# ASA 7.2(2) : Exemple de configuration d'un client VPN SSL (SVC) pour un VPN Internet public sur un stick

## Contenu



# Introduction

Ce document décrit comment installer une appliance de sécurité adaptable (ASA) 7.2.2 pour exécuter le VPN SSL sur un bâton. Cette installation applique à un cas spécifique en lequel l'ASA ne permet pas la Segmentation de tunnel et les utilisateurs connectent directement à l'ASA avant qu'ils soient permis pour aller à l'Internet.

**Remarque:** Dans la version 7.2.2 ASA, le mot clé *intra-interface de la* commande de mode de configuration d'**autorisation du même-Sécurité-trafic** permet à tout le trafic pour écrire et quitter la même interface (pas simplement le trafic d'IPsec).

# Conditions préalables

## Conditions requises

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

- L'appliance de Sécurité du pivot ASA doit exécuter la version 7.2.2
- 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. Référez-vous à installer la section de logiciel de SVC du *guide de configuration de ligne de commande d'appareils de sécurité Cisco,* pour en savoir plus de *version 7.2*.

### Composants utilisés

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

- L'appliance de sécurité adaptable de gamme Cisco 5500 (l'ASA) cette exécute la version de logiciel 7.2(2)
- Version de Client VPN SSL Cisco pour Windows 1.1.4.179
- PC qui exécute le Windows 2000 Professional ou le Windows XP
- Version 5.2(2) 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.

Pour établir une session de SVC, l'utilisateur distant écrit l'adresse IP d'une interface de webvpn des dispositifs de sécurité dans le navigateur, et le navigateur se connecte à cette interface et affiche l'écran de connexion de webvpn. Si l'utilisateur satisfait la procédure de connexion et l'authentification, et les dispositifs de sécurité identifient l'utilisateur en tant qu'exigence du SVC, les dispositifs de sécurité téléchargent le SVC à l'ordinateur distant. Si les dispositifs de sécurité identifient l'utilisateur en tant qu'ayant l'option d'utiliser le SVC, les dispositifs de sécurité téléchargent le SVC à l'ordinateur distant tout en présentant un lien sur l'écran d'utilisateur pour ignorer l'installation de SVC.

Après l'avoir téléchargé, le SVC installe et se configure, et alors le SVC reste ou se désinstalle (selon la configuration) à partir de l'ordinateur distant quand la connexion se termine.

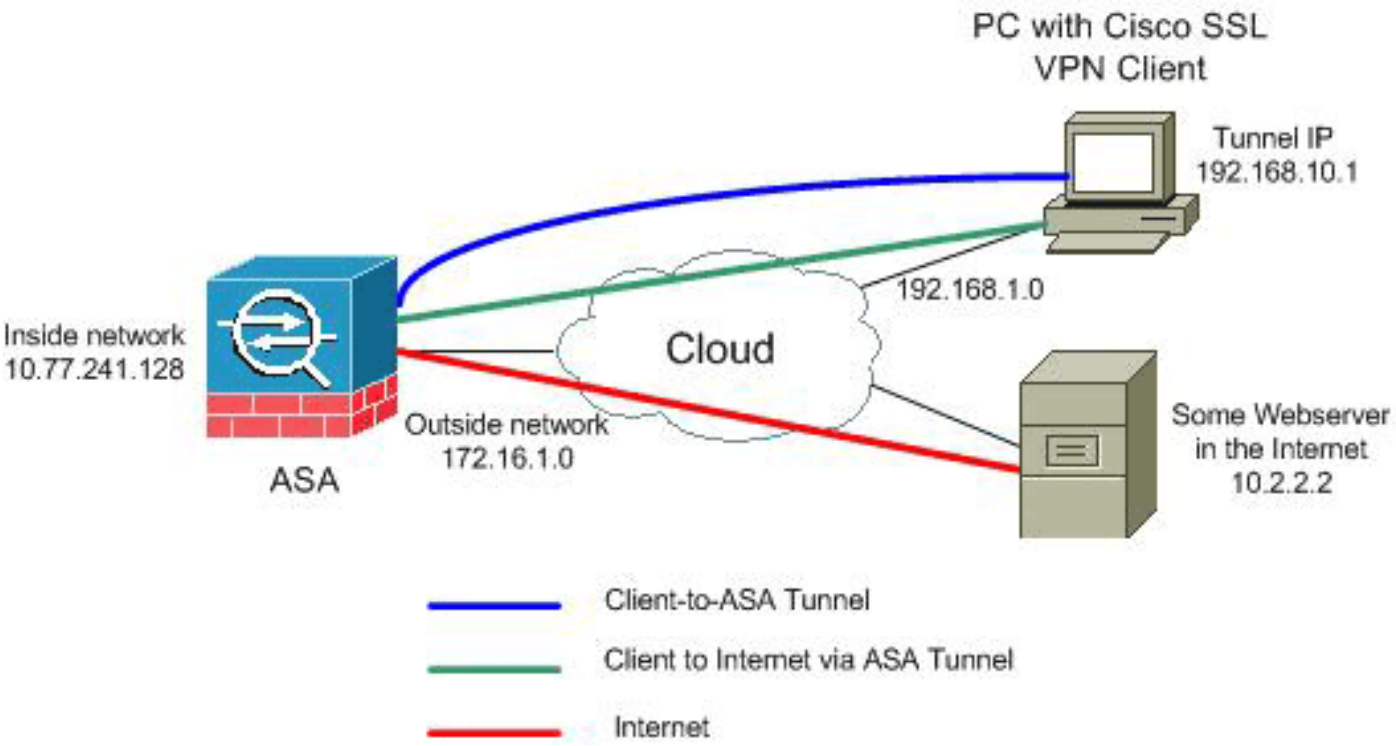
## Configurez

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 :




**Remarque:** Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

## Configurations ASA 7.2(2) utilisant l'ASDM 5.2(2)

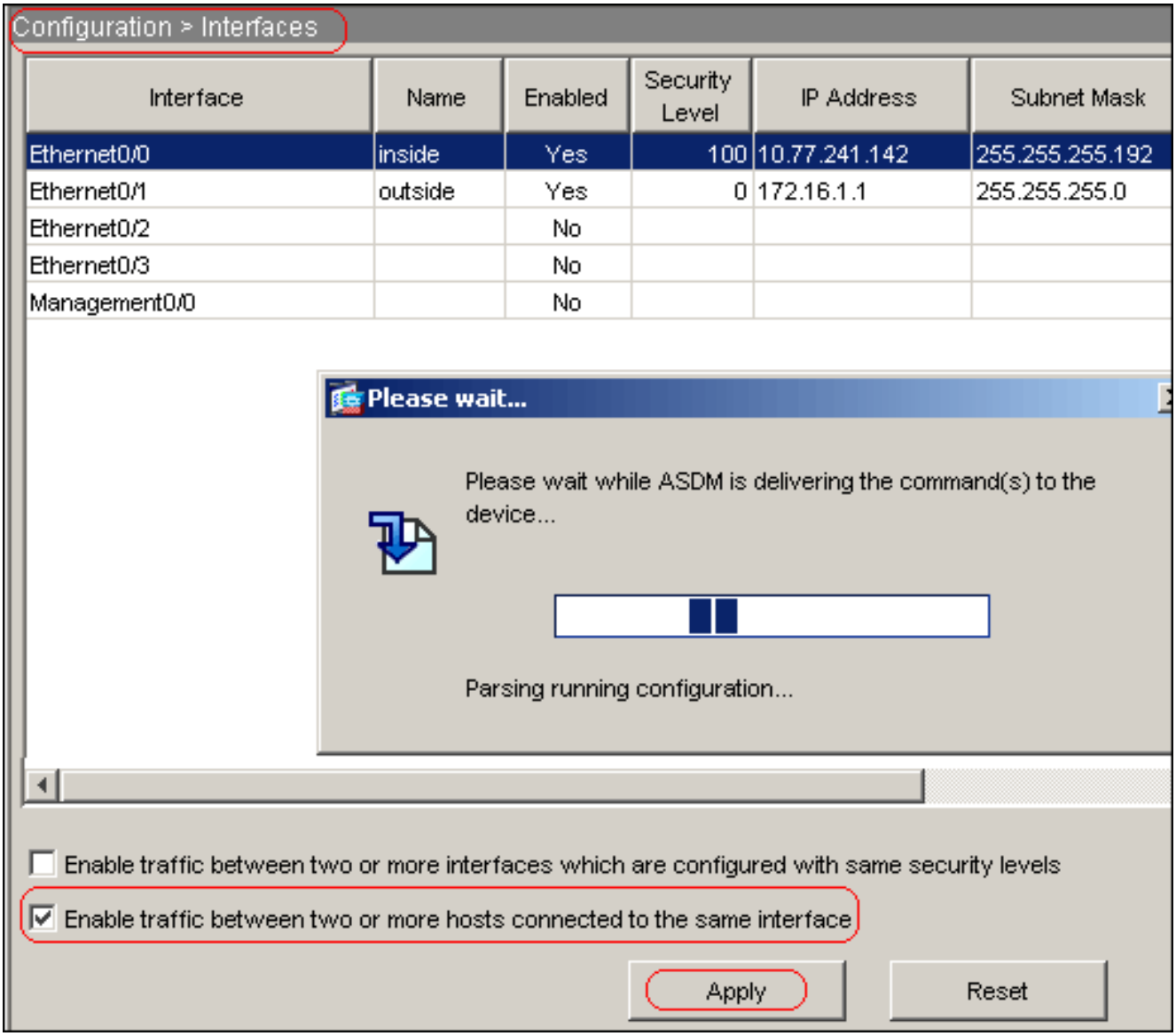
Ce document suppose les configurations de base, telles que la configuration d'interface, est déjà fait et fonctionnant correctement.

**Remarque:** Référez-vous à Permettre l'accès HTTPS pour l'ASDM afin de permettre l'ASA d'être configuré 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.

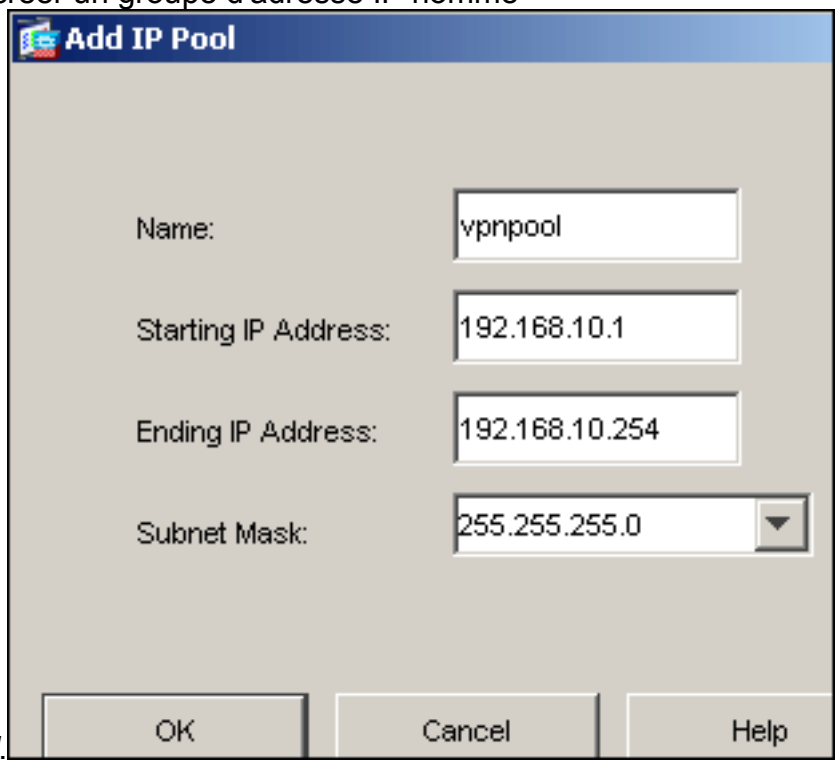
Terminez-vous ces étapes afin de configurer le VPN SSL sur un bâton dans l'ASA :

1. Choisissez le **Configuration > Interfaces**, et cochent le **trafic d'enable entre deux hôtes ou plus connectés dans la même** case d'**interface** afin de permettre au trafic de VPN SSL pour écrire et quitter la même interface.
2. Cliquez sur
   **Apply**.

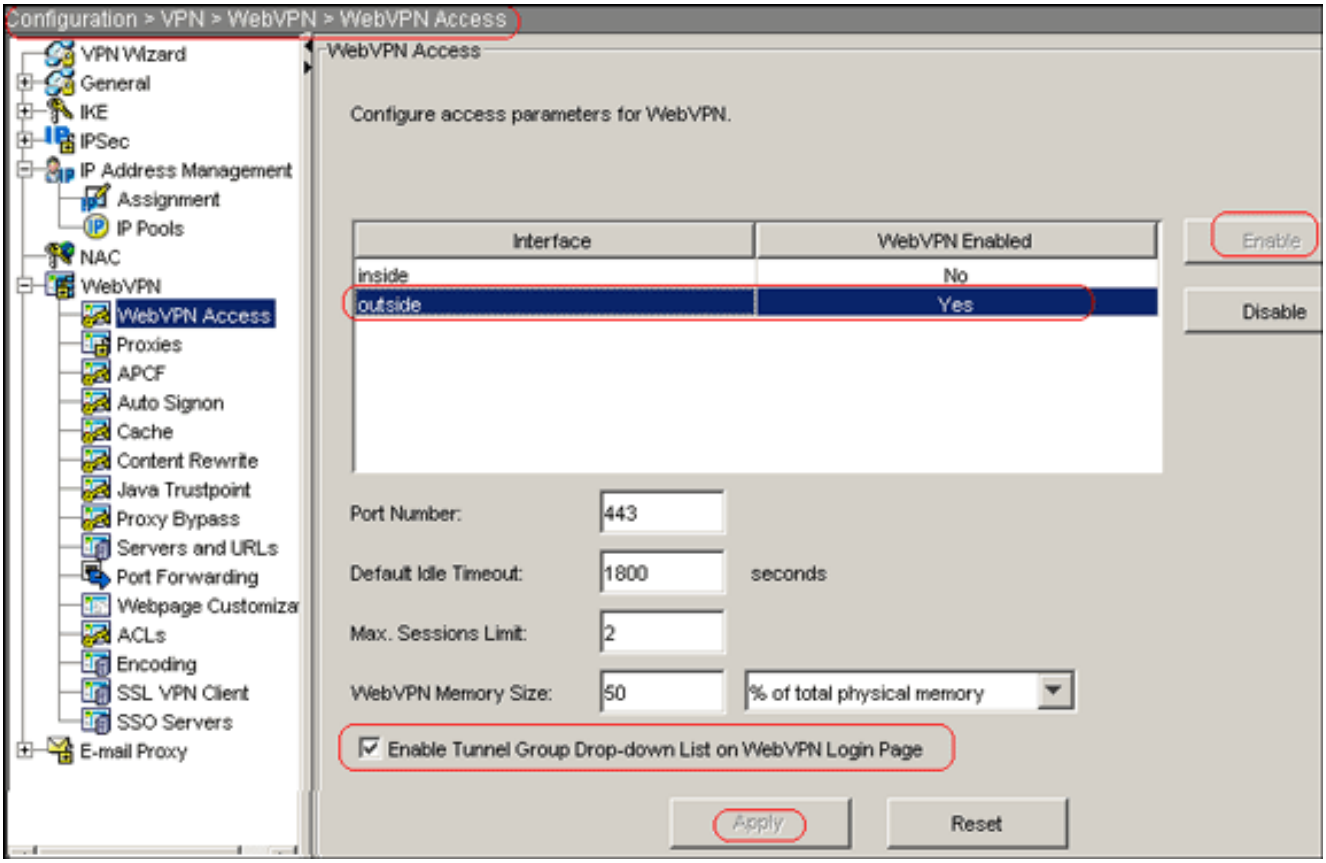



**Remarque:** Voici la commande de configuration équivalente CLI :

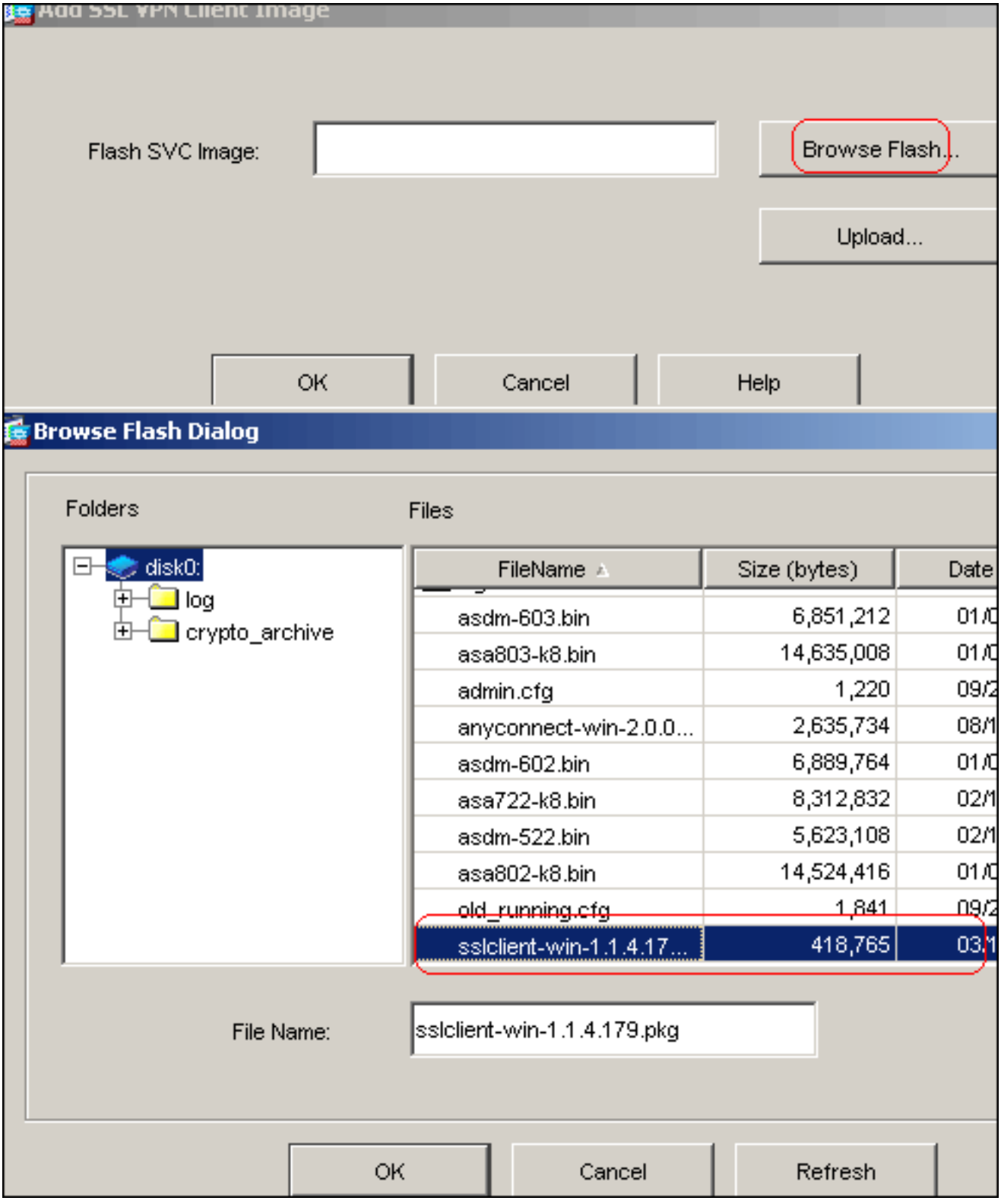
3. Choisissez la **configuration > le VPN > la gestion d'adresse IP > les groupes IP > ajoutent** afin de créer un groupe d'adresse IP nommé *vpnpool*.



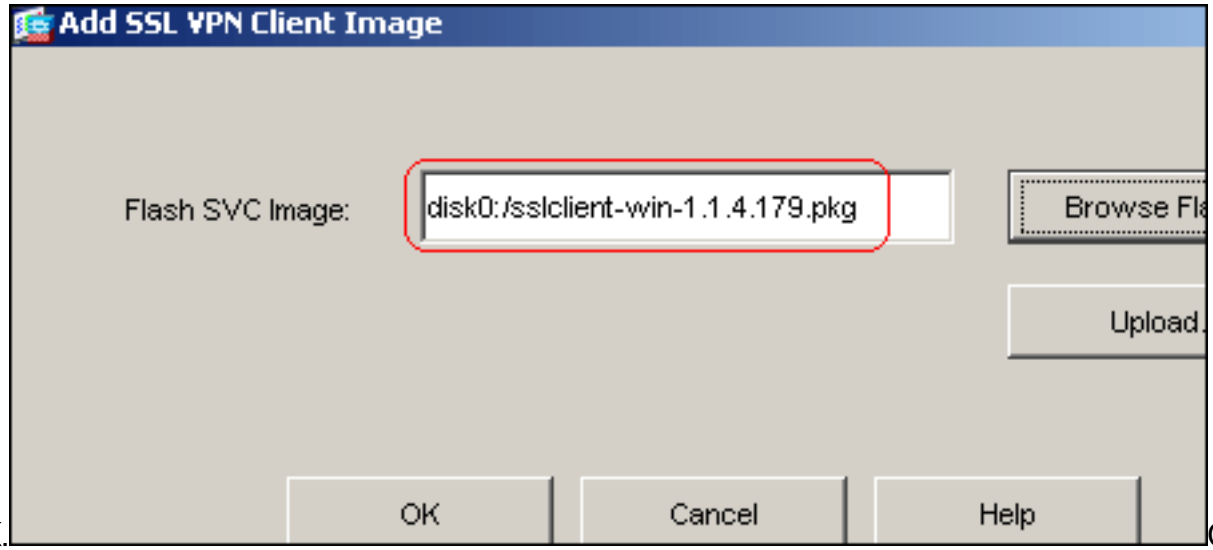
4. Cliquez sur **Apply**.**Remarque:** Voici la commande de configuration équivalente CLI :
5. Webvpn d'enable :Choisissez la **configuration > le VPN > le webvpn > le webvpn Access**, et sélectionnez l'interface extérieure.**Enable de** clic.Cochez la **liste déroulante de groupe de tunnel d'enable sur la** case de **page de connexion de webvpn** afin de permettre à des utilisateurs pour choisir leurs groupes respectifs de la page de connexion.



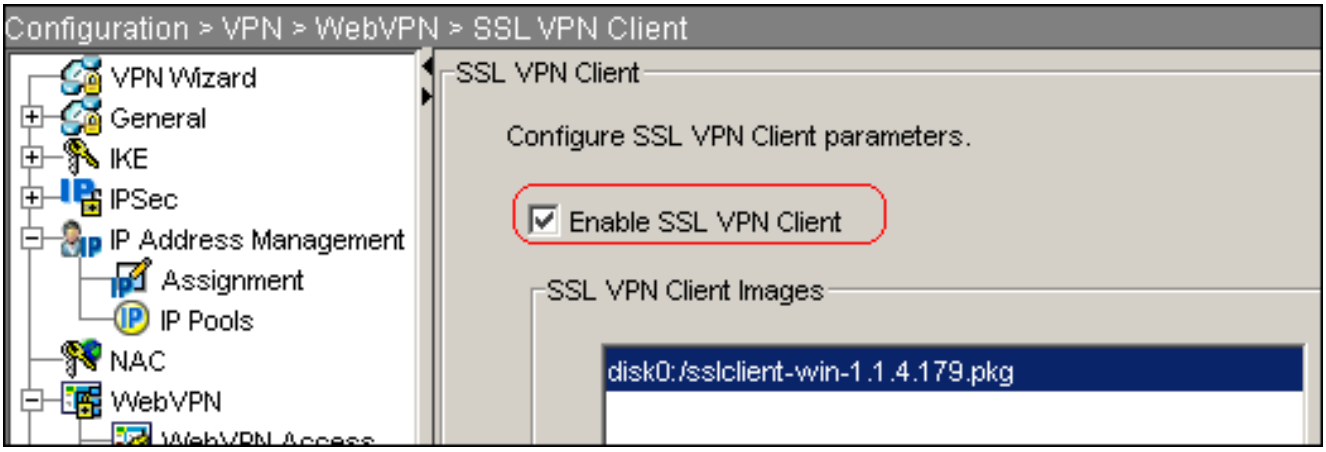

Cliquez sur **Apply**.Choisissez la **configuration > le VPN > le webvpn > le client de VPN SSL > ajoutent** afin d'ajouter l'image de client de VPN SSL de la mémoire flash de l'ASA.


Add SSL VPN Client Image
Flash SVC Image:
Browse Flash...
Upload...
OK
Cancel
Help
Browse Flash Dialog
Folders
Files
disk0:
log
crypto_archive
FileName
Size (bytes)
Date
asdm-603.bin 6,851,212
asa803-k8.bin 14,635,008
admin.cfg 1,220
anyconnect-win-2.0.0... 2,635,734
asdm-602.bin 6,889,764
asa722-k8.bin 8,312,832
asdm-522.bin 5,623,108
asa802-k8.bin 14,524,416
old_running.cfg 1,841
sslclient-win-1.1.4.17... 418,765
File Name:
sslclient-win-1.1.4.179.pkg
OK
Cancel
Refresh

Cliquez sur

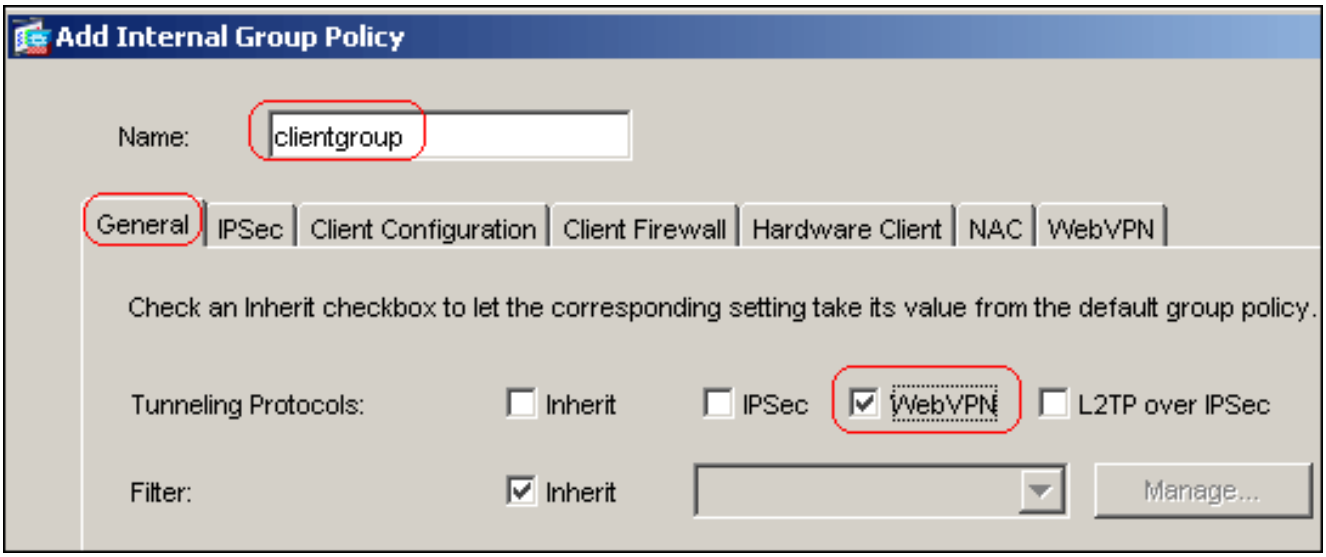



**OK**.Cliquez sur **OK**.Case de **client de VPN SSL de** clic.



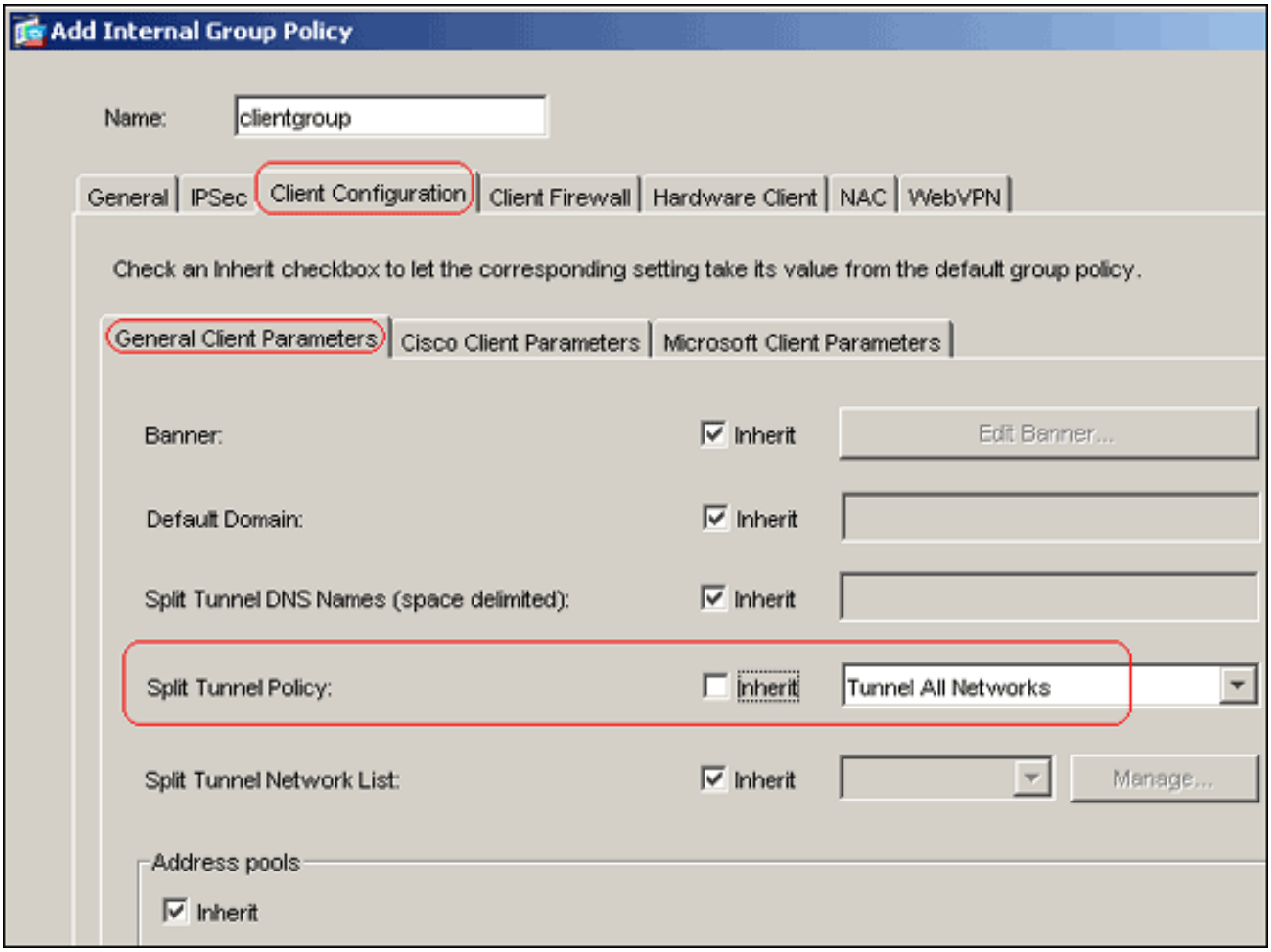

**Remarque:** Voici les commandes de configuration équivalentes CLI :

6. Configurez la stratégie de groupe :Choisissez le **Configuration > VPN > General > Group Policy > ajoutent (stratégie de groupe interne)** afin de créer une stratégie de groupe interne nommée *clientgroup*.Cliquez sur l'**onglet Général**, et sélectionnez la case de **webvpn** afin d'activer le webvpn comme protocole de Tunnellisation.

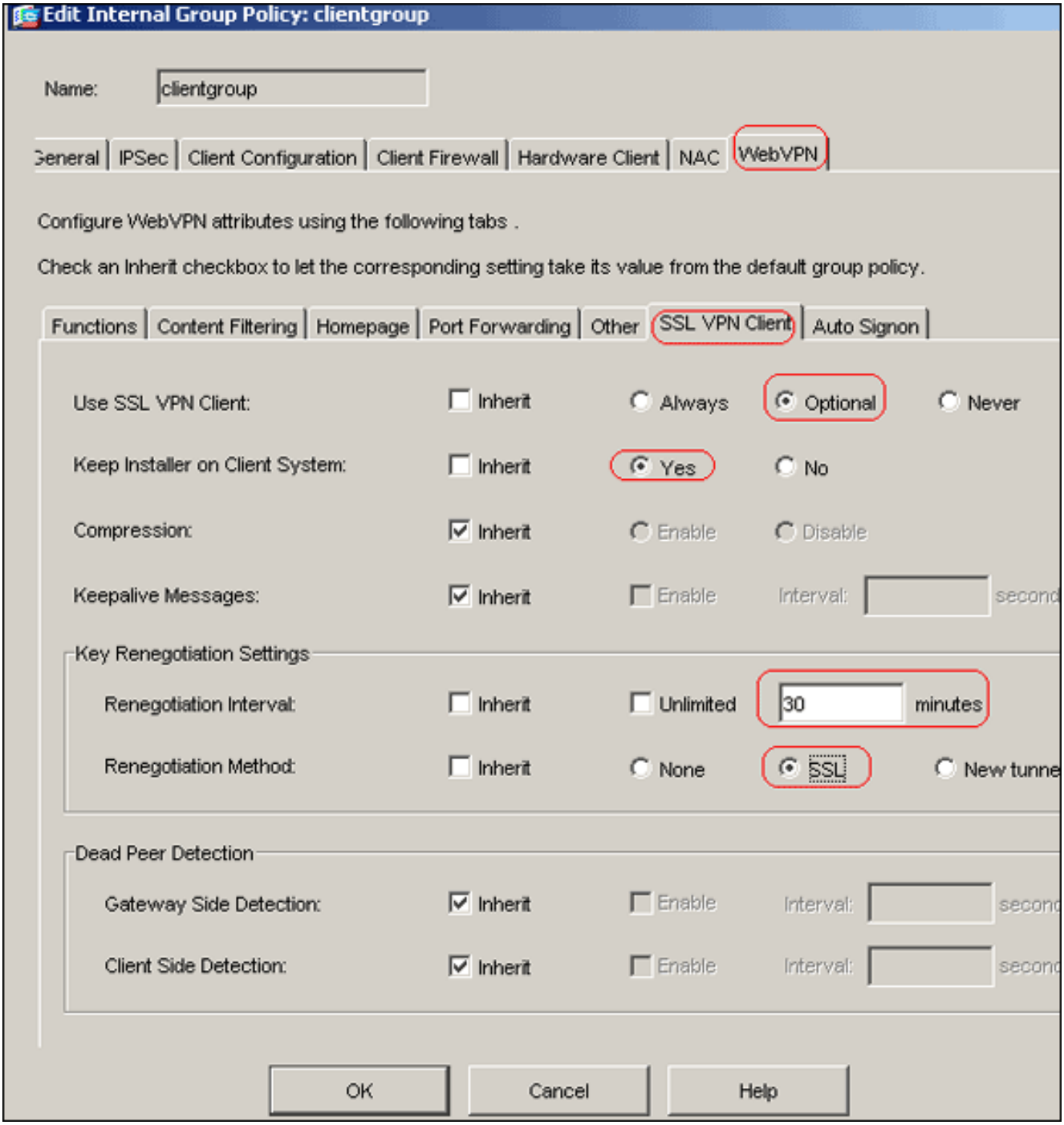



Cliquez sur l'onglet de **configuration de client**, et puis cliquez sur l'onglet du **Général Client Parameters**.Choisissez le **tunnel tous les réseaux de la** liste déroulante de stratégie de tunnel partagé afin de faire tous les paquets voyager à partir de l'ordinateur distant par un

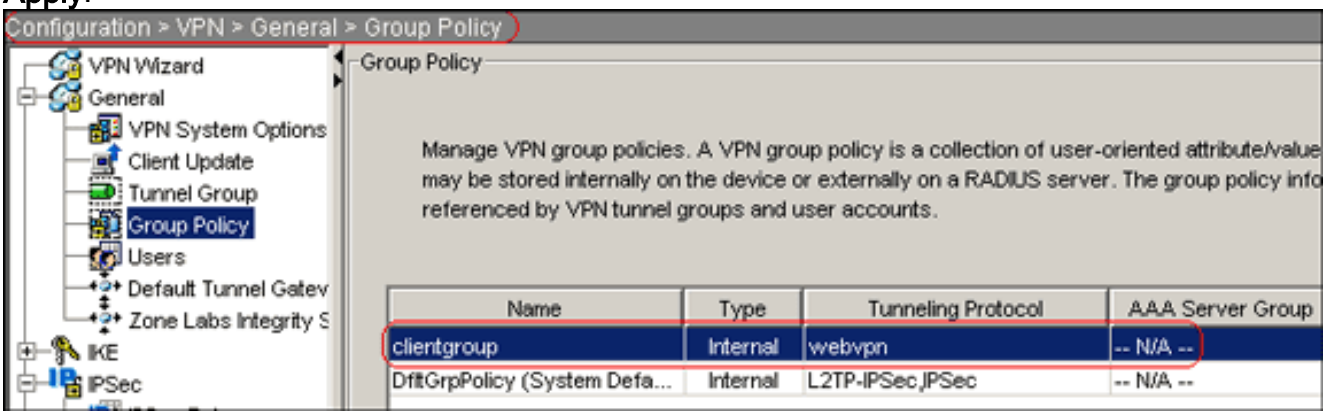
tunnel
sécurisé.




Cliquez sur l'onglet de **webvpn > de client SSLVPN**, et choisissez ces options :Pour l'option Use SSL VPN Client, désélectionnez la case à cocher **Inherit**, puis cliquez sur la case d'option **Optional**.Cette option permet au client distant pour choisir si télécharger le SVC. Le choix *Always* permet de s'assurer que le SVC est téléchargé sur le poste de travail distant pendant chaque connexion VPN SSL.Pour l'option de Keep Installer on Client System, décochez la case d'**héritage**, et cliquez sur la case d'option d'**oui**Cette option permet au logiciel de SVC pour demeurer sur la machine cliente. Par conséquent, il n'est pas nécessaire que l'ASA télécharge le logiciel SVC sur le client chaque fois qu'une connexion est établie. Cette option est un bon choix pour les utilisateurs distants qui accèdent souvent au réseau de l'entreprise.Pour l'option Renegotiation Interval, décochez la case **Inherit**, décochez la case à cocher **Unlimited** et saisissez le nombre de minutes jusqu'à une nouvelle saisie.**Remarque:** La sécurité est améliorée en fixant des limites à la durée de validité d'une clé.Pour l'option Renegotiation Method, décochez la case à cocher **Inherit** et cliquez la case d'option **SSL**.**Remarque:** La renégociation peut utiliser le tunnel actuel SSL ou un nouveau tunnel créé spécifiquement pour la renégociation.Vos attributs client VPN SSL doivent être configurés tel qu´indiqué sur cette image
:



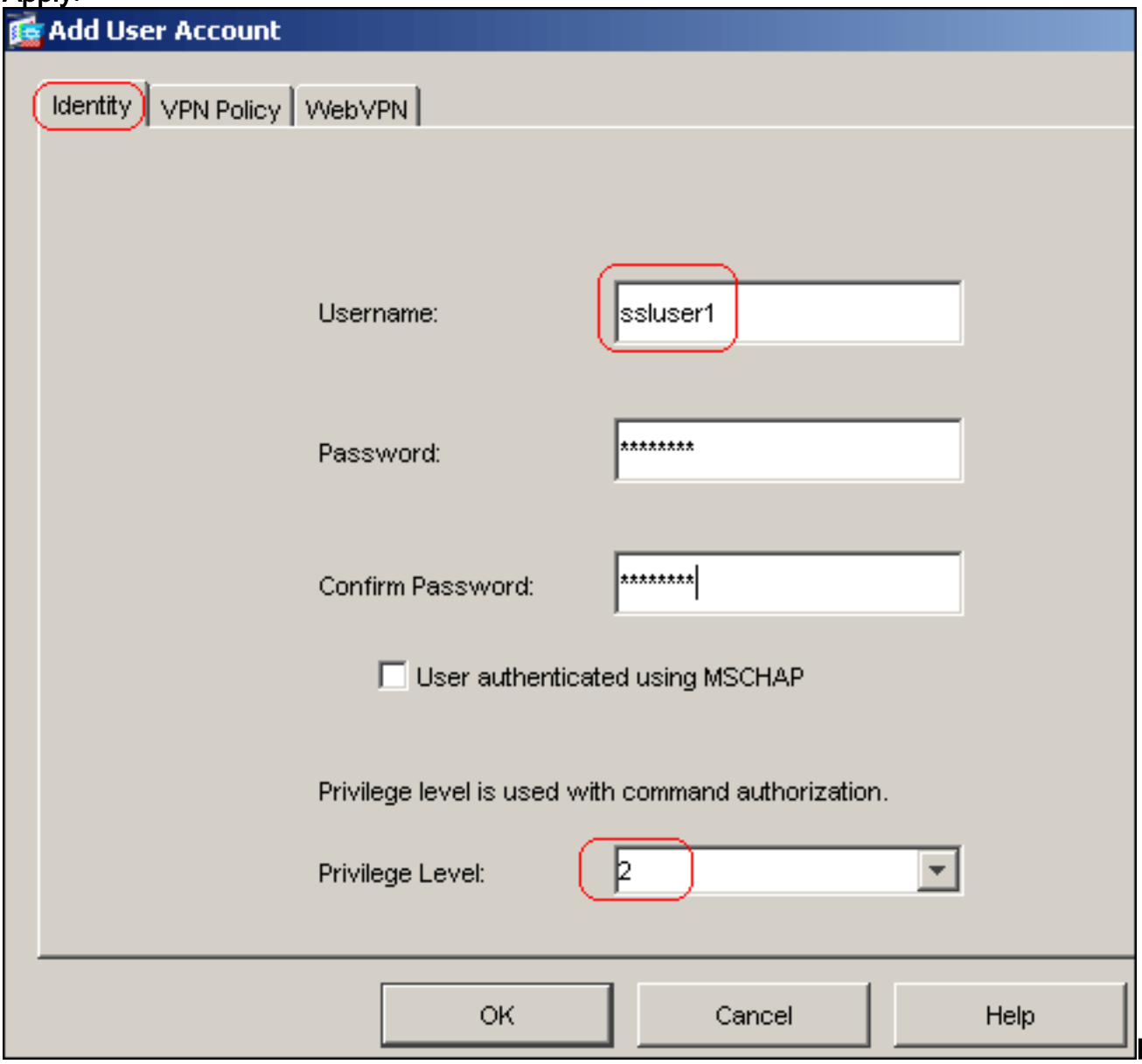

Cliquez sur **OK**, puis sur **Apply**.




**Remarque:** Voici les commandes de configuration équivalentes CLI :

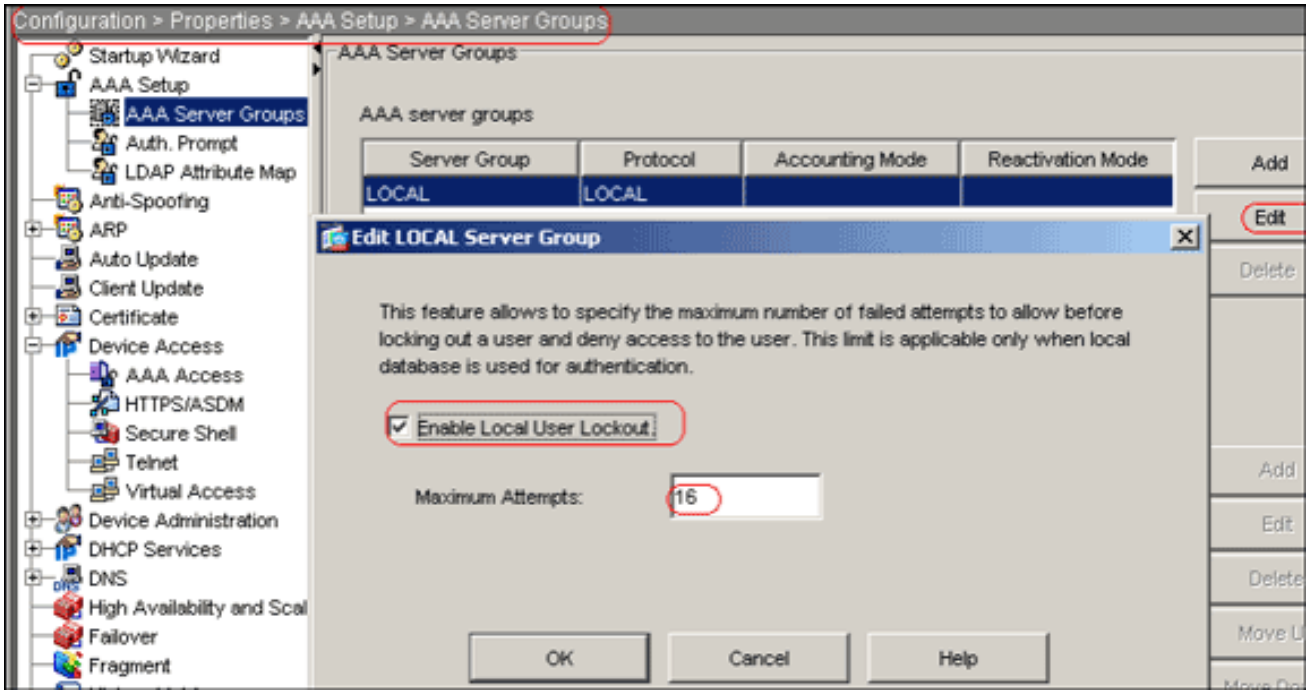
7. Choisissez la **configuration > le VPN > le général > les utilisateurs > ajoutent** afin de créer un nouveau compte utilisateur *ssluser1*.

8. Cliquez sur **OK**, puis sur **Apply**.



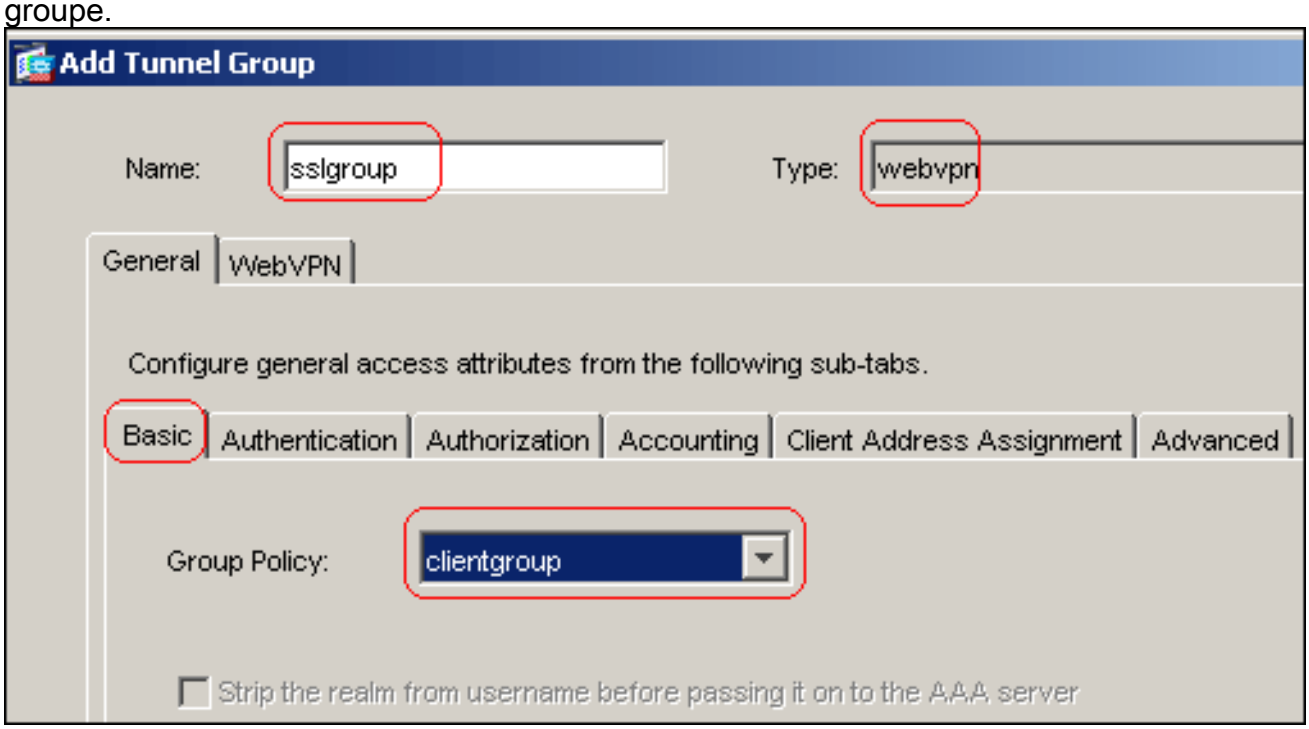

**Remarque:** Voici la commande équivalente CLI :

9. Choisissez la **configuration > le Properties > l'AAA installé > des groupes de serveurs d'AAA > éditent**.
10. Sélectionnez les les *GENS DU PAYS* par défaut de groupe de serveurs, et cliquez sur Edit.
11. Dans la boîte de dialogue de groupe de serveur local d'éditer, cliquez sur la case de **verrouillage d'utilisateur local d'enable**, et écrivez 16 dans la zone de texte maximum de tentatives.
12. Cliquez sur **OK**.

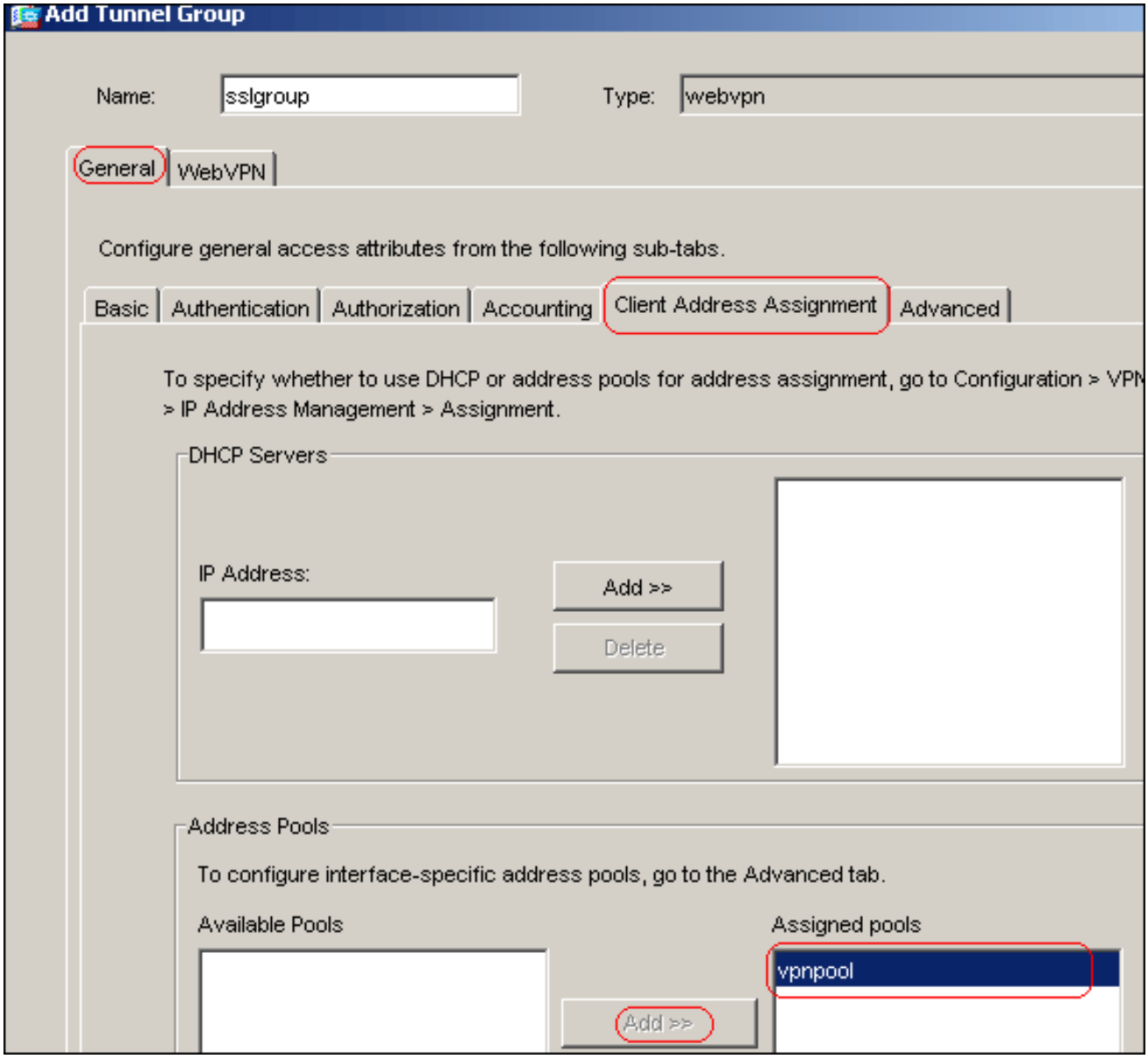



**Remarque:** Voici la commande équivalente CLI :

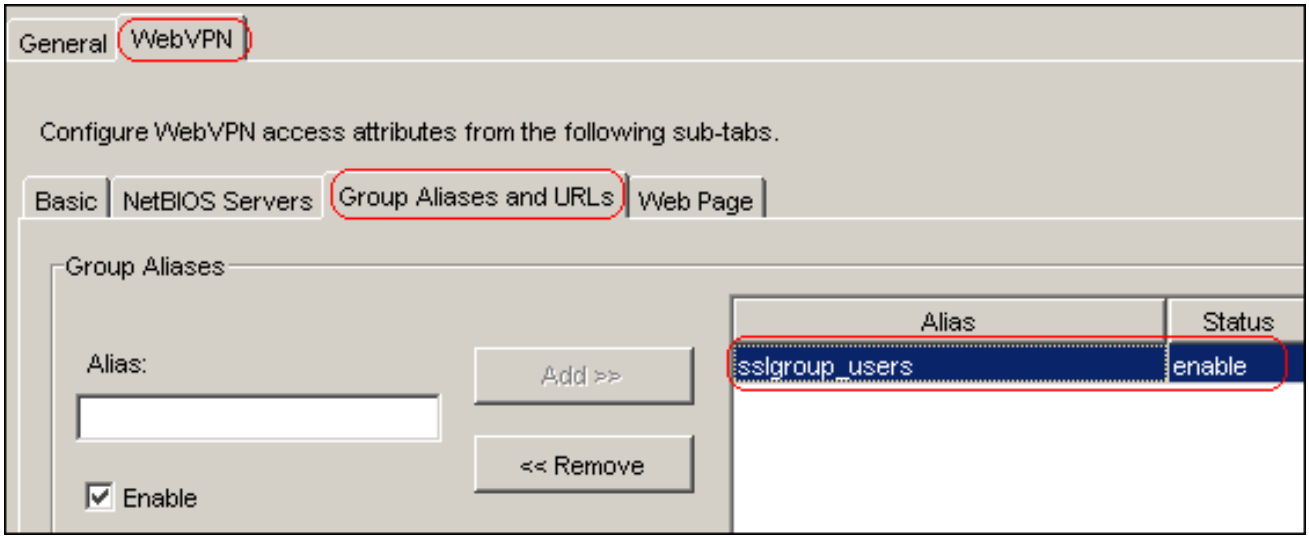
13. Configurez le groupe de tunnel :Choisissez la **configuration > le VPN > le groupe de général > de tunnel > ajoutent (accès de webvpn)** afin de créer un nouveau groupe de tunnel nommé *sslgroup*.Cliquez sur l'**onglet Général**, et puis cliquez sur l'onglet **de base**.Choisissez le **clientgroup de la** liste déroulante de stratégie de groupe.




Cliquez sur l'**onglet Client Address Assignment**, et puis cliquez sur Add afin d'assigner le *vpnpool* disponible de pool d'adresses.



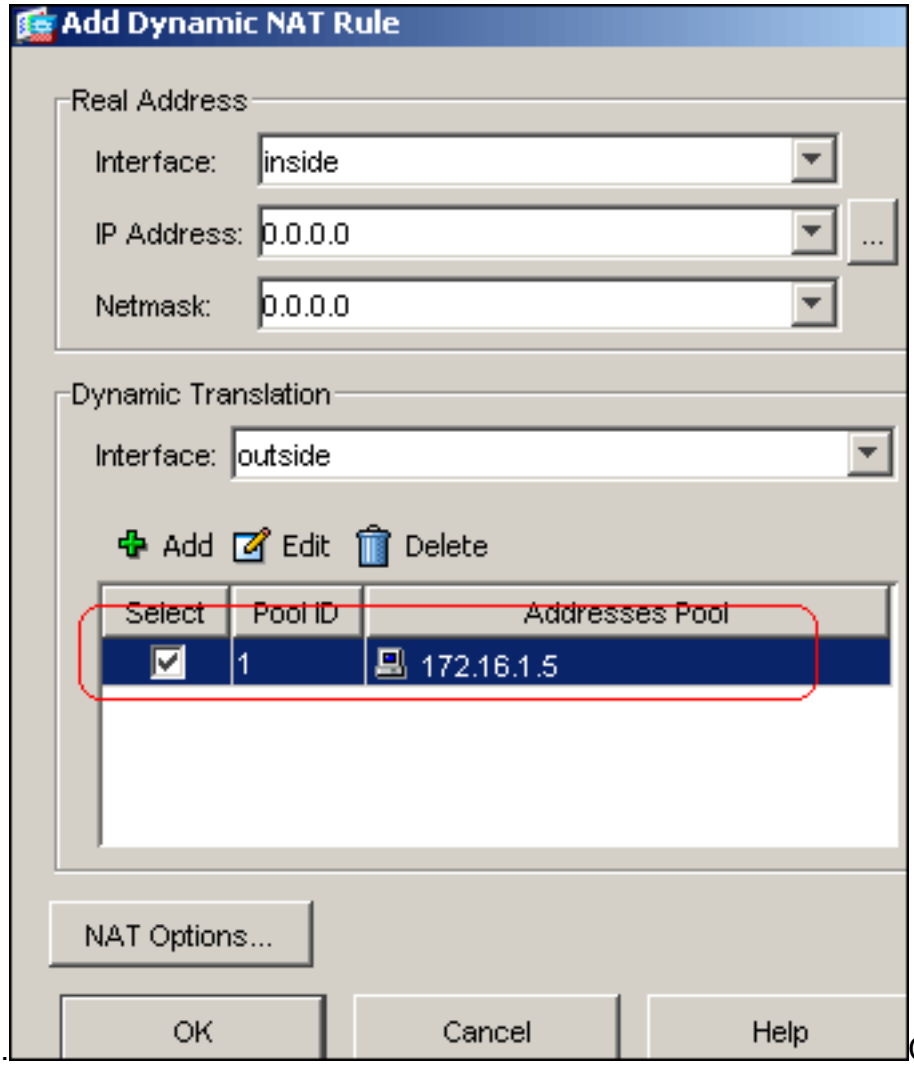

Cliquez sur l'onglet de **webvpn**, et puis cliquez sur l'onglet de **pseudonymes et URLs de groupe**.Introduisez le pseudonyme dans la case de paramètre, et cliquez sur Add afin de l'ajouter à la liste de noms de groupe sur la page de connexion.



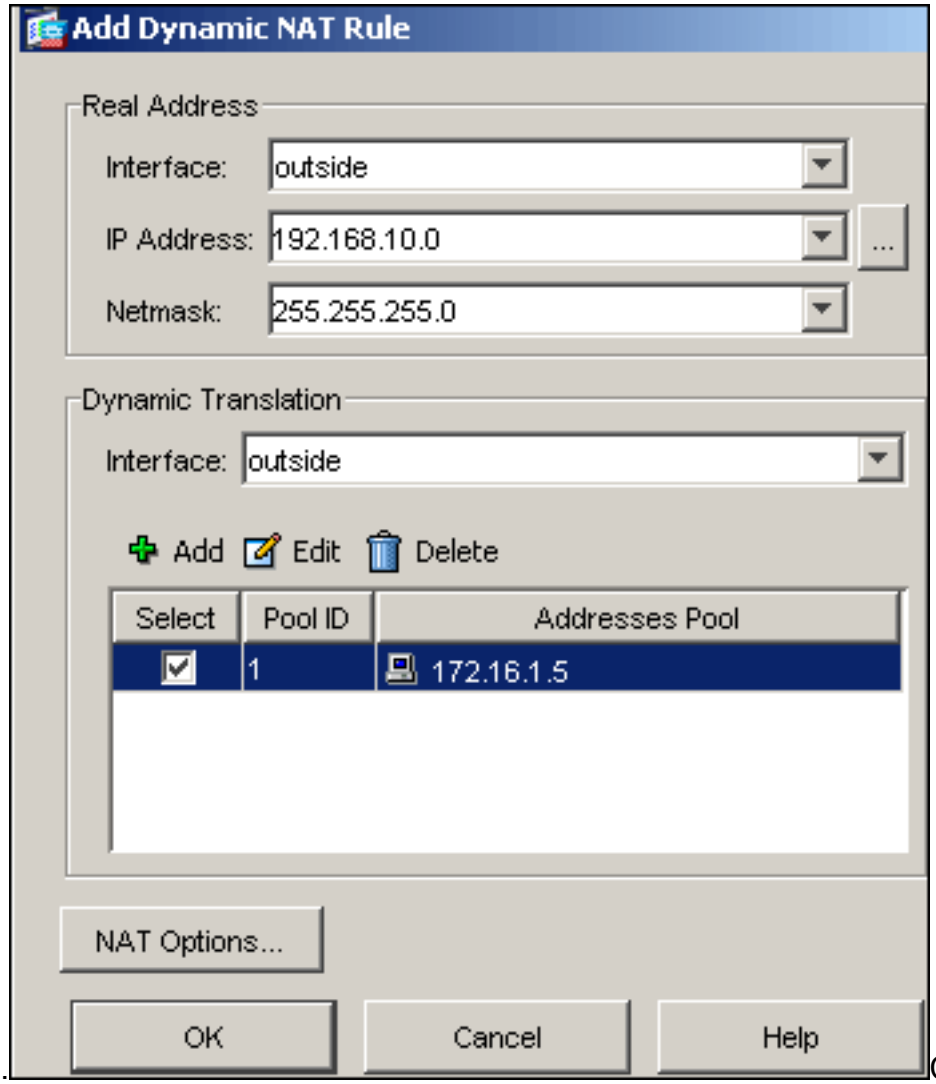

Cliquez sur **OK**, puis sur **Apply**.**Remarque:** Voici les commandes de configuration équivalentes CLI :

14. Configurez NAT :Choisissez le **Configuration > NAT > ajoutent > ajoutent la règle NAT**

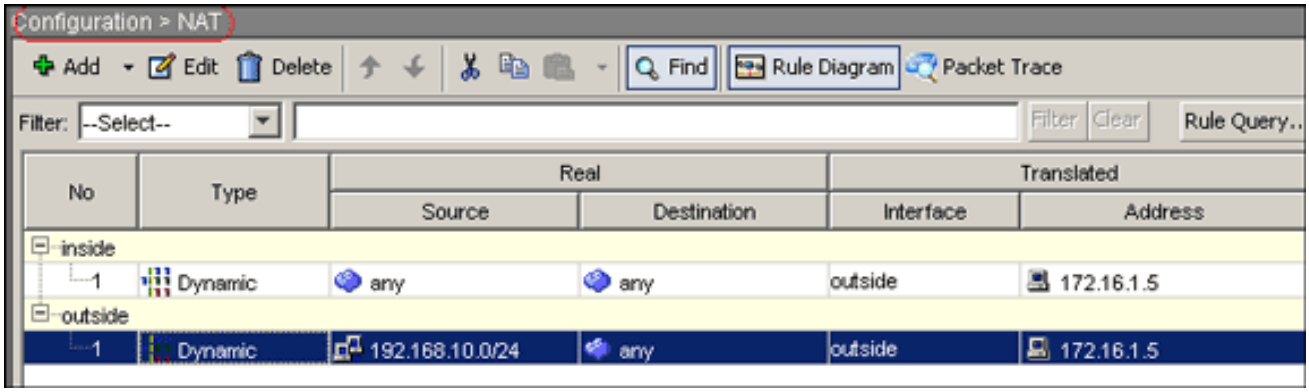
**dynamique** de permettre le trafic qui provient le réseau intérieur à traduire avec l'utilisation de l'adresse IP extérieure




172.16.1.5. Cliquez sur **OK**.Choisissez le **Configuration > NAT > ajoutent > ajoutent la règle NAT dynamique** de permettre le trafic qui provient le réseau extérieur 192.168.10.0 à traduire avec l'utilisation de l'adresse IP extérieure




172.16.1.5.Cliquez sur **OK**.




Cliquez sur **Apply**.**Remarque:** Voici les commandes de configuration équivalentes CLI :

## Configuration ASA 7.2(2) CLI

| Cisco ASA 7.2(2) |
| --- |
| ciscoasa#**show running-config**<br>: Saved<br>:<br>ASA Version 7.2(2)<br>!<br>hostname ciscoasa<br>enable password 8Ry2YjIyt7RRXU24 encrypted<br>names<br>! |

```
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter
!--- and exit the same interface. access-list 100
extended permit icmp any any pager lines 24 mtu inside
1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients. no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.bin no asdm history enable arp
timeout 14400 global (outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !---
(the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal
```

```
!--- Create an internal group policy "clientgroup."
group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelall

!--- Encrypt all the traffic coming from the SSL VPN
Clients. webvpn
  svc required

!--- Activate the SVC under webvpn mode svc keep-
installer installed

!--- When the security appliance and the SVC perform a
rekey, they renegotiate !--- the crypto keys and
initialization vectors, increasing the security of !---
the connection. svc rekey time 30

--- Command that specifies the number of minutes from
the start of the !--- session until the rekey takes
place, from 1 to 10080 (1 week).  svc rekey method ssl

!--- Command that specifies that SSL renegotiation takes
place during SVC rekey. username ssluser1 password
ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1." aaa local
authentication attempts max-fail 16

!--- Enable the AAA local authentication. http server
enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart tunnel-
group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as
WebVPN. tunnel-group sslgroup general-attributes
 address-pool vpnpool

!--- Associate the address pool vpnpool created.
default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created.
tunnel-group sslgroup webvpn-attributes

 group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users. telnet
timeout 5 ssh timeout 5 console timeout 0 ! 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
webvpn
 enable outside

!--- Enable WebVPN on the outside interface. svc image
disk0:/sslclient-win-1.1.4.179.pkg 1
```

```
!--- Assign an order to the SVC image. svc enable

!--- Enable the security appliance to download SVC
images to remote computers. tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the
WebVPN Login page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

## Établir la connexion VPN SSL avec SVC

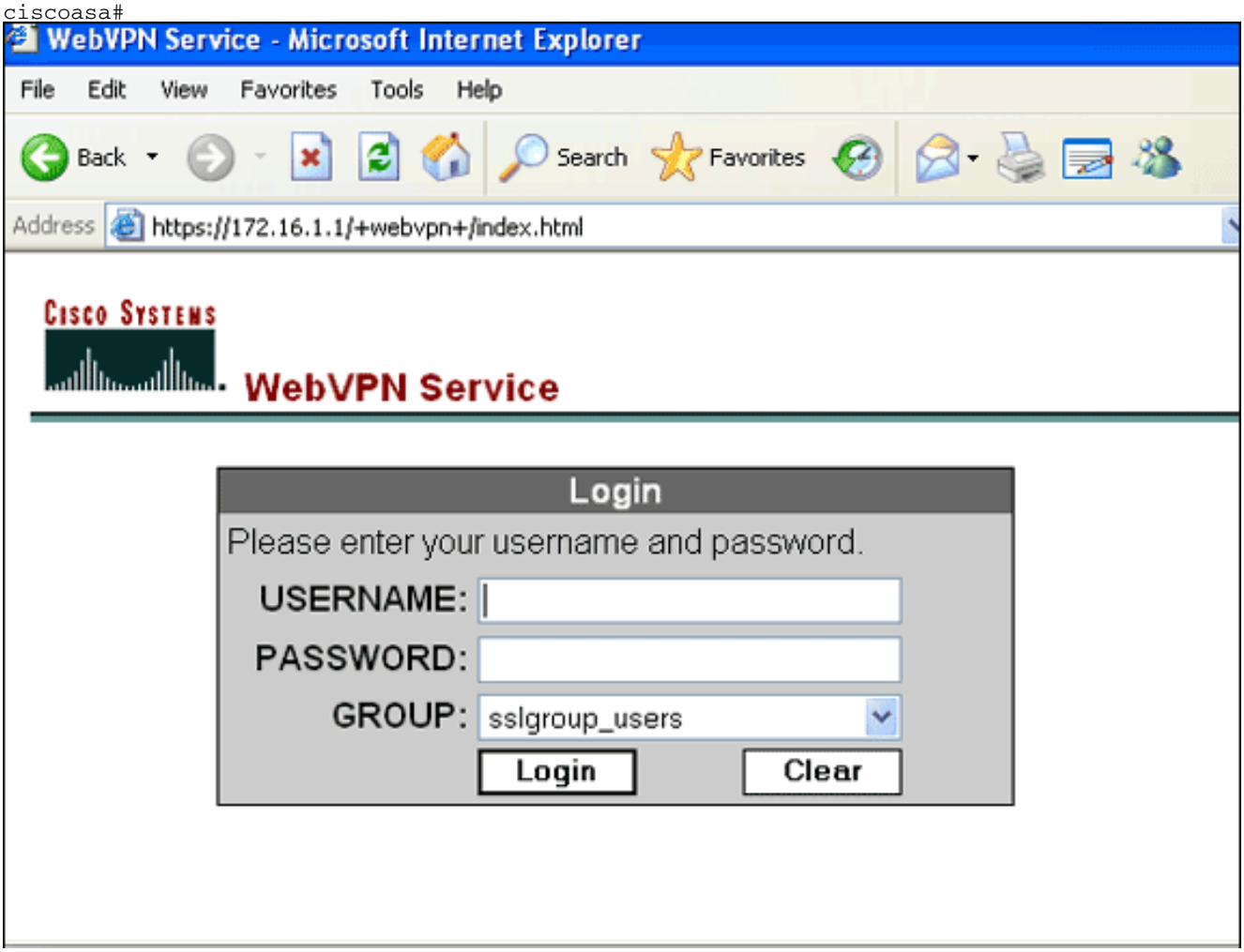
Terminez-vous ces étapes afin d'établir une connexion de VPN SSL avec l'ASA.

1. Saisissez la zone adresse de votre navigateur Web l'URL ou l'adresse IP pour l'interface de webvpn de l'ASA.Exemple :`ciscoasa#show running-config`

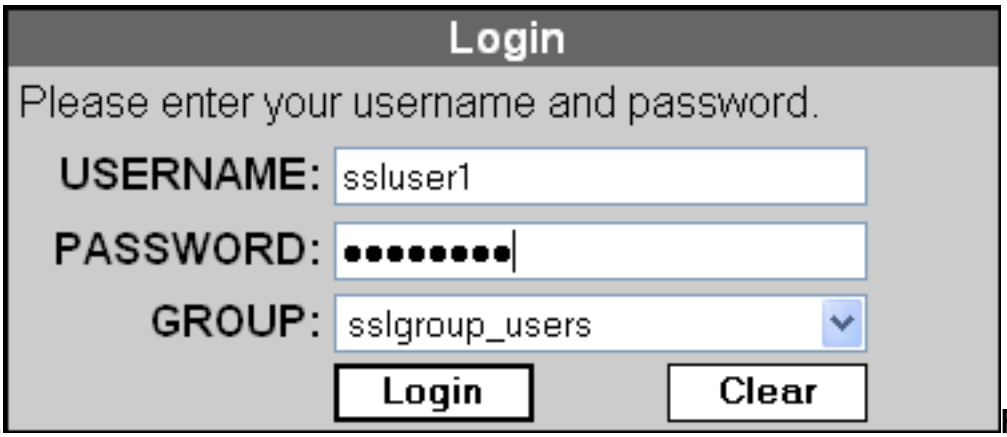
```
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter !--- and exit the same interface.
access-list 100 extended permit icmp any any pager lines 24 mtu inside 1500 mtu outside
1500 ip local pool vpnpool 192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients. no failover icmp unreachable rate-limit 1
```

```
burst-size 1 asdm image disk0:/asdm-522.bin no asdm history enable arp timeout 14400 global
(outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN Clients. !--- Note: Uses an RFC
1918 range for lab setup. !--- Apply an address from your public range provided by your
ISP. nat (inside) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !--- (the addresses from vpn-pool). nat
(outside) 1 192.168.10.0 255.255.255.0

access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup." group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-policy tunnelall

!--- Encrypt all the traffic coming from the SSL VPN Clients. webvpn
  svc required

!--- Activate the SVC under webvpn mode svc keep-installer installed

!--- When the security appliance and the SVC perform a rekey, they renegotiate !--- the
crypto keys and initialization vectors, increasing the security of !--- the connection. svc
rekey time 30

--- Command that specifies the number of minutes from the start of the !--- session until
the rekey takes place, from 1 to 10080 (1 week).  svc rekey method ssl

!--- Command that specifies that SSL renegotiation takes place during SVC rekey. username
ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1." aaa local authentication attempts max-fail 16

!--- Enable the AAA local authentication. http server enable http 0.0.0.0 0.0.0.0 inside no
snmp-server location no snmp-server contact snmp-server enable traps snmp authentication
linkup linkdown coldstart tunnel-group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as WebVPN. tunnel-group sslgroup general-
attributes
 address-pool vpnpool

!--- Associate the address pool vpnpool created. default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-
attributes

 group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console
timeout 0 ! 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 webvpn
 enable outside
```

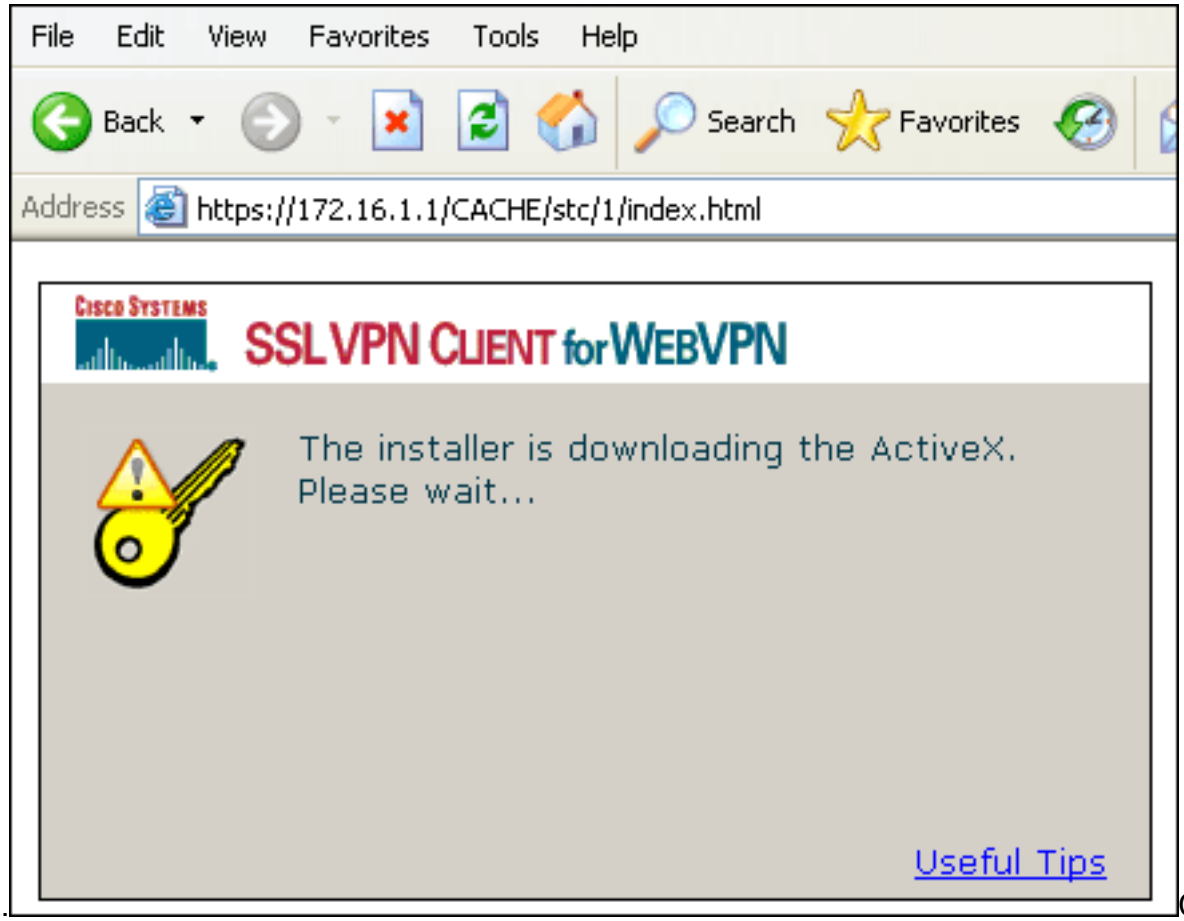
```
!--- Enable WebVPN on the outside interface. svc image disk0:/sslclient-win-1.1.4.179.pkg 1

!--- Assign an order to the SVC image. svc enable

!--- Enable the security appliance to download SVC images to remote computers. tunnel-
group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page. prompt hostname
context Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```



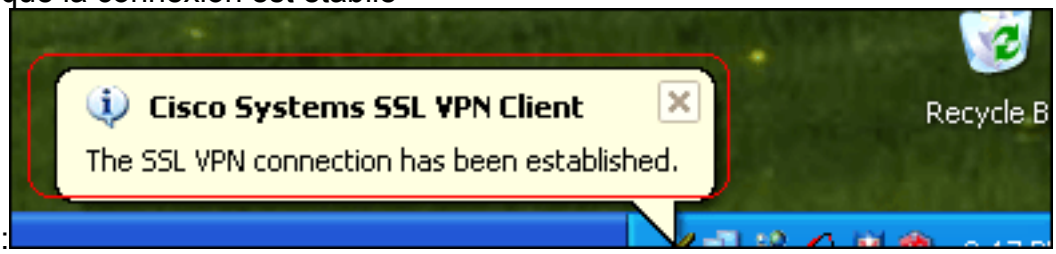

2. Entrez votre nom d'utilisateur et mot de passe, et puis choisissez votre groupe respectif de la liste déroulante de



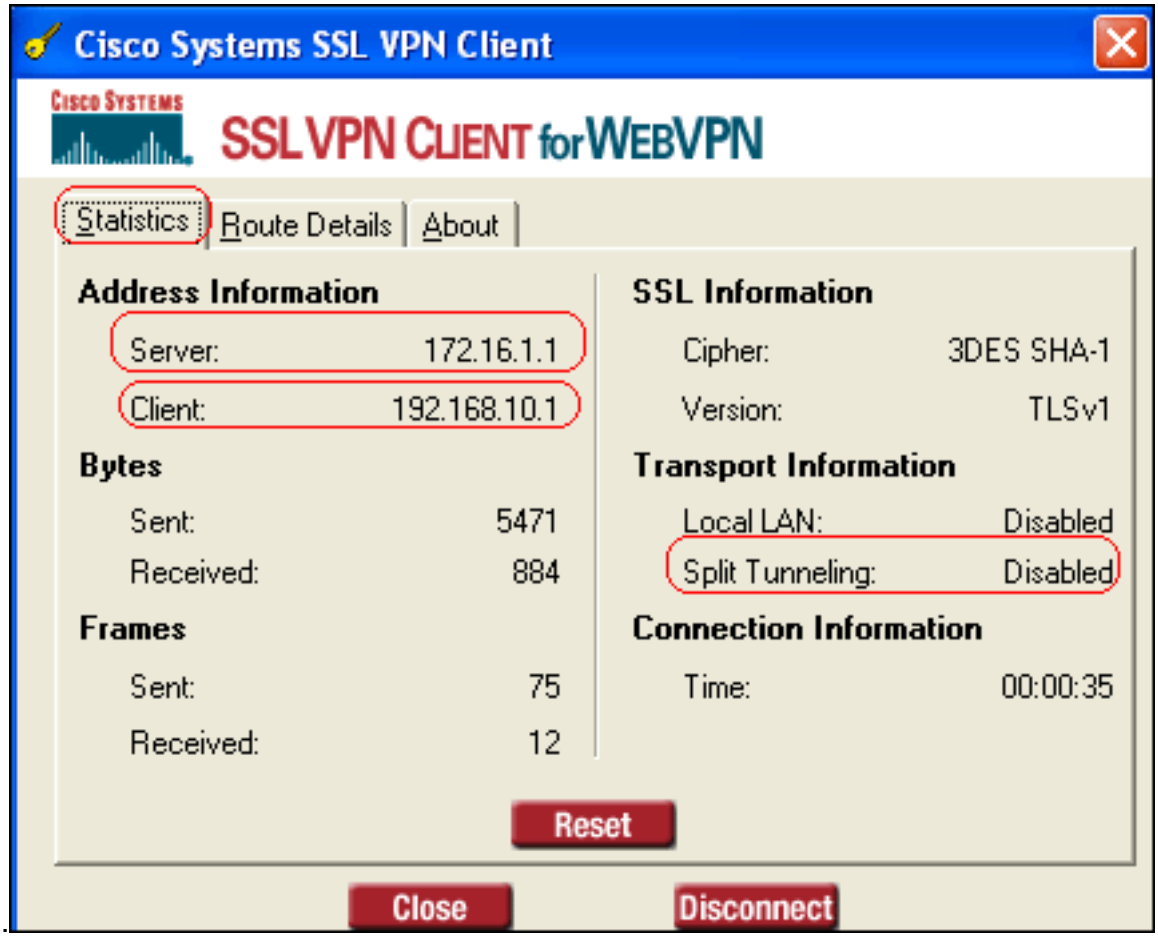

groupe. **Remarque:** Le logiciel d'ActiveX doit être installé dans votre ordinateur avant que vous téléchargiez le client de VPN

SSL. 

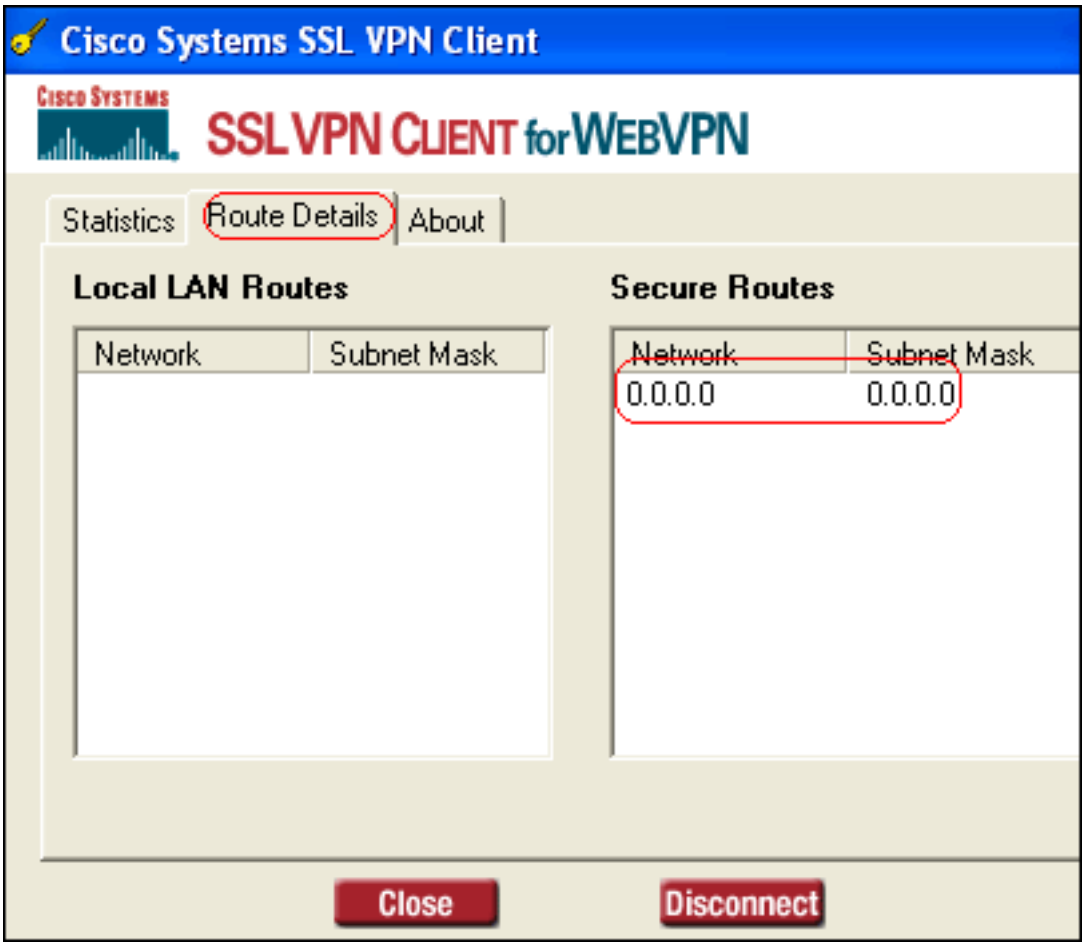
Cette boîte de dialogue apparaît pendant que la connexion est établie : 

Ce message apparaît une fois que la connexion est établie : 


3. Une fois que la connexion est établie, double-cliquer l'icône principale jaune qui apparaît dans la barre des tâches de votre ordinateur.L'affiche des informations de boîte de dialogue de client de VPN SSL de Cisco Systems au sujet de la connexion


Cisco Systems SSL VPN Client
SSL VPN CLIENT for WEBVPN
Statistics
Route Details
About
Address Information
Server: 172.16.1.1
Client: 192.168.10.1
Bytes
Sent: 5471
Received: 884
Frames
Sent: 75
Received: 12
SSL Information
Cipher: 3DES SHA-1
Version: TLSv1
Transport Information
Local LAN: Disabled
Split Tunneling: Disabled
Connection Information
Time: 00:00:35
Reset
Close
Disconnect

SSL.


Cisco Systems SSL VPN Client
SSL VPN CLIENT for WEBVPN
Statistics
Route Details
About
Local LAN Routes
Network
Subnet Mask
Secure Routes
Network
Subnet Mask
0.0.0.0
0.0.0.0
Close
Disconnect


## Vérifiez

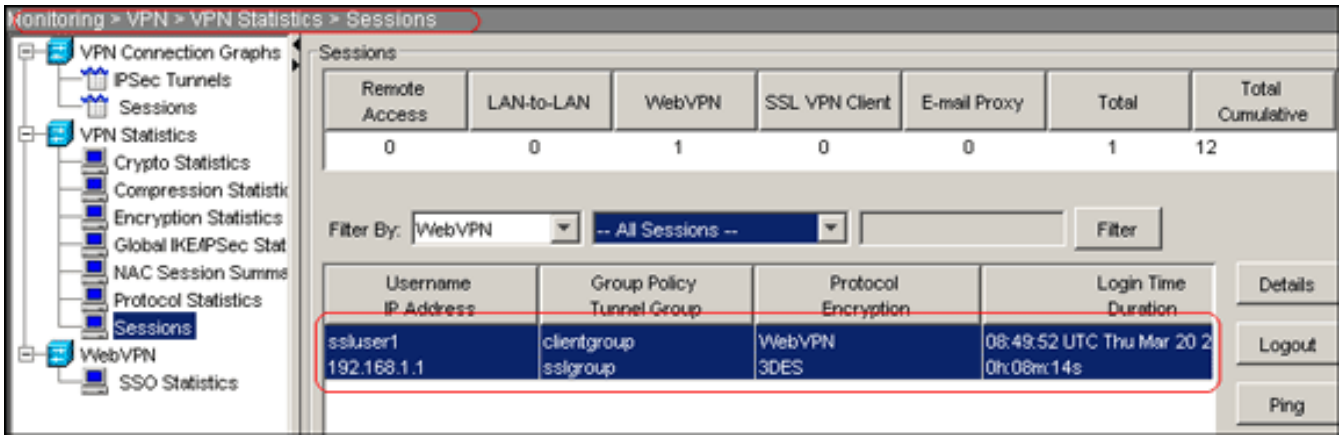
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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 de SVC enregistrées dans la mémoire flash de l'ASA.
```
ciscoasa#show webvpn svc
1. disk0:/sslclient-win-1.1.4.179.pkg 1
  CISCO STC win2k+ 1.0.0
  1,1,4,179
  Fri 01/18/2008 15:19:49.43

1 SSL VPN Client(s) installed
```
- **show vpn-sessiondb svc** — Affiche les informations sur les connexions SSL actuelles.
```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username     : ssluser1
Index        : 1
Assigned IP  : 192.168.10.1           Public IP    : 192.168.1.1
Protocol     : SVC                    Encryption   : 3DES
Hashing      : SHA1
Bytes Tx     : 131813                 Bytes Rx     : 5082
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver   : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
Tunnel Group : sslgroup
```

```
Login Time   : 12:38:47 UTC Mon Mar 17 2008
Duration     : 0h:00m:53s
Filter Name  :
```

- **show webvpn group-alias** — Affiche l'alias configuré pour différents groupes.`ciscoasa#`**`show webvpn group-alias`**
  `Tunnel Group: `**`sslgroup`**`  Group Alias: `**`sslgroup_users enabled`**
- Dans l'ASDM, choisissez le **Monitoring > VPN > VPN Statistics > Sessions** afin de visualiser des informations sur les sessions en cours de webvpn dans l'ASA.




# Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- **<username de nom de déconnexion de VPN-sessiondb >** — Te permet pour fermer une session la session de VPN SSL pour le nom d'utilisateur spécifié.`ciscoasa#`**`vpn-sessiondb logoff name ssluser1`**

  **`Called vpn_remove_uauIth: success!`**
  **`webvpn_svc_np_tear_down: no ACL`**
  **`NFO: Number of sessions with name "ssluser1" logged off : 1`**

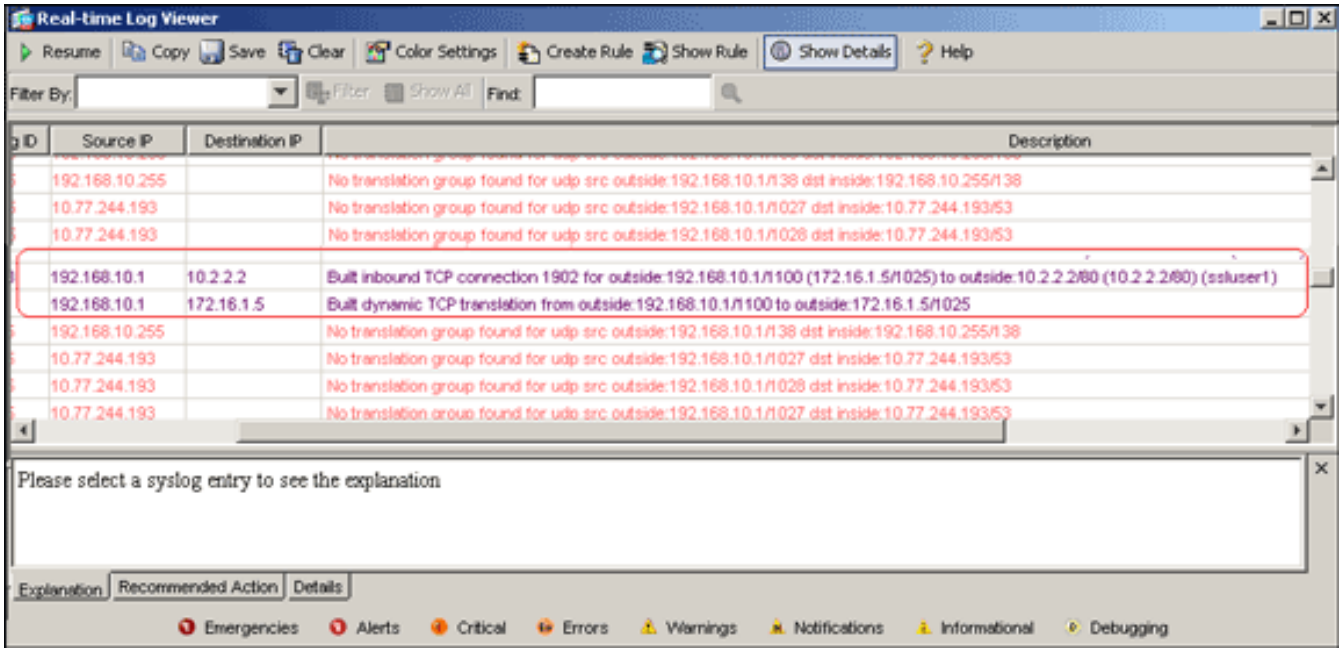
  De même, vous pouvez employer le **svc de déconnexion de VPN-sessiondb de** commande afin de terminer toutes les sessions de SVC.**Remarque:** Si le PC passe en mode veille ou veille prolongée, alors la connexion VPN SSL peut être terminée.

  **`webvpn_rx_data_cstp`**
  **`webvpn_rx_data_cstp: got message`**
  **`SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc)`**
  **`Called vpn_remove_uauth: success!`**
  **`webvpn_svc_np_tear_down: no ACL`**
  `ciscoasa#`**`show vpn-sessiondb svc`**
  `INFO: There are presently no active sessions`
- **Svc <1-255> de debug webvpn** — Fournit les événements en temps réel de webvpn afin d'établir la session.`Ciscoasa#`**`debug webvpn svc 7`**

```
ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179'
```

```
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED
```

- Dans l'ASDM, choisissez le **Monitoring > logging > Real-time Log Viewer > View** afin de visualiser les événements en temps réel. Ces exemples affichent les informations de session entre le SVC 192.168.10.1 et le web server 10.2.2.2 en Internet par l'intermédiaire d'ASA 172.16.1.5.



# Informations connexes

- Page de support pour appliances de sécurité adaptables de la gamme Cisco 5500
- PIX/ASA 7.x et client VPN pour le VPN d'Internet public sur un exemple de configuration de bâton
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- Support et documentation techniques - Cisco Systems