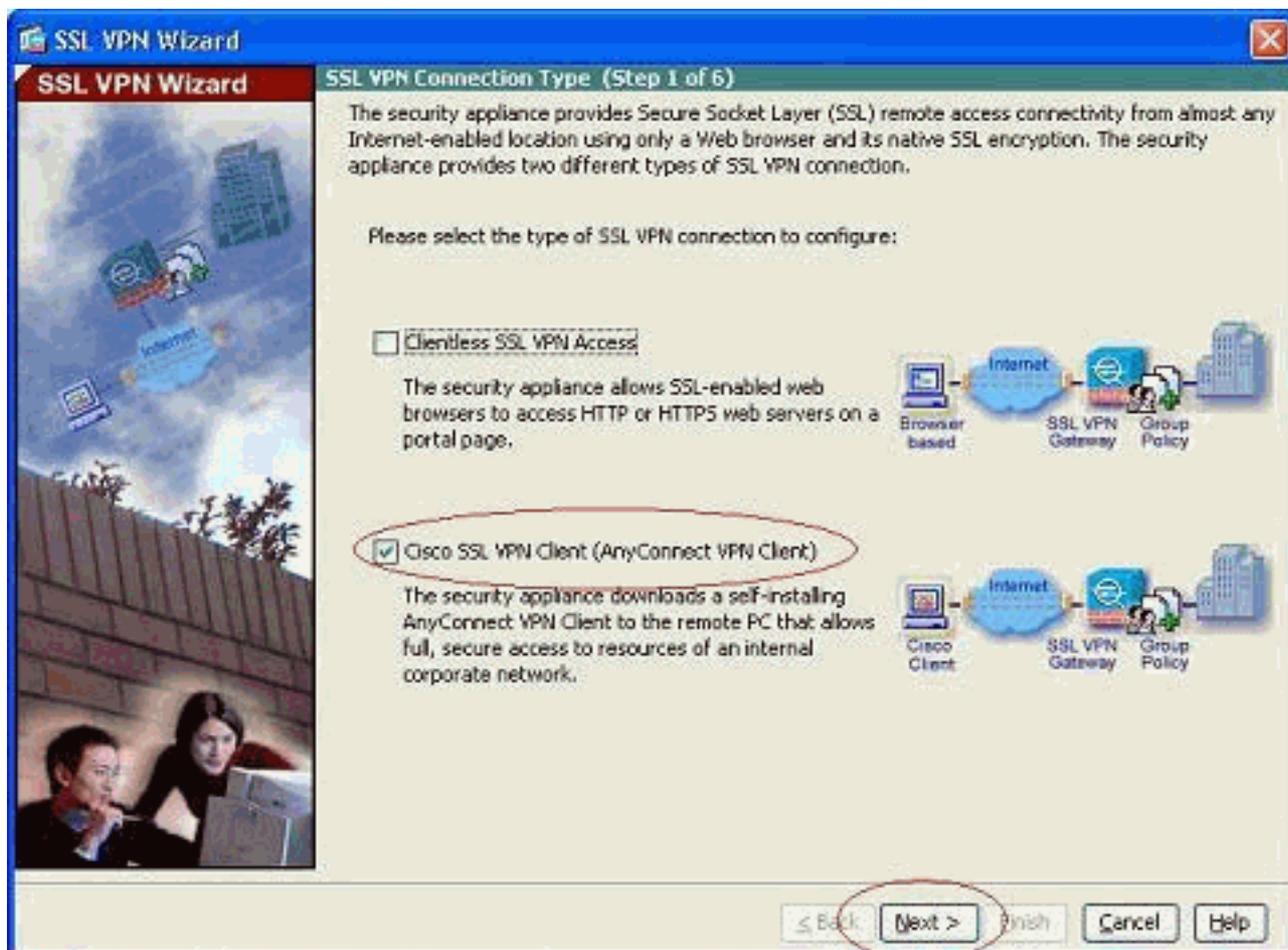
Remarque : WebVPN et ASDM ne peuvent pas être activés sur la même interface ASA, sauf si vous modifiez les numéros de port. Référez-vous à [ASDM et WebVPN activés sur la même interface d'ASA pour plus d'informations](#).

Complétez ces étapes afin de configurer le VPN SSL à l'aide de l'Assistant VPN SSL.

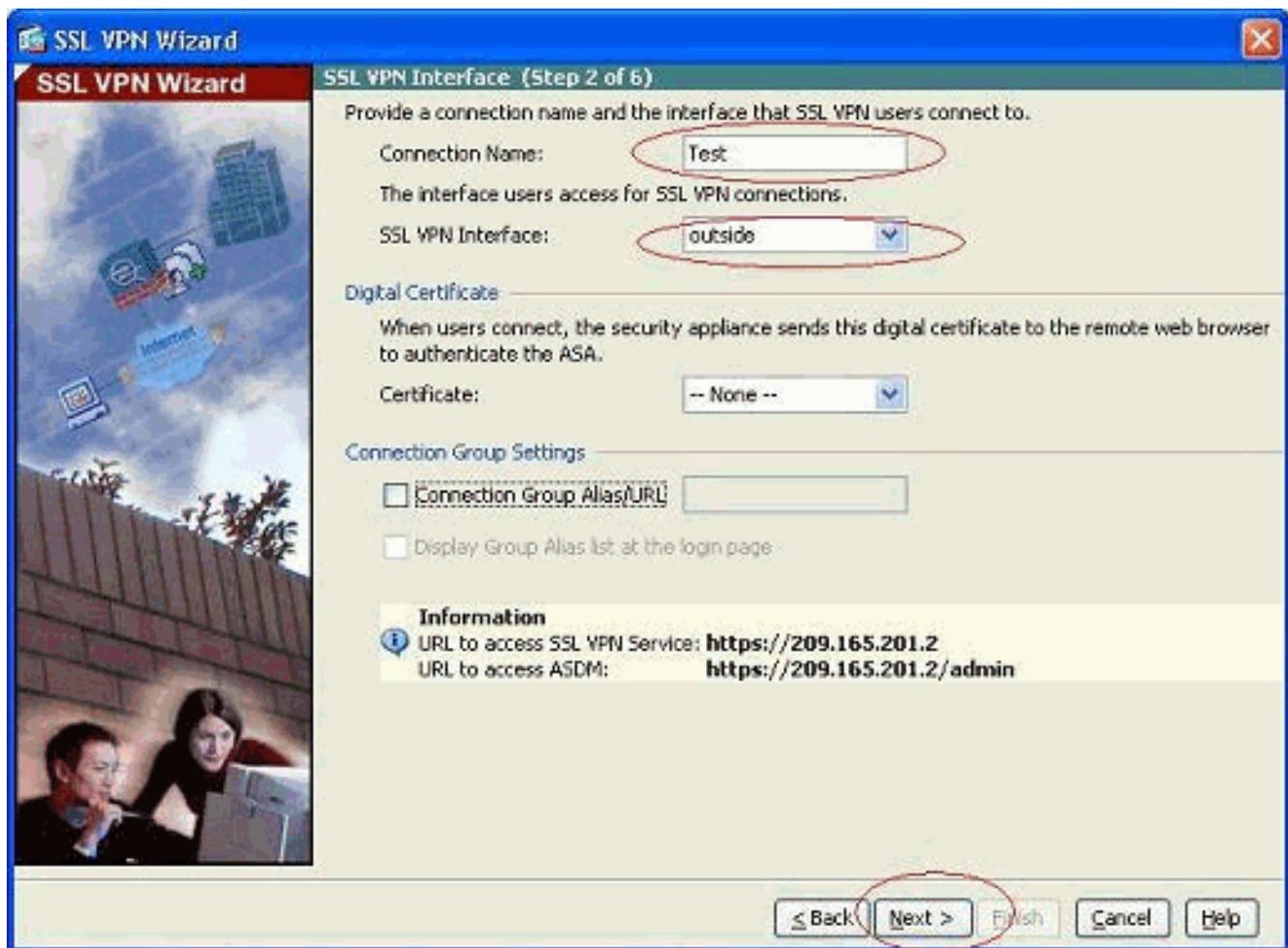
1. Dans le menu Assistants, sélectionnez **Assistant VPN SSL**.



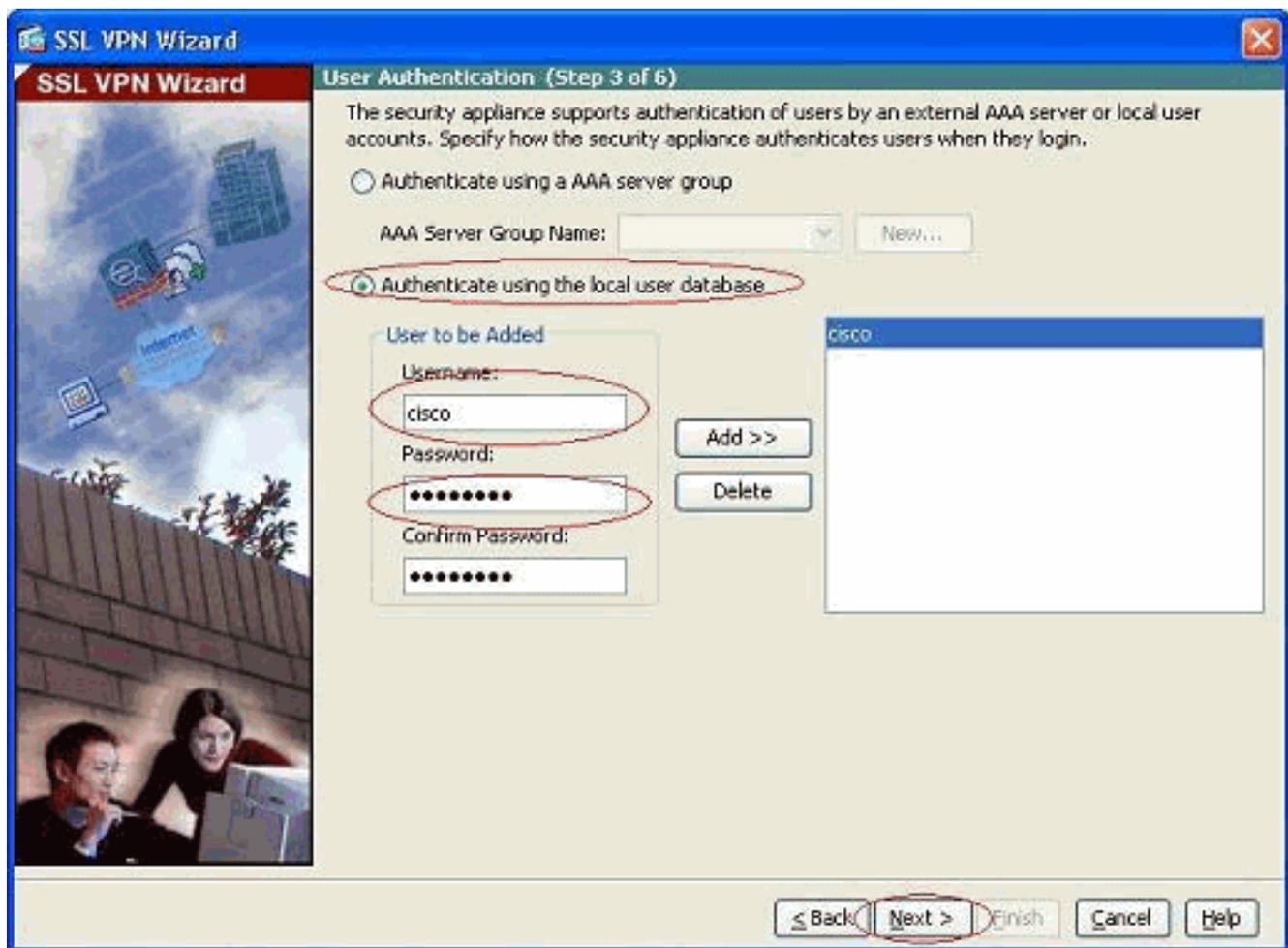
2. Cochez la case **Client VPN SSL Cisco**, puis cliquez sur **Suivant**.



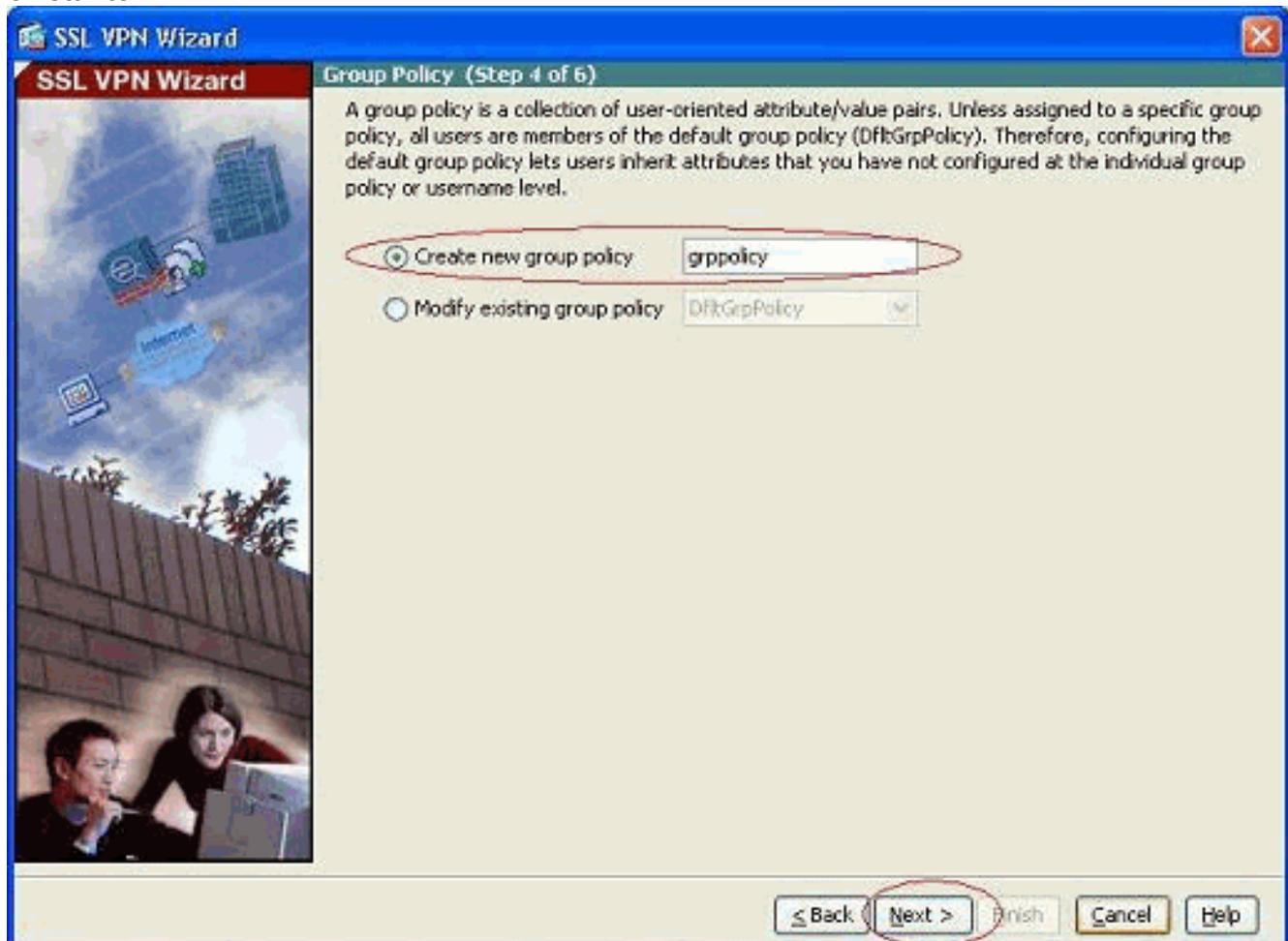
3. Entrez un nom pour la connexion dans le champ Nom de la connexion, puis choisissez l'interface utilisée par l'utilisateur pour accéder au VPN SSL dans la liste déroulante Interface VPN SSL.



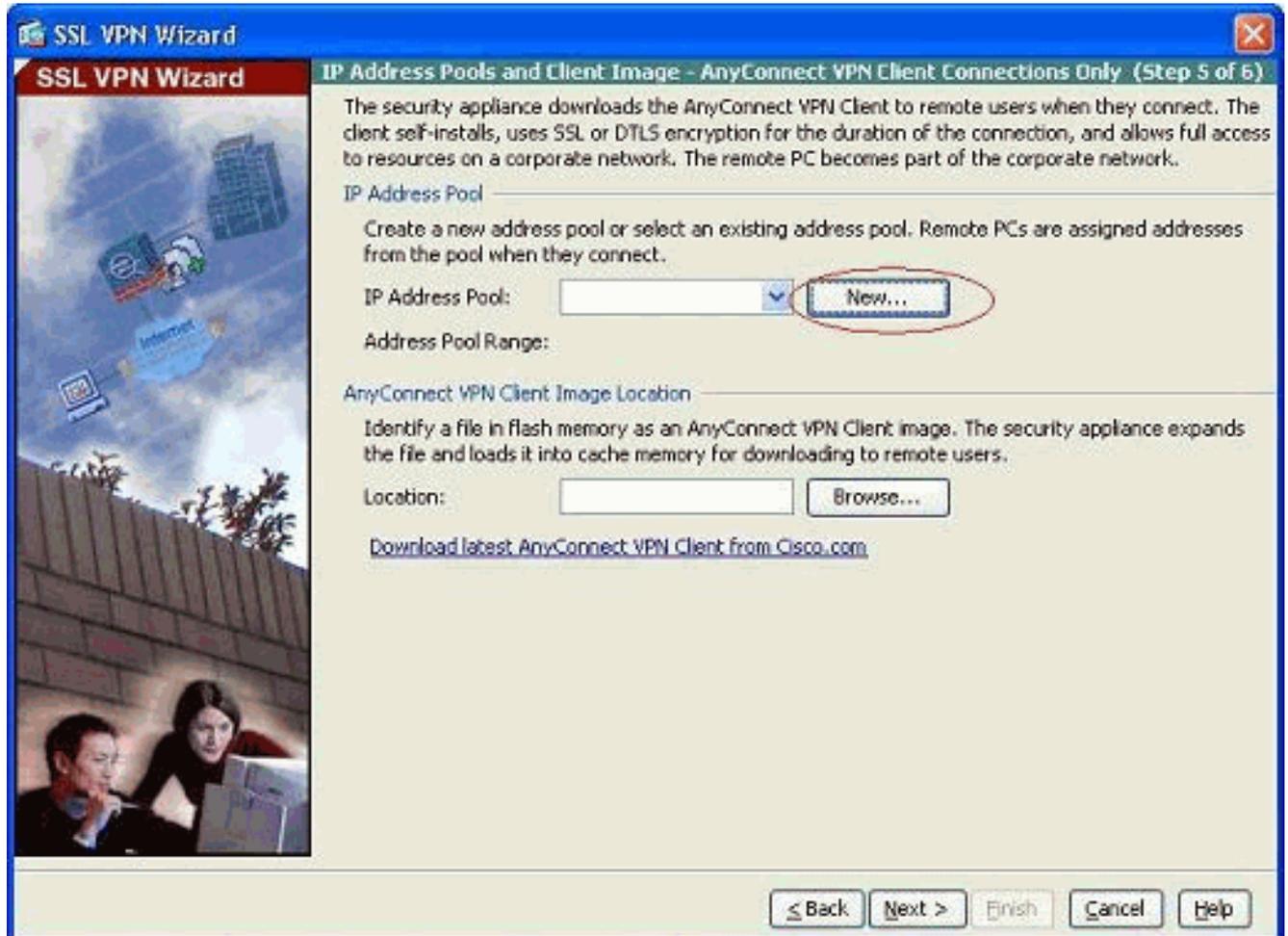
4. Cliquez sur **Next** (Suivant).
5. Choisissez un mode d'authentification, puis cliquez sur **Suivant**. (Cet exemple utilise l'authentification locale.)



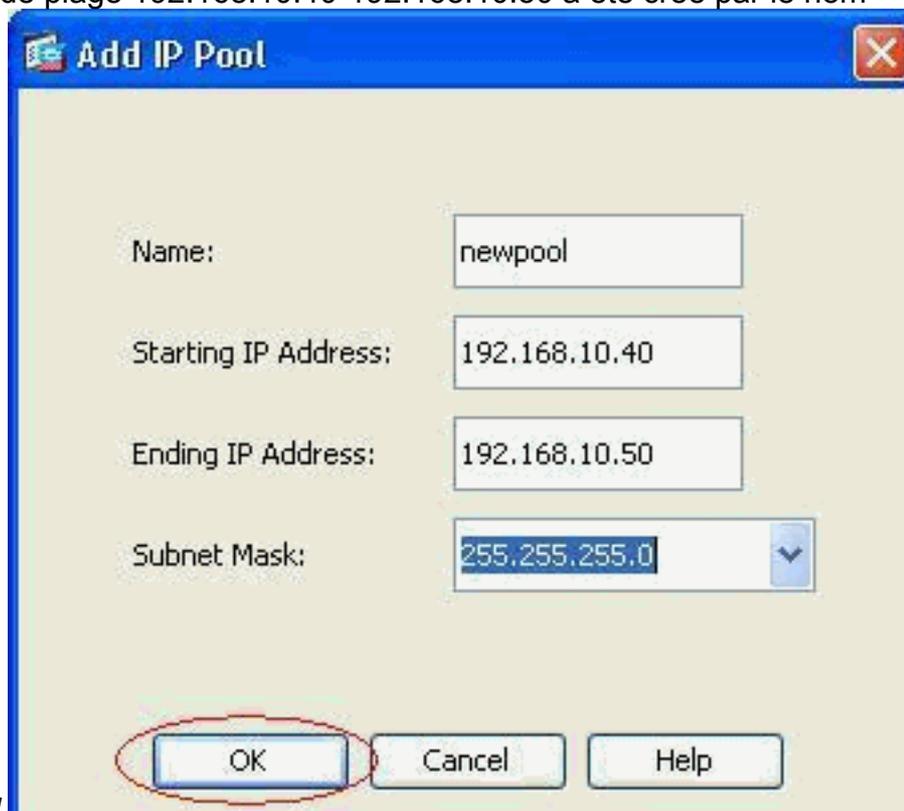
6. Créez une nouvelle stratégie de groupe autre que la stratégie de groupe par défaut existante.



7. Créez un nouveau pool d'adresses qui sera attribué aux PC clients VPN SSL une fois qu'ils seront connectés.



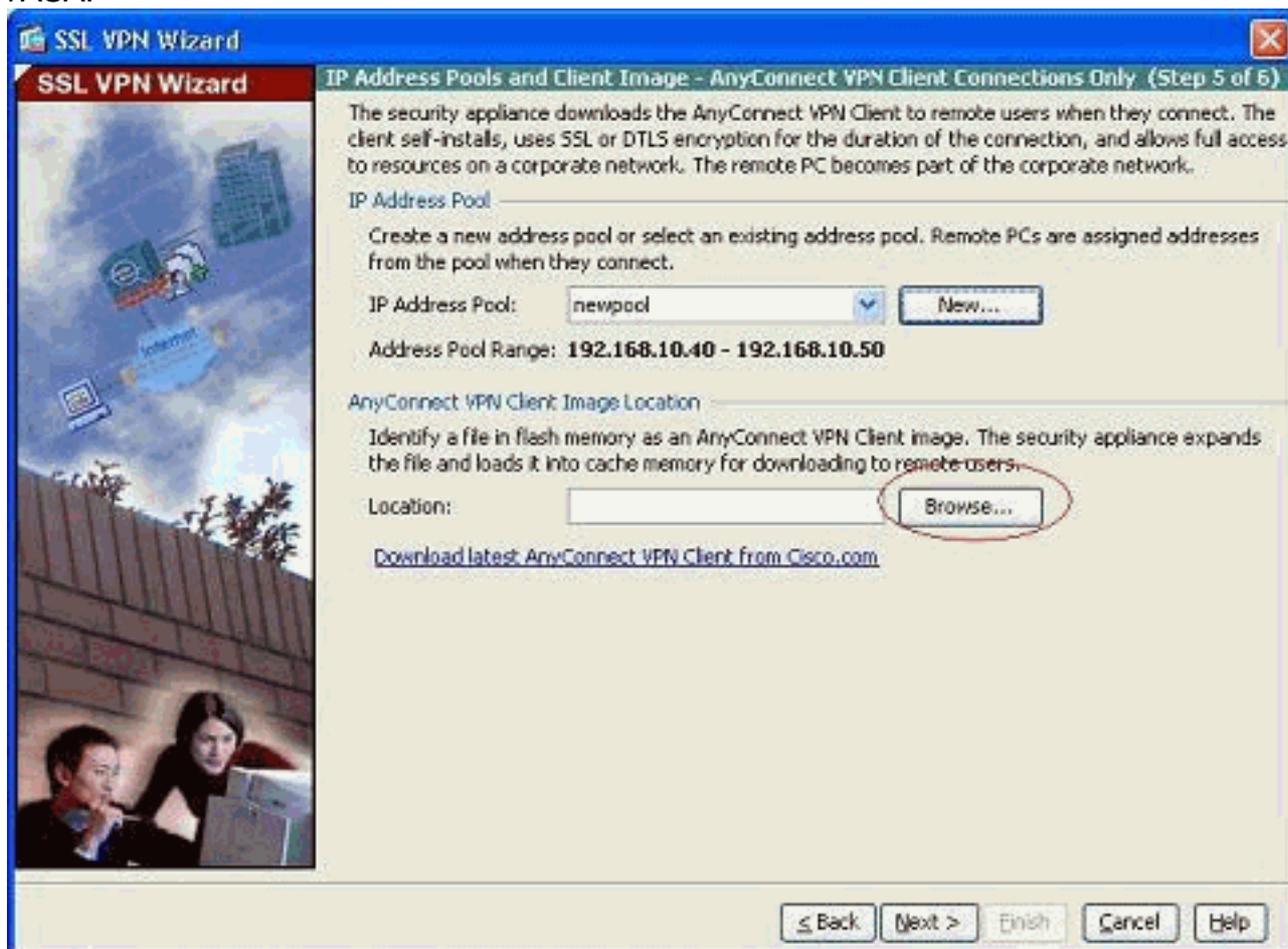
Un pool de plage 192.168.10.40-192.168.10.50 a été créé par le nom



newpool.

8. Cliquez sur **Parcourir** afin de choisir et de télécharger l'image du client VPN SSL dans la

mémoire flash de l'ASA.



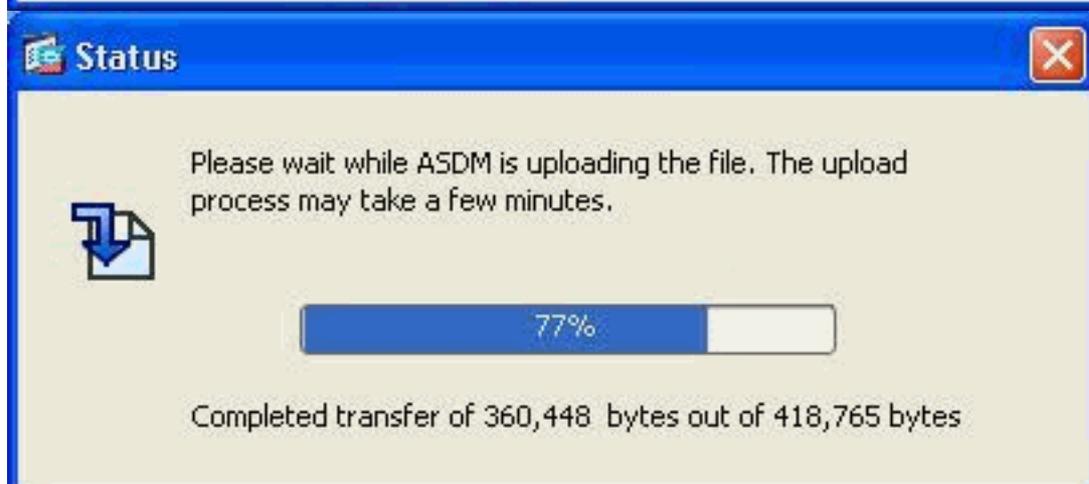
9. Cliquez sur **Upload** afin de définir le chemin d'accès au fichier à partir du répertoire local de l'ordinateur.



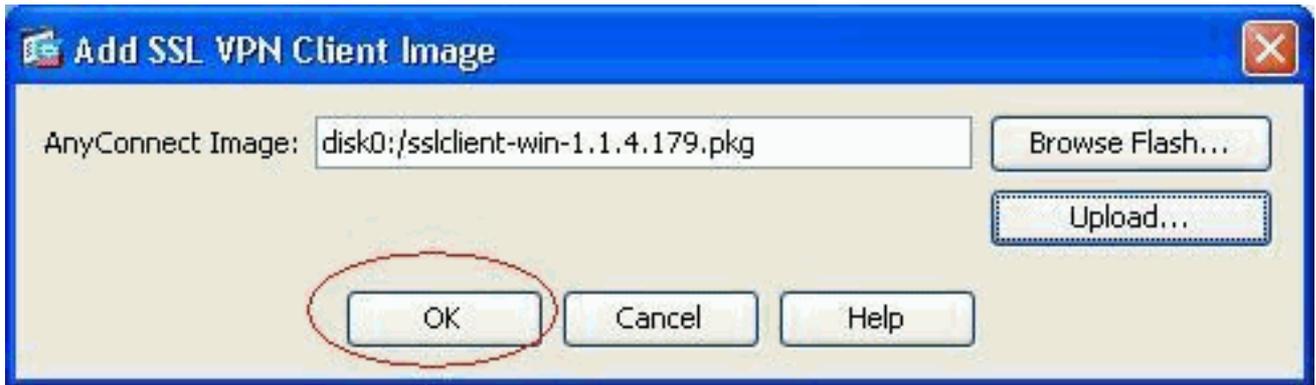
10. Cliquez sur **Parcourir les fichiers locaux** afin de sélectionner le répertoire dans lequel le fichier sslclient.pkg existe.



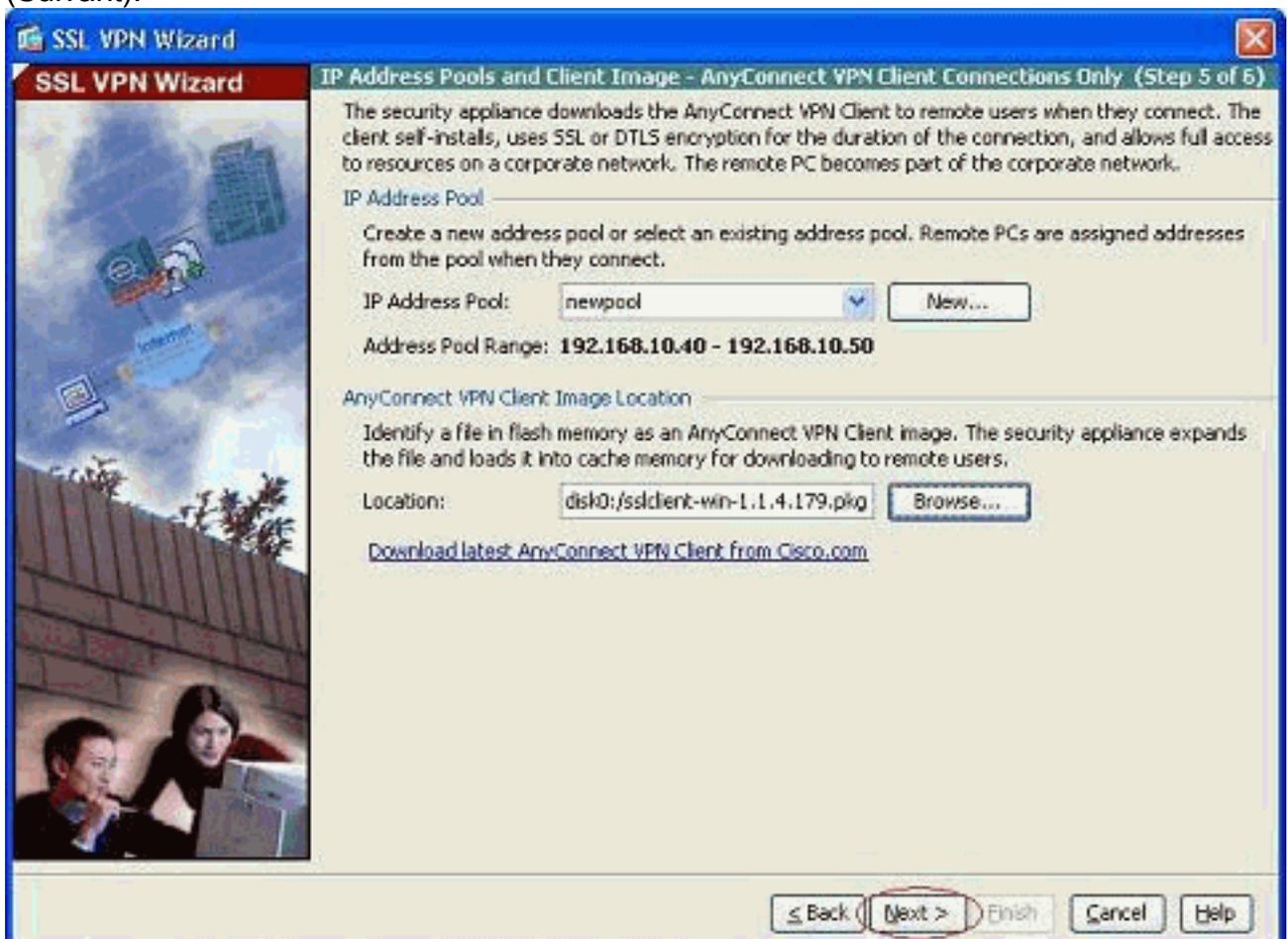
11. Cliquez sur **Upload File** afin de télécharger le fichier sélectionné dans la mémoire flash d'ASA.



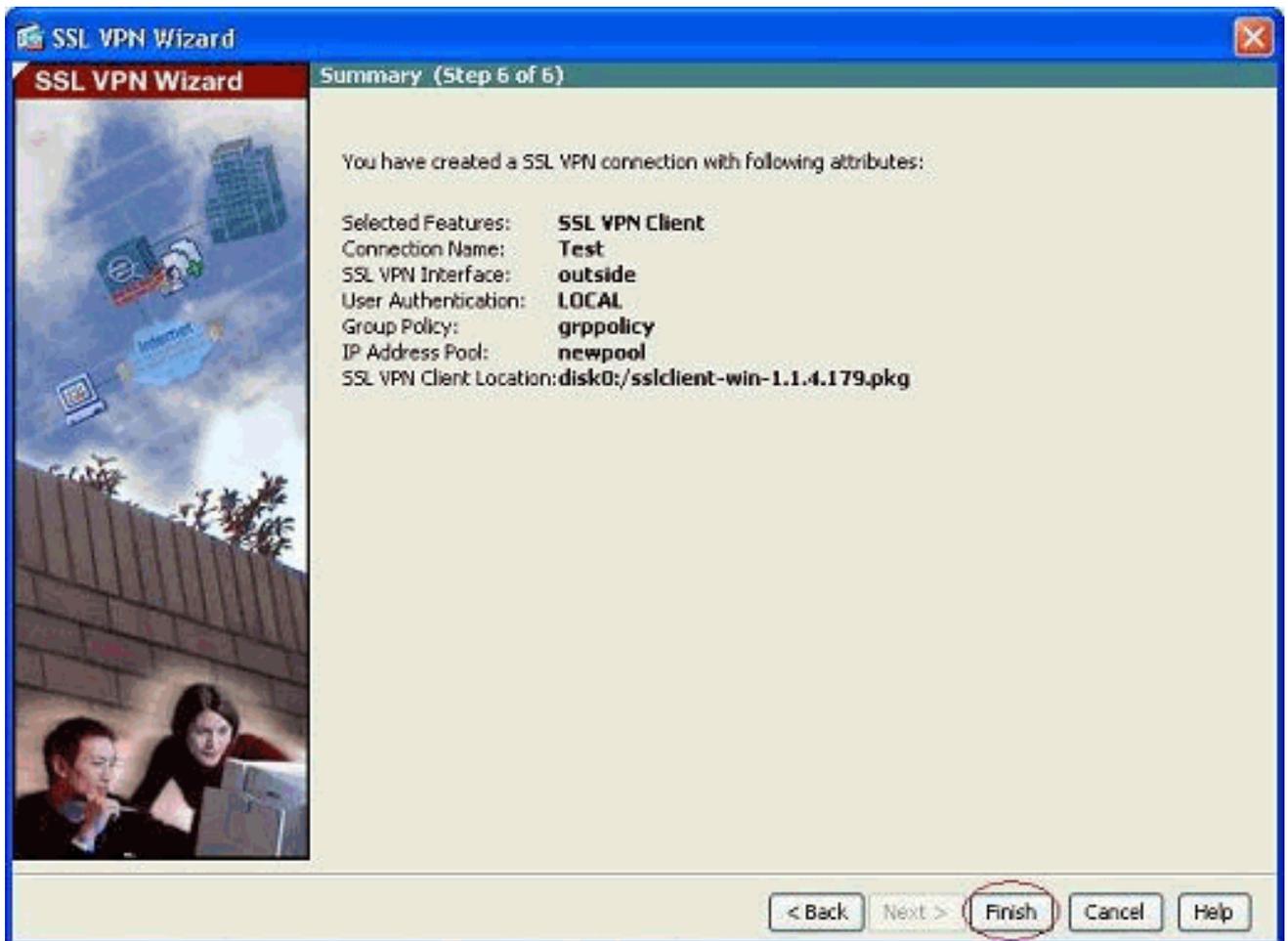
12. Une fois le fichier téléchargé sur la mémoire flash d'ASA, cliquez sur **OK** pour terminer cette tâche.



13. Il affiche maintenant le dernier fichier pkg anyconnect téléchargé sur la mémoire flash d'ASA. Cliquez sur **Next** (Suivant).



14. Le résumé de la configuration du client VPN SSL est affiché. Cliquez sur **Terminer** pour terminer l'Assistant.



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

Dans l'interface de ligne de commande, vous pouvez observer une configuration supplémentaire. La configuration complète de l'interface de ligne de commande est présentée ci-dessous et des commandes importantes ont été mises en surbrillance.

```
ciscosa

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#

```

Vérification

Les commandes indiquées 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**.

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

Dépannage

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

Informations connexes

- [Prise en charge des appareils de sécurité adaptatifs de la 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](#)