ASA 7.1/7.2 : Exemple de configuration d'autorisation de la transmission tunnel partagée pour SVC sur le dispositif ASA

Contenu

Introduction

Ce document fournit des instructions pas à pas sur la façon dont permettre à des clients vpn de Protocole SSL (Secure Socket Layer) (SVC) l'accès à Internet tandis qu'ils sont percés un tunnel dans une appliance de sécurité adaptable Cisco (ASA). Cette configuration permet l'accès sécurisé de SVC aux ressources de l'entreprise par le SSL et donne l'accès à Internet sans garantie avec l'utilisation de la Segmentation de tunnel.

La possibilité de transmettre du trafic sécurisé comme du trafic non sécurité sur la même interface est connue sous le nom de transmission tunnel partagée. La Segmentation de tunnel exige que vous spécifiez exactement que le trafic est sécurisé et ce qui est la destination de ce trafic, de sorte que seulement le trafic indiqué entre dans le tunnel, alors que le repos est décrypté transmis à travers le réseau public (Internet).

Conditions préalables

Conditions requises

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

- Privilèges d'administrateur locaux sur tous les postes de travail distants
- Commandes Javas et ActiveX sur le poste de travail distant
- Le port 443(SSL) n'est pas bloqué n'importe où le long du chemin de connexion

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**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 de l'ASA, qui doit être téléchargée 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 de pour en savoir plus de guide de configuration ASA.
- PC qui exécute le professionnel SP4 de Windows 2000 ou les Windows XP SP2
- 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.

Afin d'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 vous satisfaites la procédure de connexion et l'authentification, et les dispositifs de sécurité vous identifient en tant qu'exigence du SVC, les dispositifs de sécurité téléchargent le SVC à l'ordinateur distant. Si les dispositifs de sécurité vous identifient avec l'option d'utiliser le SVC, les dispositifs de sécurité téléchargent le SVC à l'ordinateur distant tandis qu'ils présentent un lien sur la fenêtre pour ignorer l'installation de SVC.

Après que vous téléchargement, le SVC installe et se configure, et puis les restes de SVC ou se désinstalle, qui dépend de la configuration, à partir de l'ordinateur distant quand la connexion se termine.

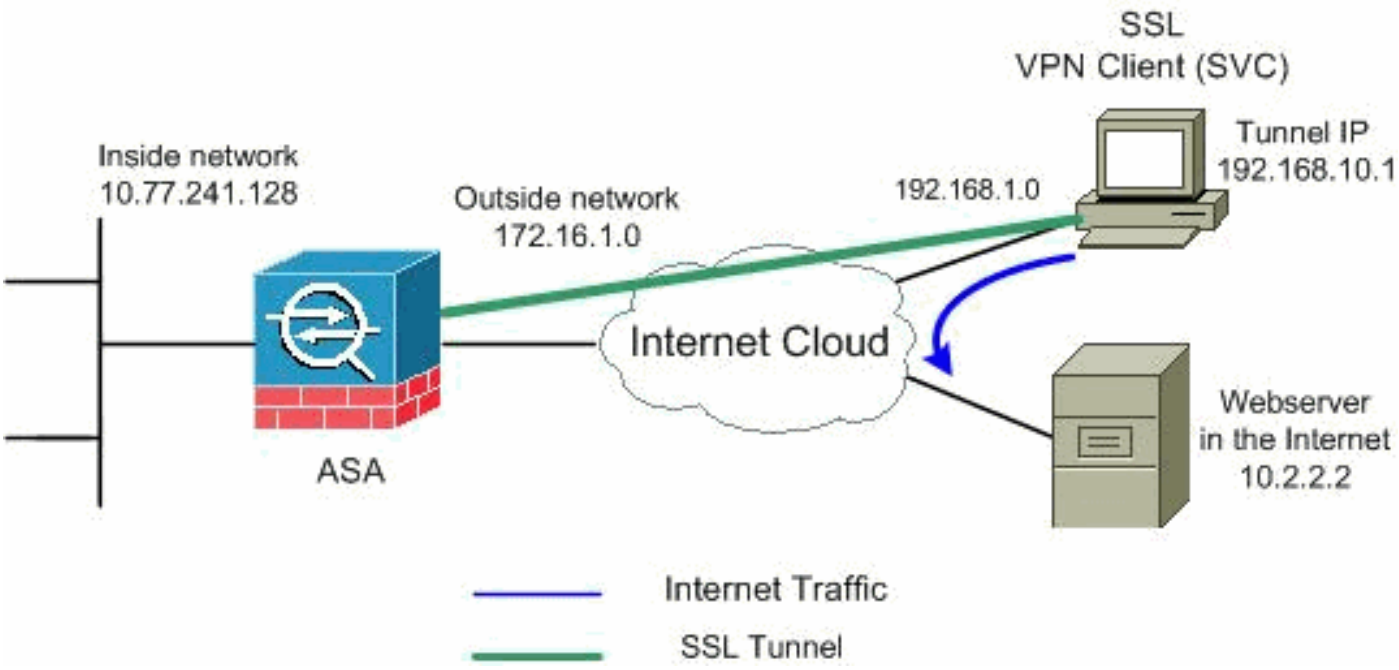
Configurez

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

Remarque: Utilisez l'Outil de recherche de commande (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 :

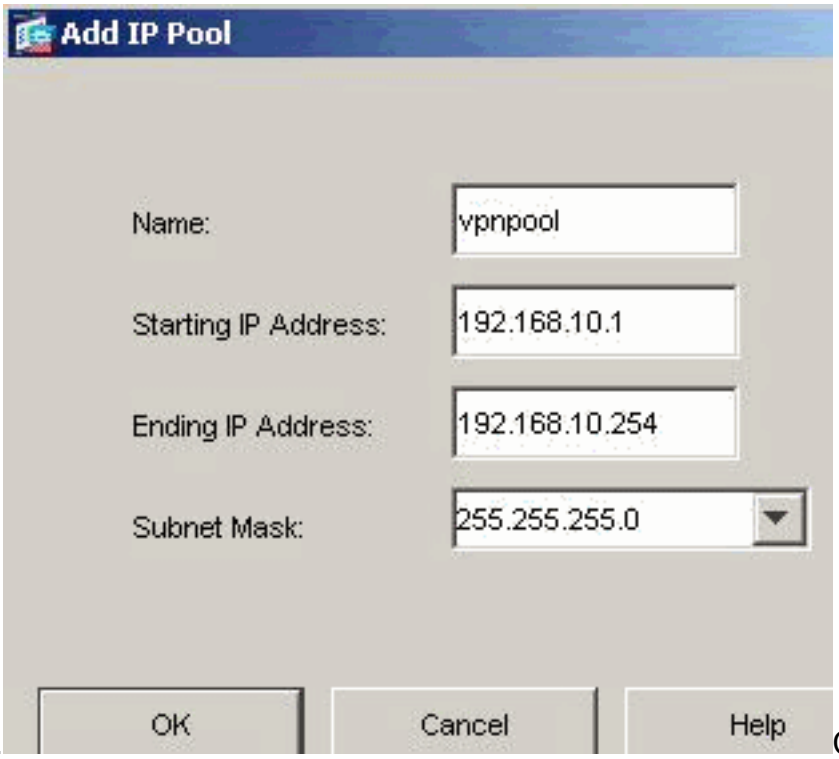


Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurations ASA utilisant l'ASDM 5.2(2)

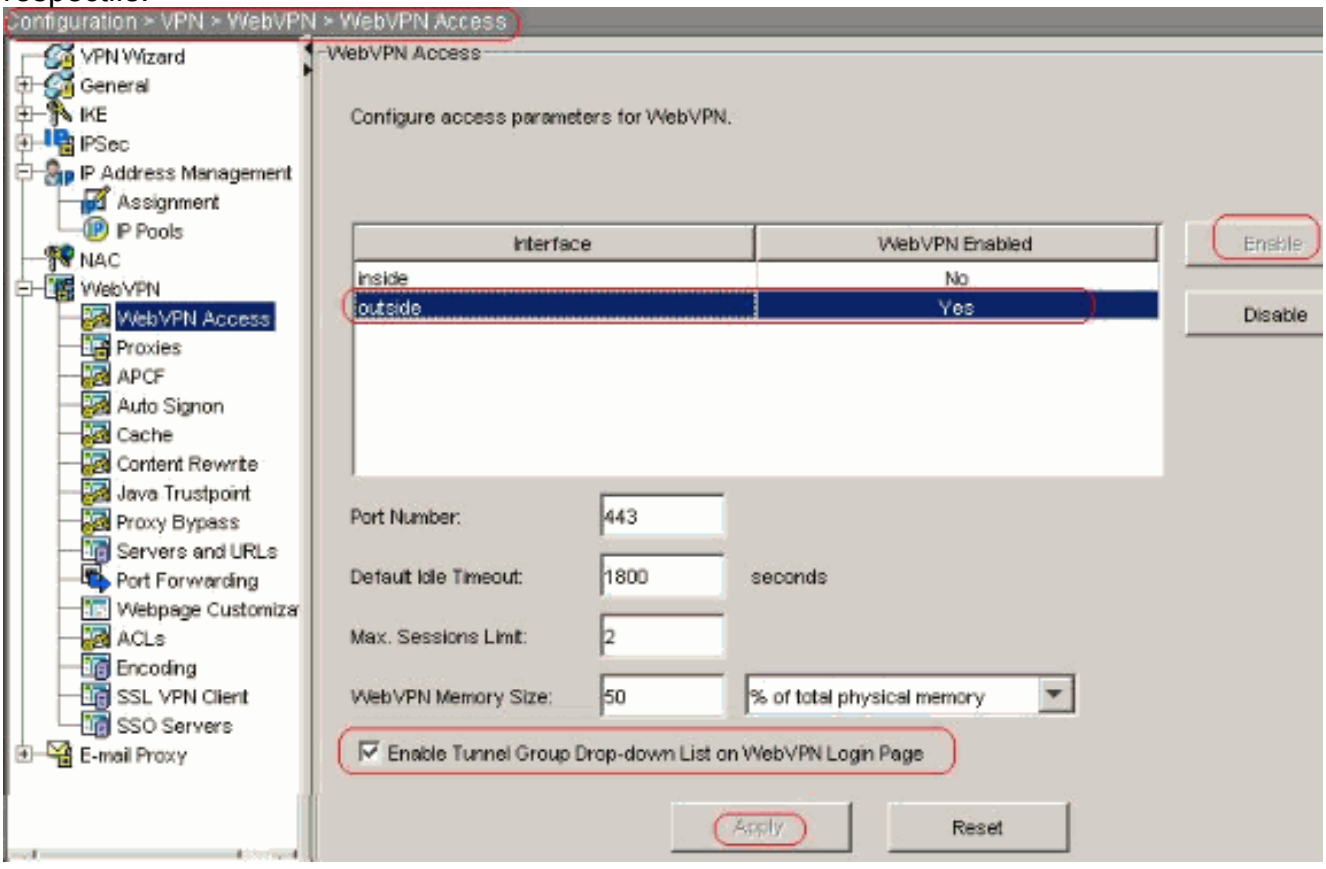
Terminez-vous ces étapes afin de configurer le VPN SSL sur l'ASA avec la Segmentation de tunnel comme affichée :

1. Le document suppose que la configuration de base telle que la configuration d'interface et ainsi de suite sont déjà faites et fonctionnent 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.
2. Choisissez la **configuration > le VPN > la gestion d'adresse IP > les groupes IP** afin de créer un groupe d'adresse IP : **vpnpool** pour des clients

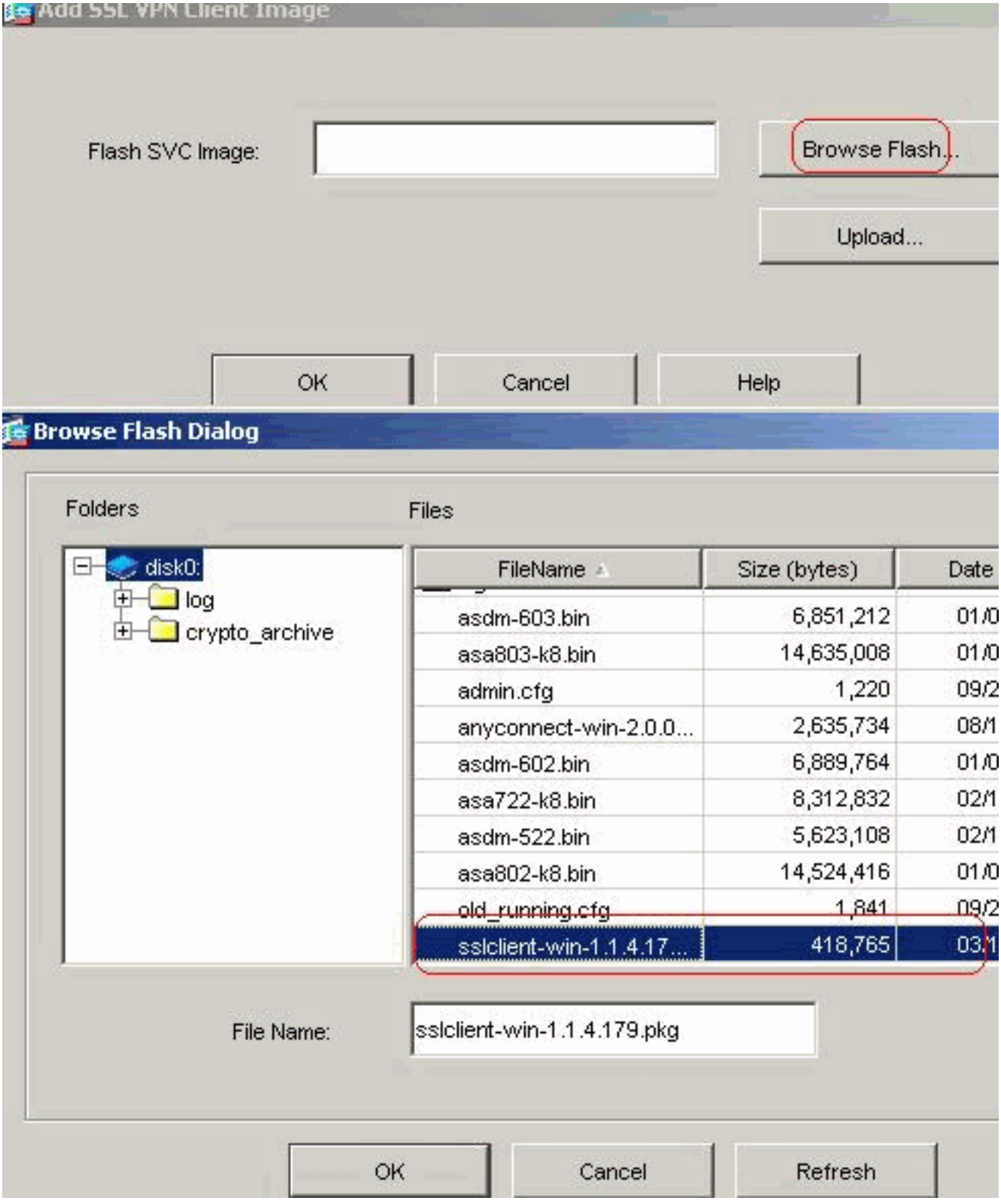


vpn. Cliquez sur **Apply**.

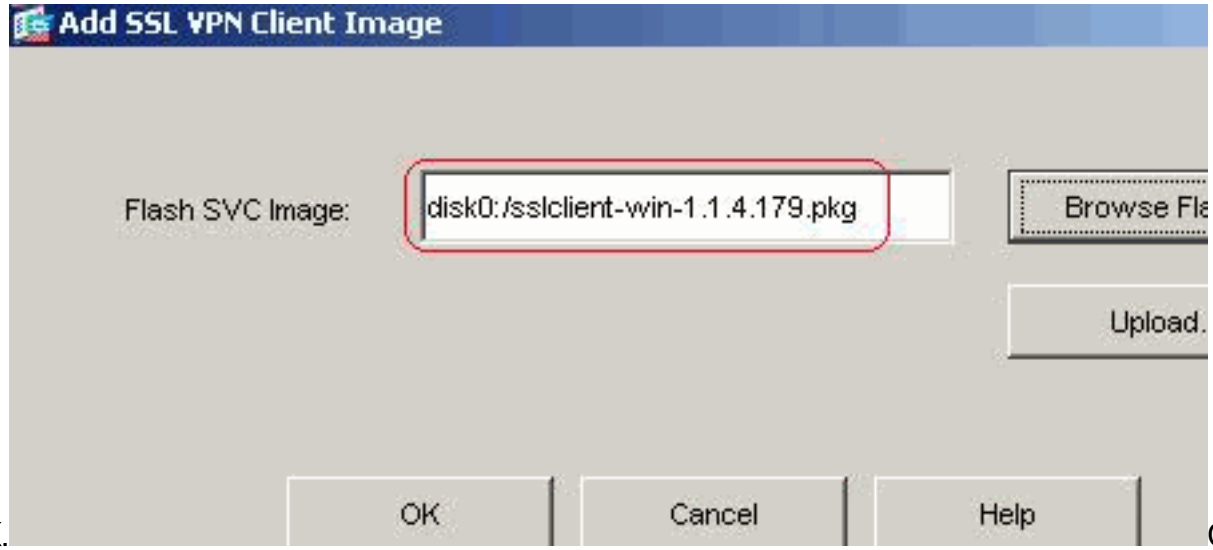
3. **Webvpn d'enable**Choisissez la **configuration > le VPN > le webvpn > le webvpn Access** et mettez en valeur l'interface extérieure avec la souris et cliquez sur l'**enable**. **La liste déroulante de groupe de tunnel d'enable de** contrôle **sur la** case de **page de connexion de webvpn** afin d'activer la baisse semblent vers le bas dans la page de connexion pour des utilisateurs, choisir leurs groupes respectifs.



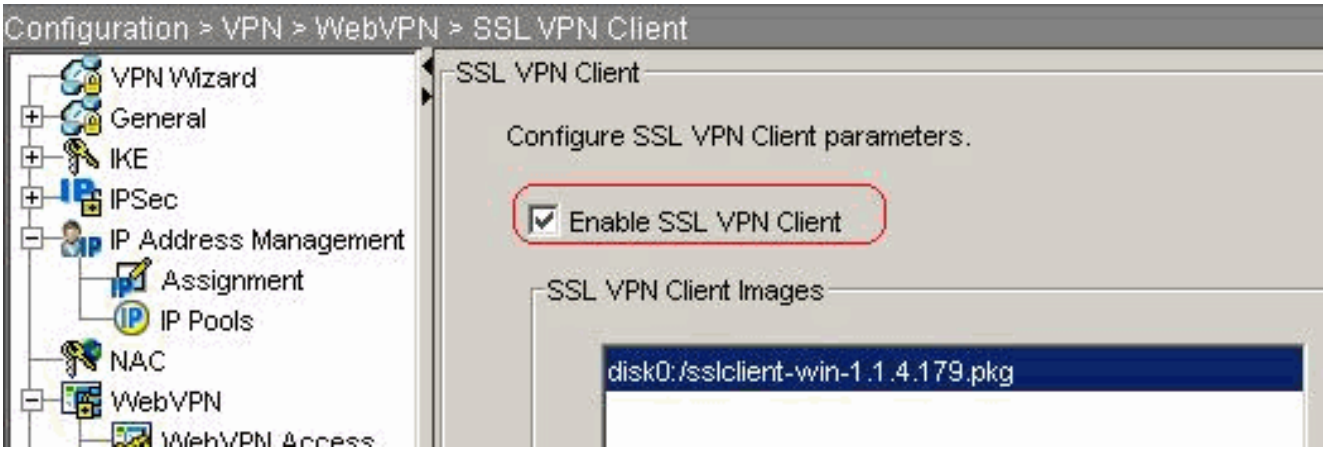
Cliquez sur **Apply**.Choisissez la **configuration > le VPN > le webvpn > le client de VPN SSL > ajoutent** afin d'ajouter l'image de client de VPN SSL de la mémoire flash de l'ASA comme affichée.


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
01/0
asa803-k8.bin
14,635,008
01/0
admin.cfg
1,220
09/2
anyconnect-win-2.0.0...
2,635,734
08/1
asdm-602.bin
6,889,764
01/0
asa722-k8.bin
8,312,832
02/1
asdm-522.bin
5,623,108
02/1
asa802-k8.bin
14,524,416
01/0
old_running.cfg
1,841
09/2
sslclient-win-1.1.4.17...
418,765
03/1
File Name:
sslclient-win-1.1.4.179.pkg
OK
Cancel
Refresh

Cliquez sur

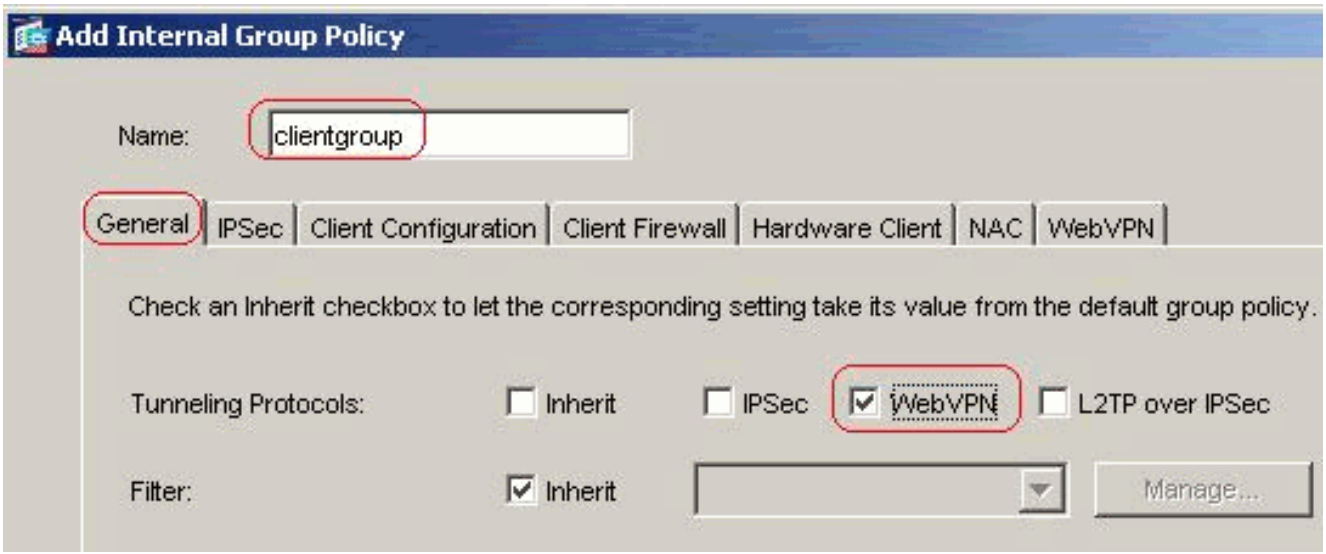


OK.Cliquez sur **OK**.Case de **client de VPN SSL de** clic.



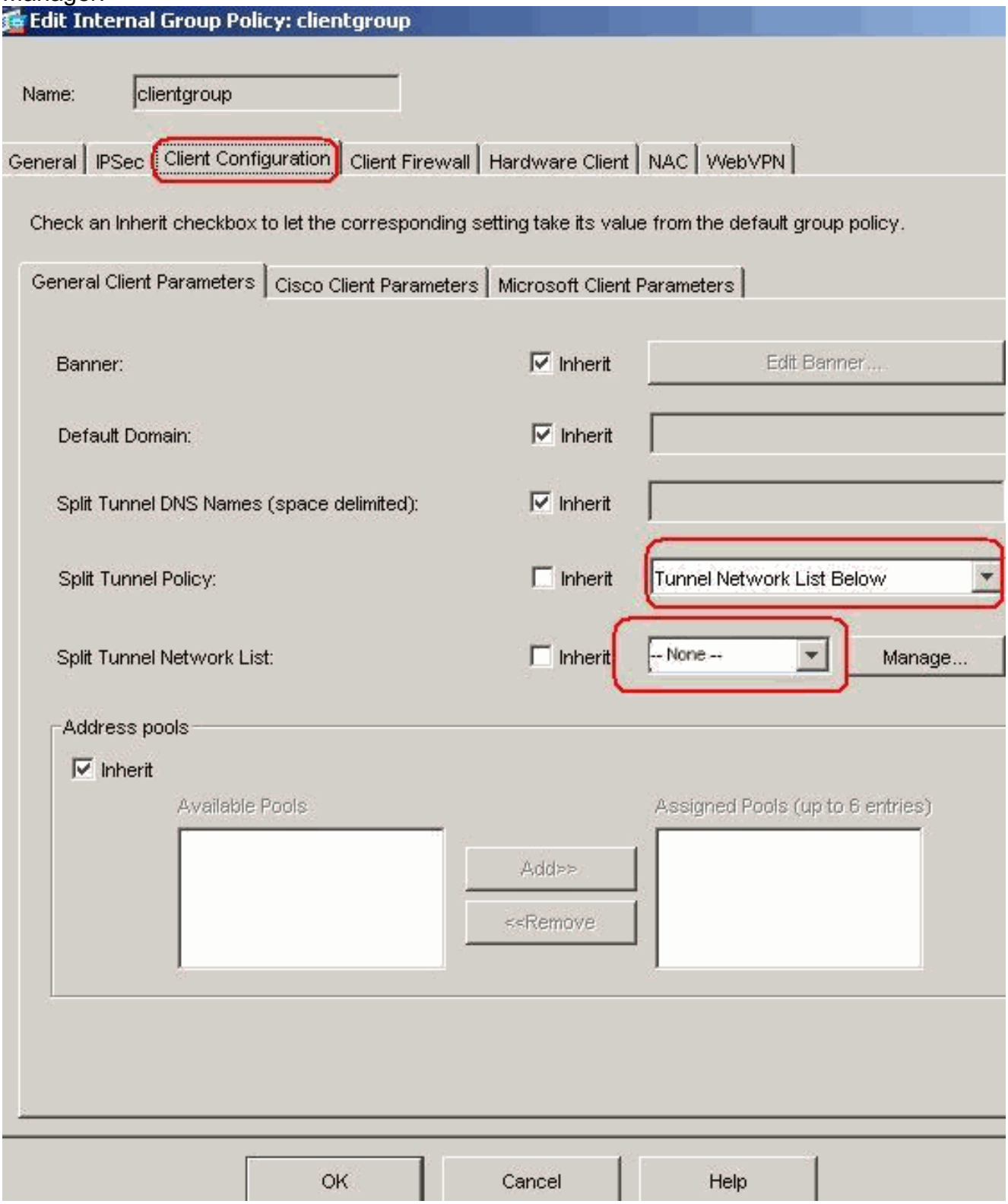
Cliquez sur **Apply**.**Configuration CLI équivalente :**

4. **Configurez la stratégie de groupe**Choisissez le **Configuration > VPN > General > Group Policy > ajoutent (stratégie de groupe interne)** afin de créer un **clientgroup** interne de stratégie de groupe. Sous le **général**, choisissez la case de **webvpn** afin d'activer le webvpn comme protocole de Tunnellisation.

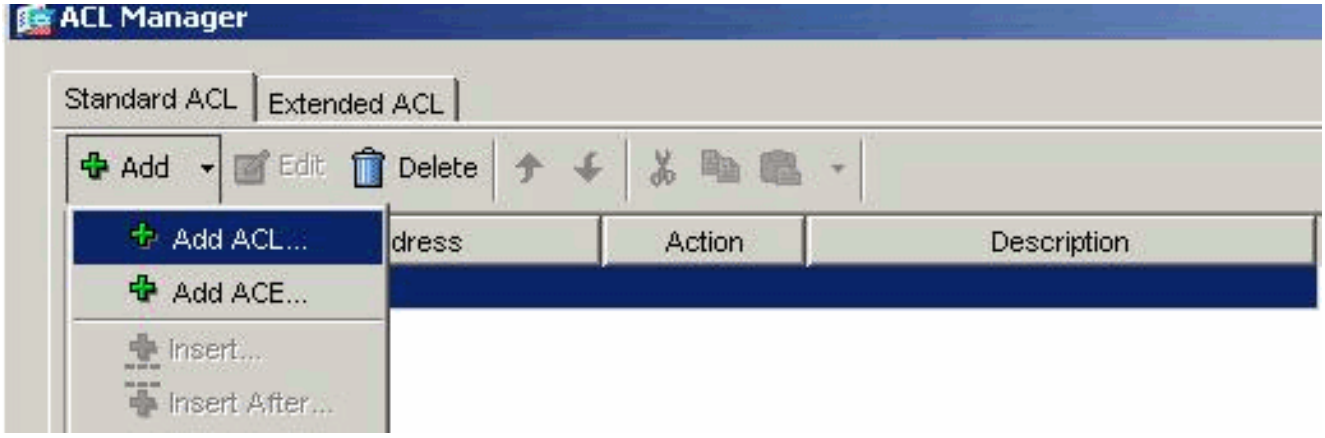


Dans l'onglet de **configuration > de Général Client Parameters de client**, décochez la case d'**héritage** pour la stratégie de tunnel partagé et choisissez la **liste des réseaux de tunnel ci-dessous de la** liste déroulante.Désactivez la case **Inherit** pour la liste Split Tunnel Network

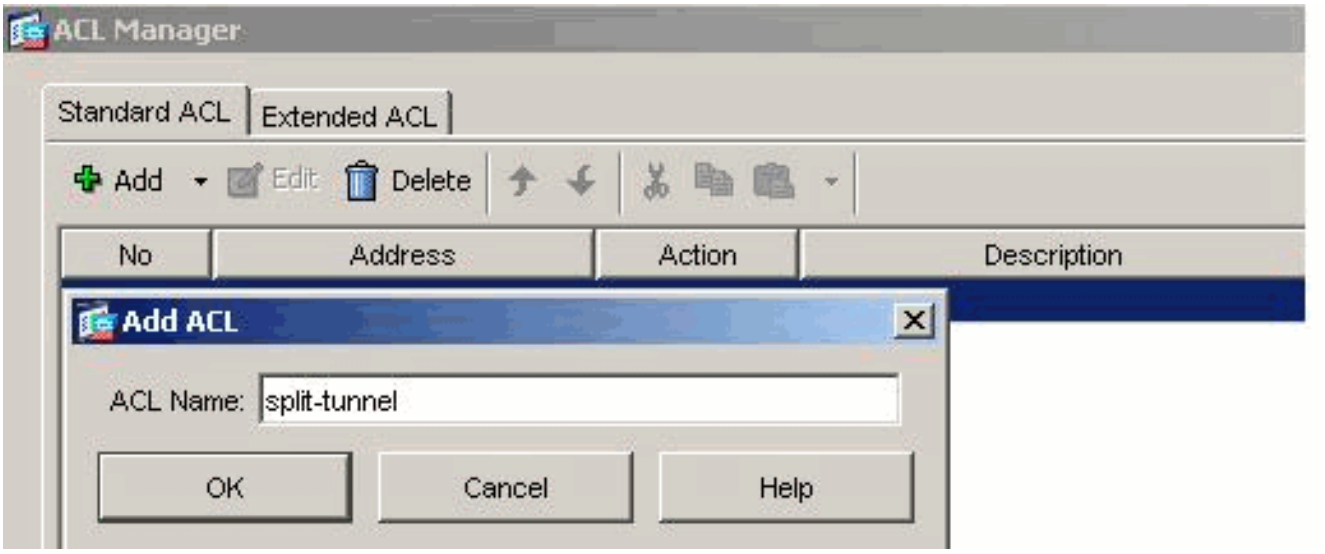
List, puis cliquez sur **Manage** pour lancer l'ACL
Manager.



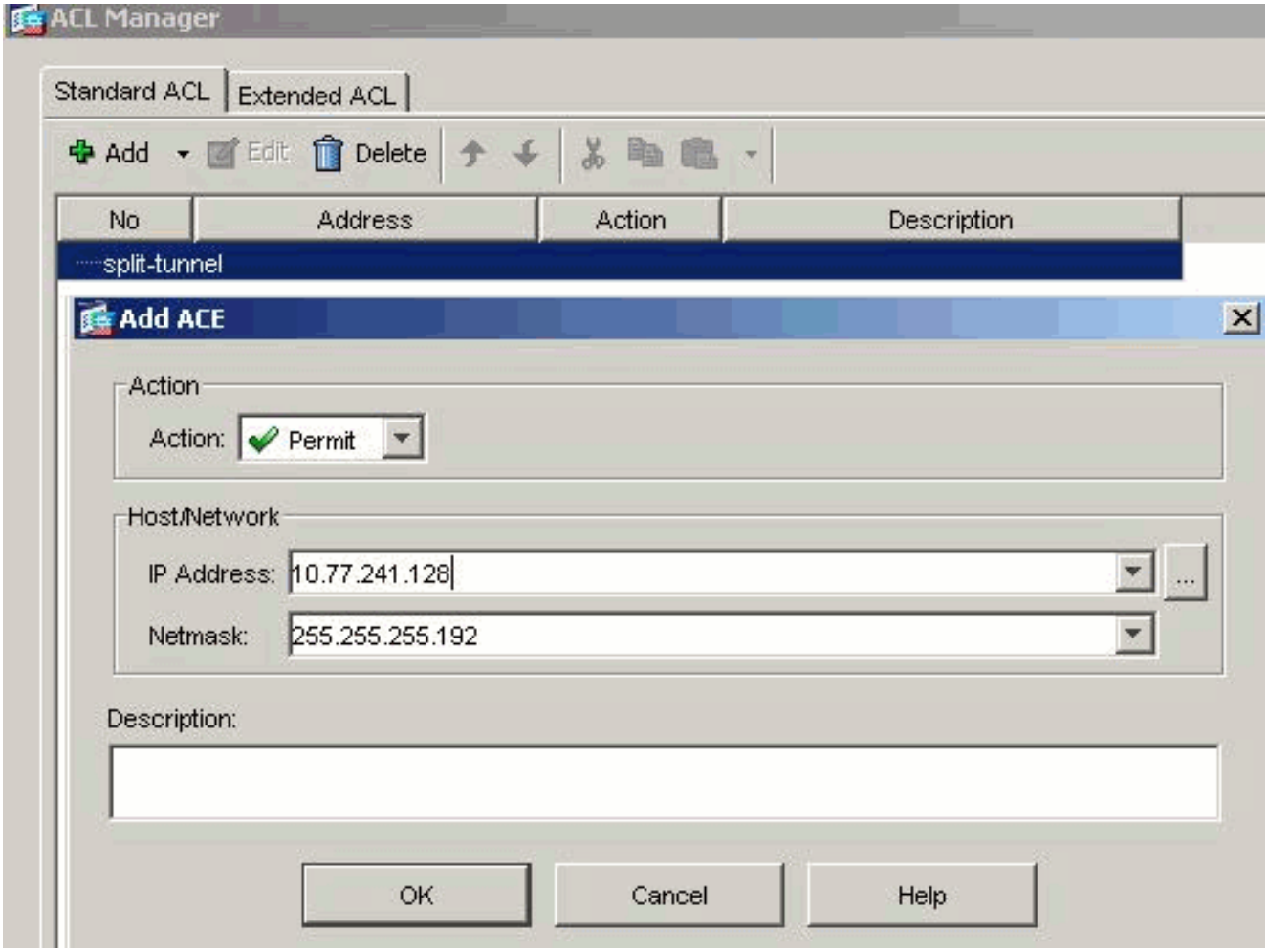
Chez le gestionnaire d'ACL, choisissez **ajoutent > ajoutent l'ACL…** afin de créer une nouvelle liste
d'accès.



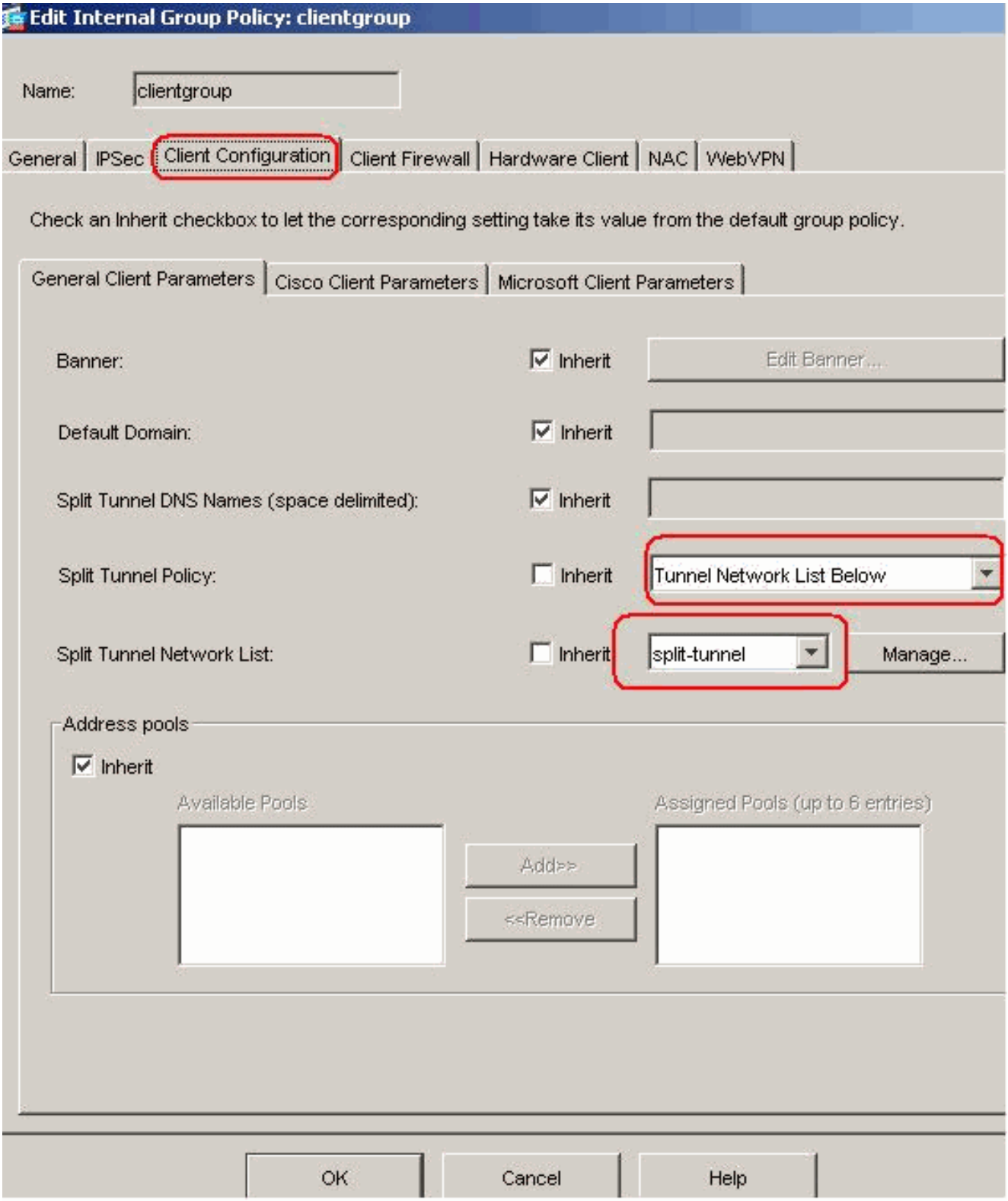
Fournissez un nom pour l'ACL et cliquez sur **OK**.



Une fois le nom de l'ACL créé, choisissez **Add > Add ACE** afin d'ajouter une entrée de contrôle d'accès (ACE).Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est 10.77.241.128/26 et choisit l'**autorisation**.Cliquez sur **OK** afin de quitter l'ACL Manager.

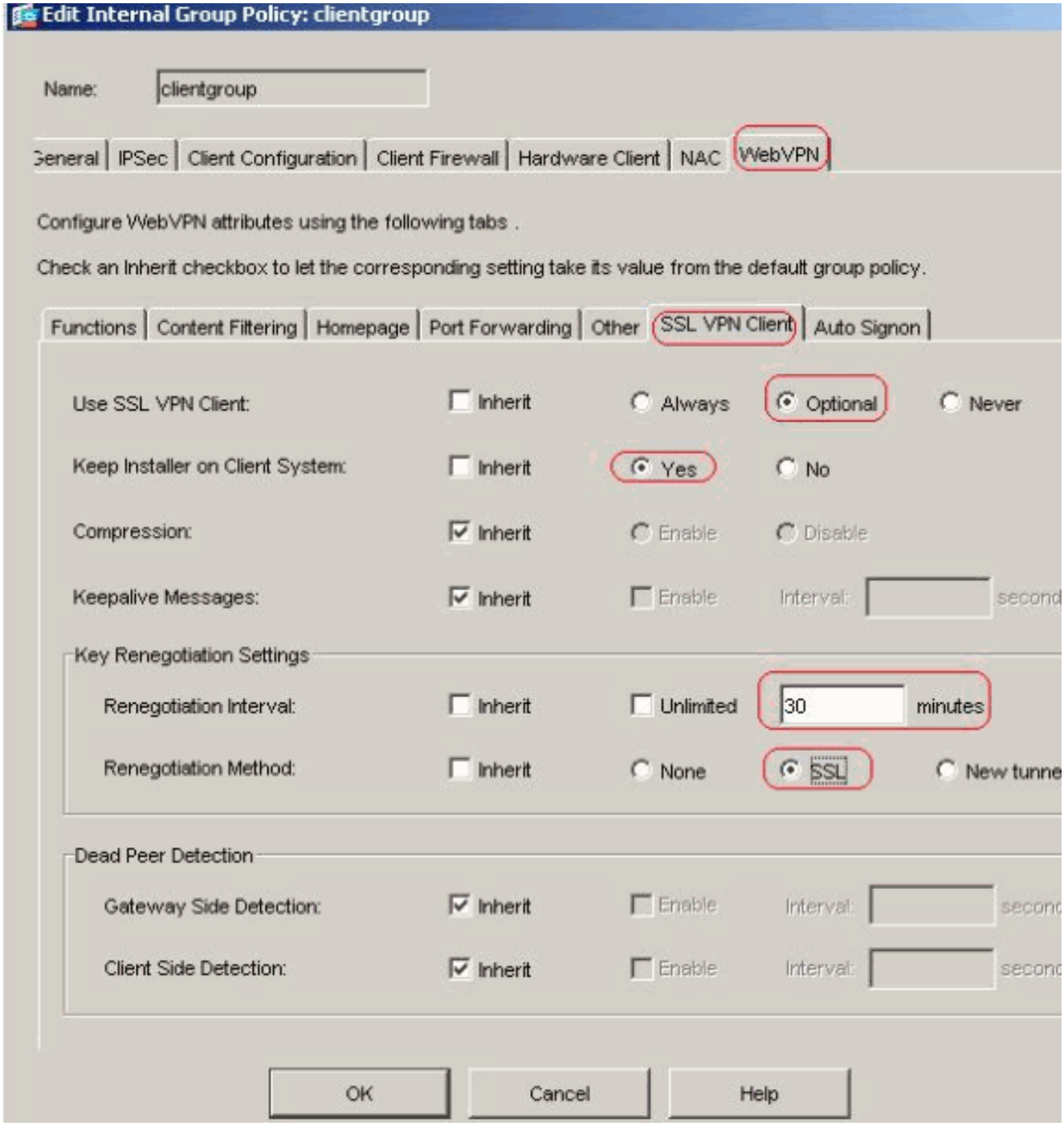


Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste Split Tunnel Network List.Cliquez sur **OK** afin de retourner à la configuration de la stratégie de groupe.

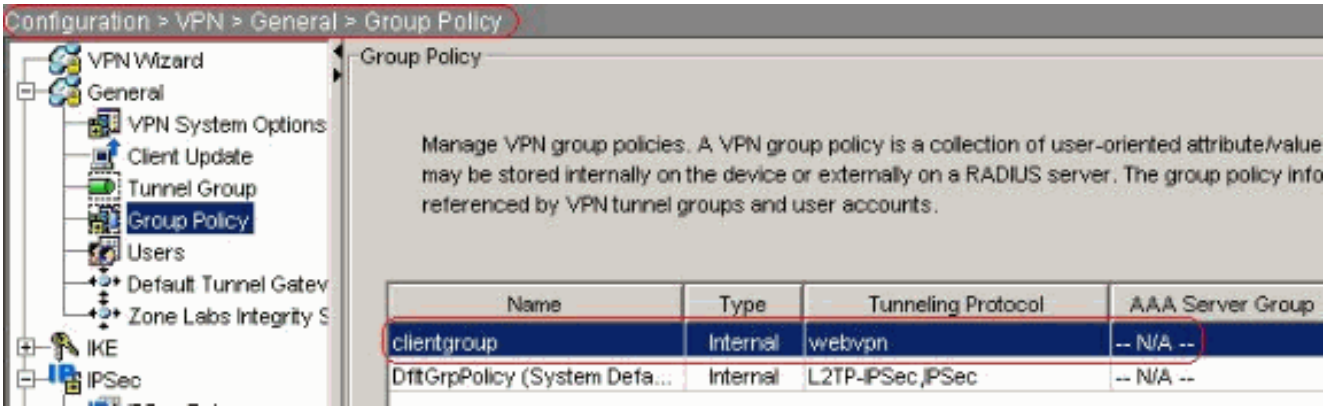


Dans la page principale, cliquez sur Apply et puis **envoyez** (s'il y a lieu) afin d'envoyer les commandes à l'ASA.Pour l'option Client de VPN SSL d'utilisation, décochez la case d'**héritage** et cliquez sur la case d'option **facultative**.Ce choix permet au client distant pour choisir si cliquer sur l'onglet de **webvpn > de client SSLVPN**, et choisir ces options :Ne téléchargez pas 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 Keep Installer on Client System, désélectionnez la case à cocher **Inherit**, puis cliquez sur le bouton radio **Yes**.Cette action permet au logiciel SVC de demeurer sur l'ordinateur client. 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.La Sécurité est améliorée quand vous fixez les limites sur la durée qu'une clé est valide.Pour l'option Renegotiation Method, décochez la case à cocher **Inherit** et cliquez la case d'option **SSL**. La renégociation peut utiliser le tunnel SSL actuel ou un nouveau tunnel créé expressément pour la renégociation.Vos attributs client VPN SSL doivent être configurés tel qu´indiqué sur cette image
:

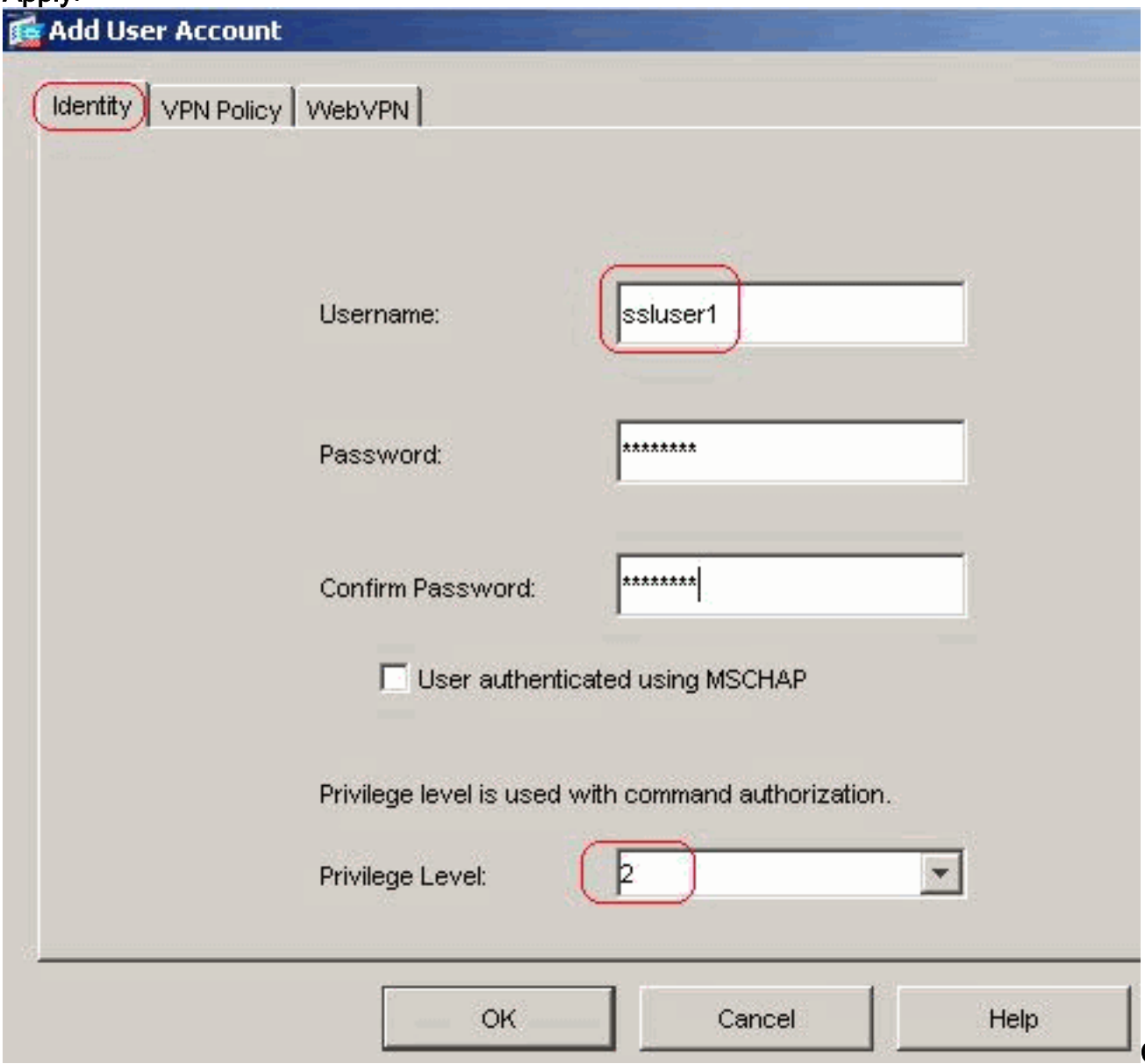


Cliquez sur **OK**, puis sur **Apply**.



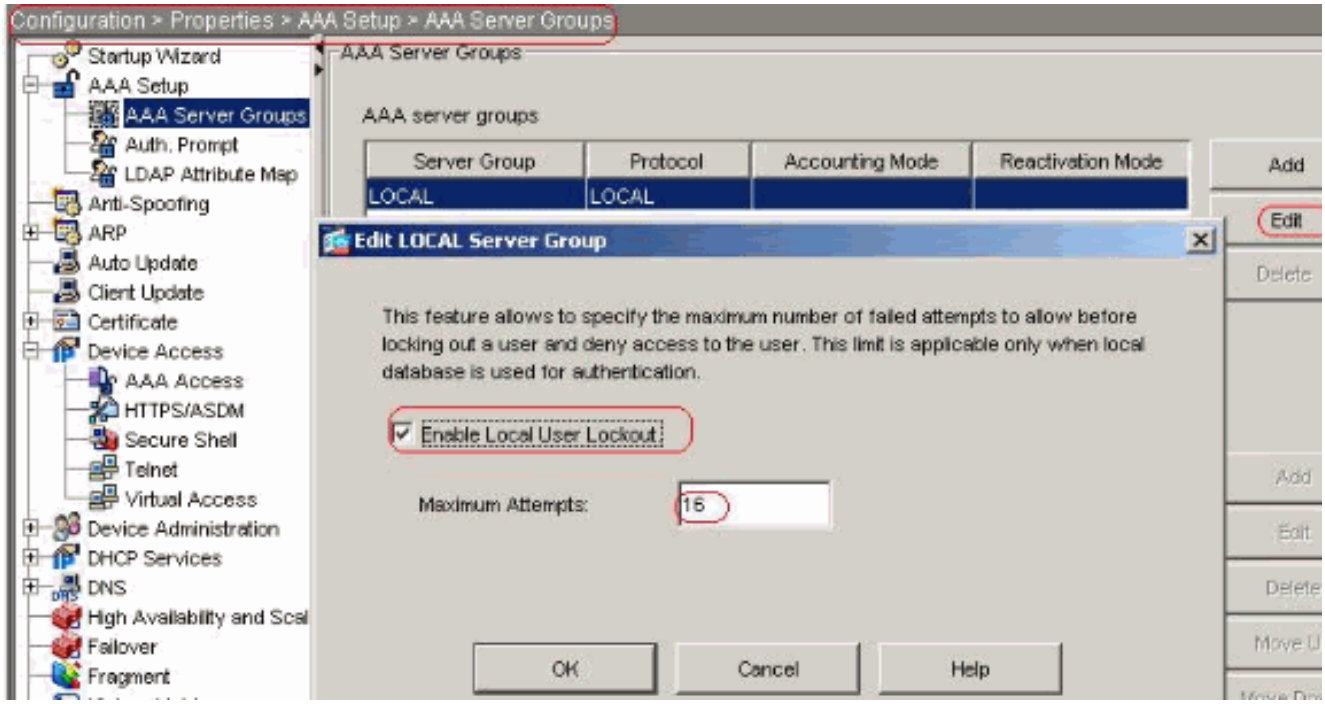
Configuration CLI équivalente :

5. Choisissez la **configuration > le VPN > le général > les utilisateurs > ajoutent** afin de créer un nouveau compte utilisateur **ssluser1**. Cliquez sur **OK**, puis sur **Apply**.



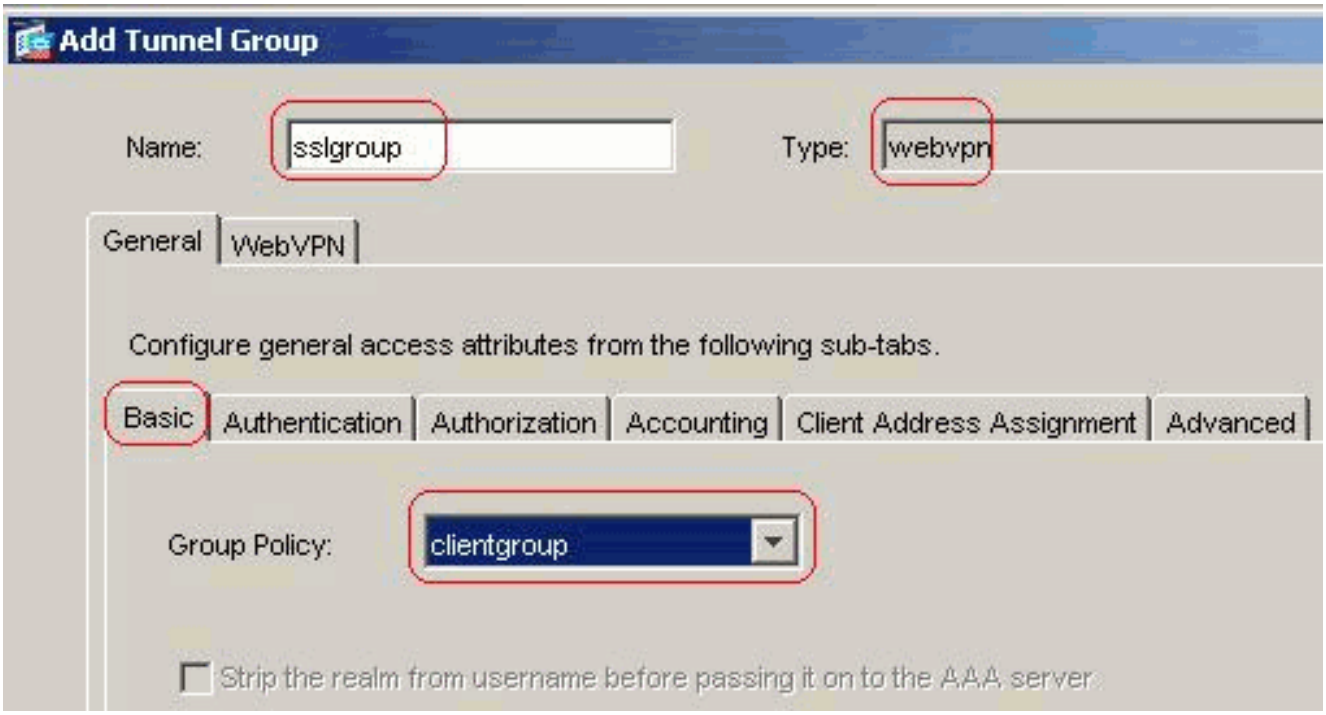
Configuration CLI équivalente :

6. Choisissez la **configuration > le Properties > l'AAA installé > des groupes de serveurs d'AAA > éditent** afin de modifier les **GENS DU PAYS de** groupe de serveurs par défaut et choisir la case de **verrouillage d'utilisateur local d'enable** avec le maximum tente la valeur en tant que **16**.

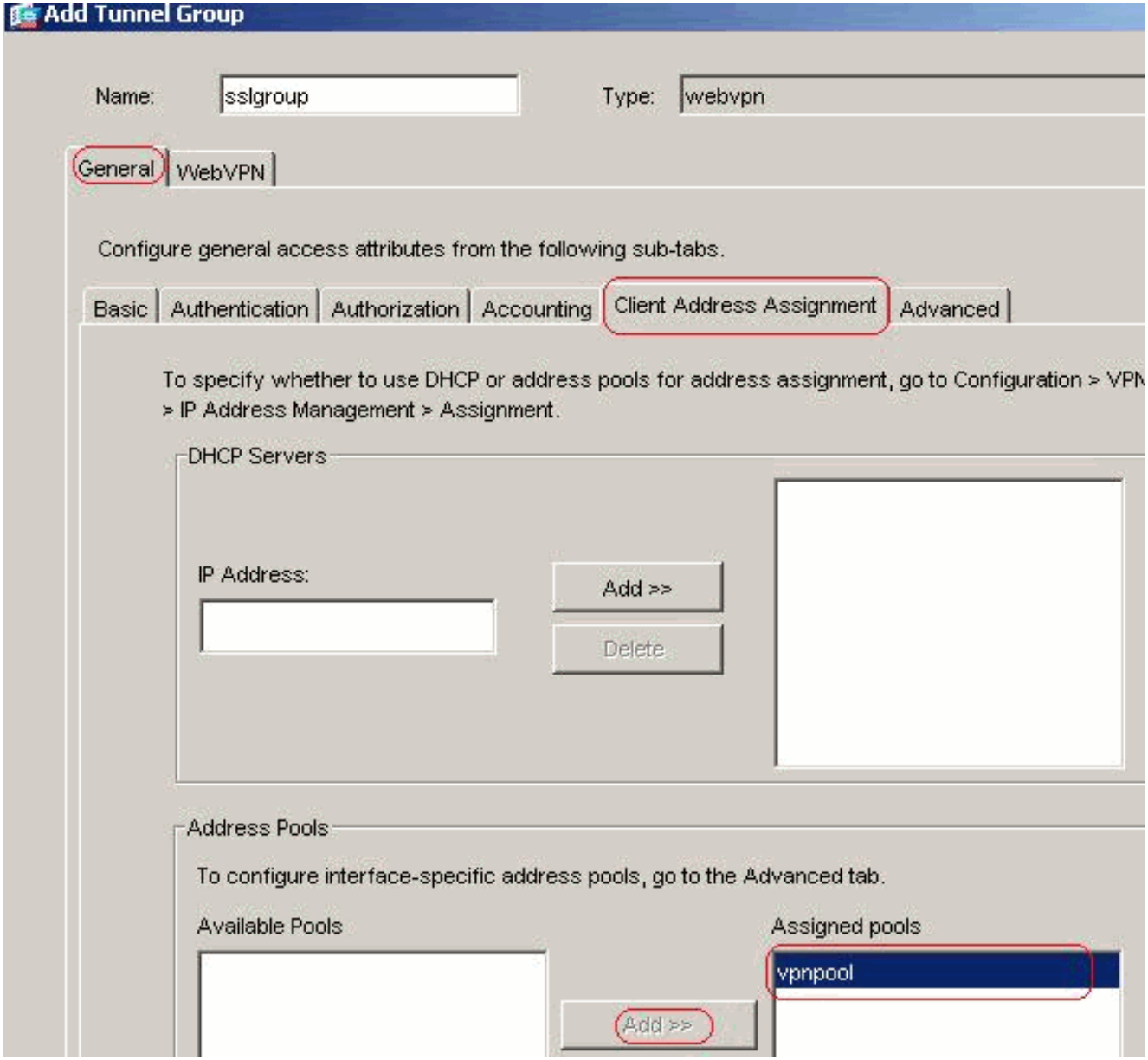


Configuration CLI équivalente :

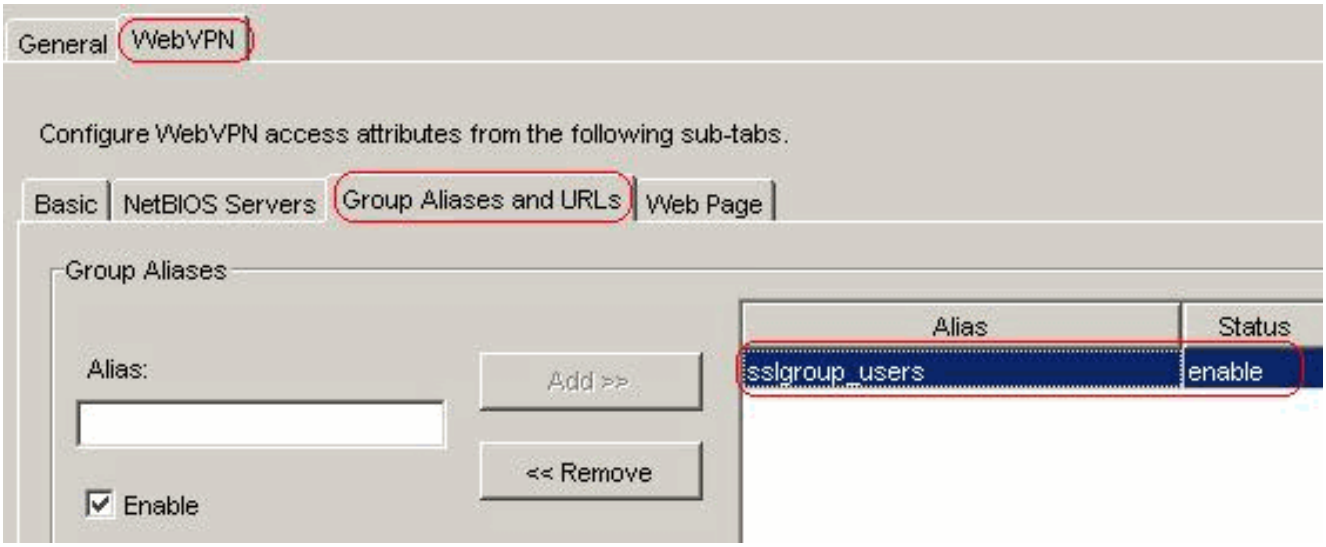
7. **Configurez le groupe de tunnel**Choisissez la **configuration > le VPN > le groupe de général > de tunnel > ajoutent (accès de webvpn)** afin de créer un nouveau **sslgroup de** groupe de tunnel.Dans l'onglet **général > de base**, choisissez la stratégie de groupe comme **clientgroup de la** liste déroulante.



En général **> l'onglet Client Address Assignment**, sous des pools d'adresses, cliquent sur Add **>>** afin d'assigner le **vpnpool** disponible de pool d'adresses.

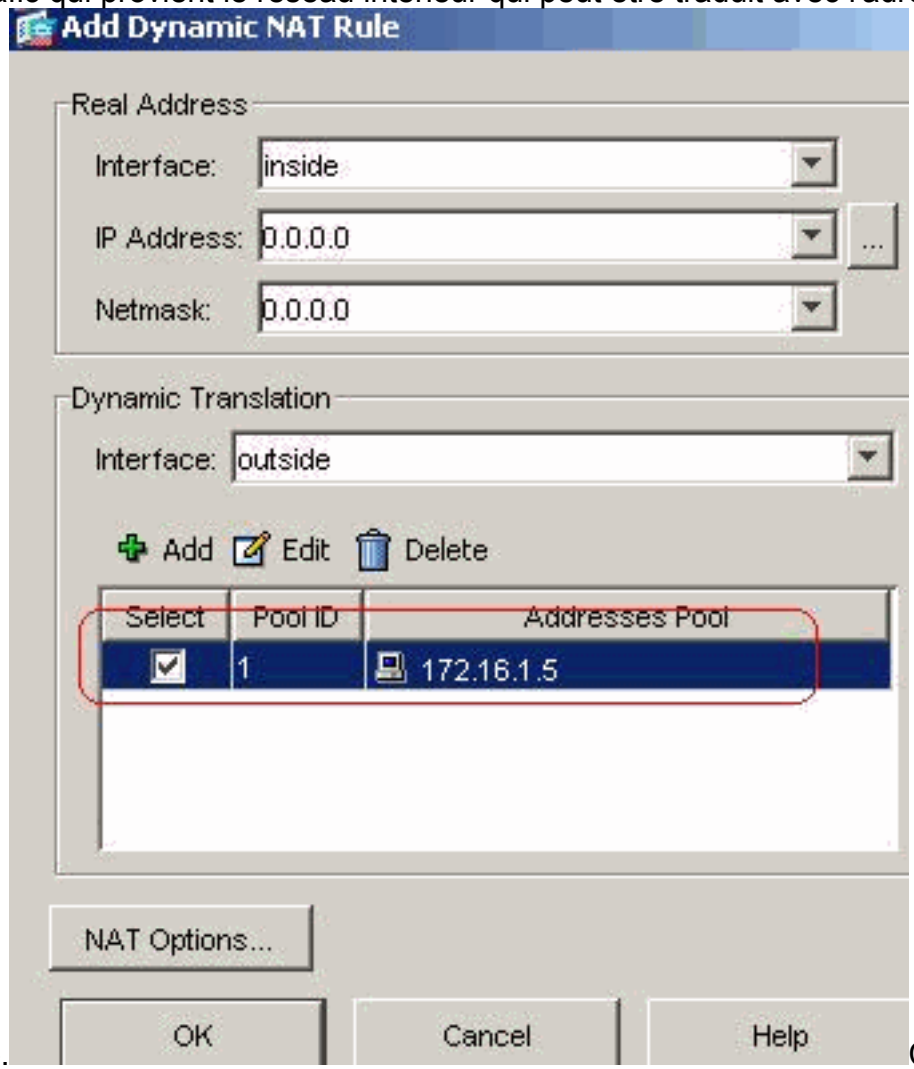


Dans l'onglet de **webvpn > de pseudonymes et URLs de groupe**, introduisez le pseudonyme dans la case de paramètre et cliquez sur Add **>>** afin de la faire apparaître dans la liste de noms de groupe dans la page de
connexion.



Cliquez sur **OK**, puis sur **Apply.Configuration CLI équivalente :**

8. [Configurer NAT](#)Choisissez le **Configuration > NAT > ajoutent > ajoutent la règle NAT**

dynamique pour le trafic qui provient le réseau intérieur qui peut être traduit avec l'adresse IP extérieure 172.16.1.5. 

Cliquez sur OK et cliquez sur Apply en page principale.**Configuration CLI équivalente :**

9. Configurez le nat exemption pour le retour-trafic de l'intérieur du réseau au client vpn.`ciscoasa(config)#`**`access-list nonat permit ip 10.77.241.0 192.168.10.0`** `ciscoasa(config)#`**`access-list nonat permit ip 192.168.10.0 10.77.241.0`** `ciscoasa(config)#`**`nat (inside) 0 access-list nonat`**

Configuration ASA 7.2(2) utilisant le CLI

Cisco ASA 7.2(2)
`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 access-list split-tunnel standard permit 10.77.241.128 255.255.255.192` *`!--- ACL for Split Tunnel network list for encryption.`* `access-list nonat permit ip 10.77.241.0 192.168.10.0 access-list nonat permit ip 192.168.10.0 10.77.241.0` *`!--- ACL to define the traffic to be exempted from NAT.`* `pager lines 24 mtu`

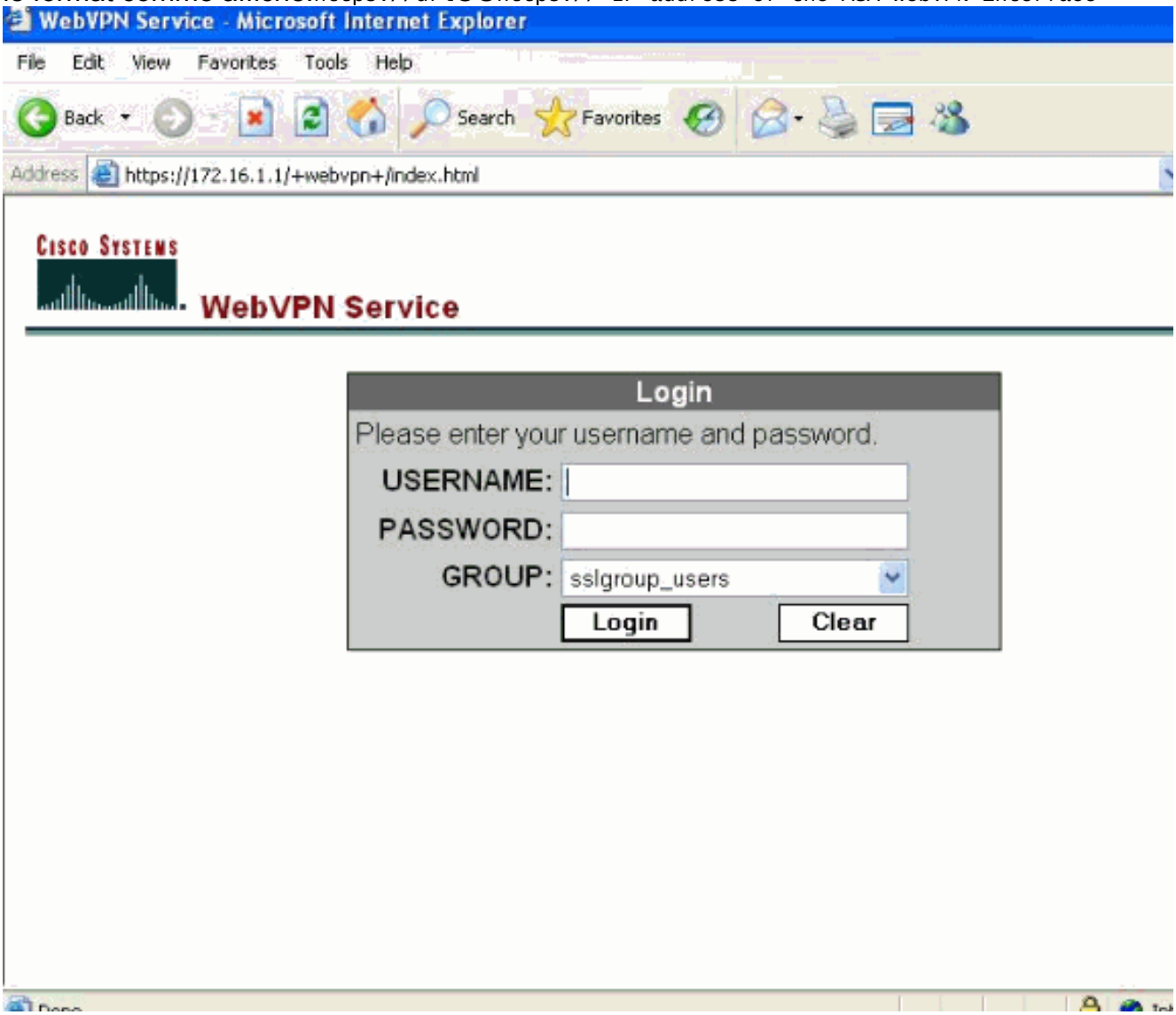
```
inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 !--- The address pool for
the SSL VPN Clients no failover icmp unreachable rate-
limit 1 burst-size 1 asdm image disk0:/asdm-522.bin no
asdm history enable arp timeout 14400 global (outside) 1
172.16.1.5 !--- The global 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) 0 access-list
nonat !--- The traffic permitted in "nonat" ACL is
exempted from NAT. nat (inside) 1 0.0.0.0 0.0.0.0
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
tunnelspecified split-tunnel-network-list value split-
tunnel !--- Encrypt the traffic specified in the split
tunnel ACL only. 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, !--- and increase 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#
```

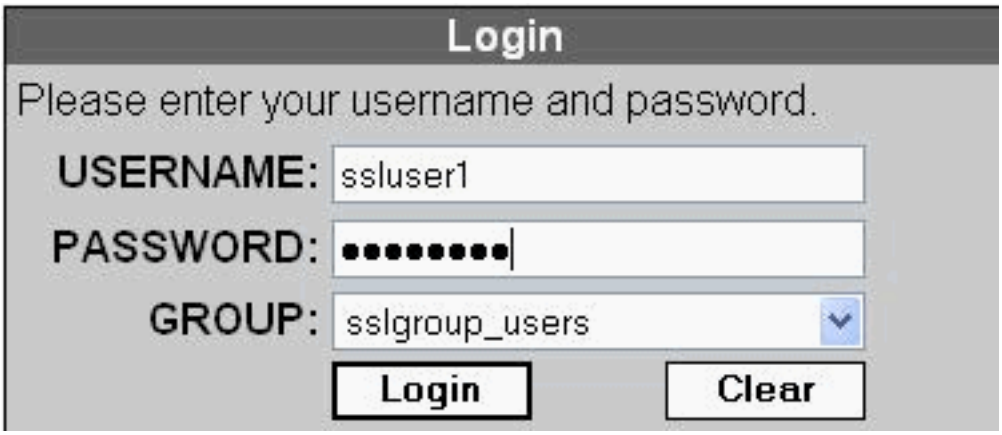
Établir la connexion VPN SSL avec SVC

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

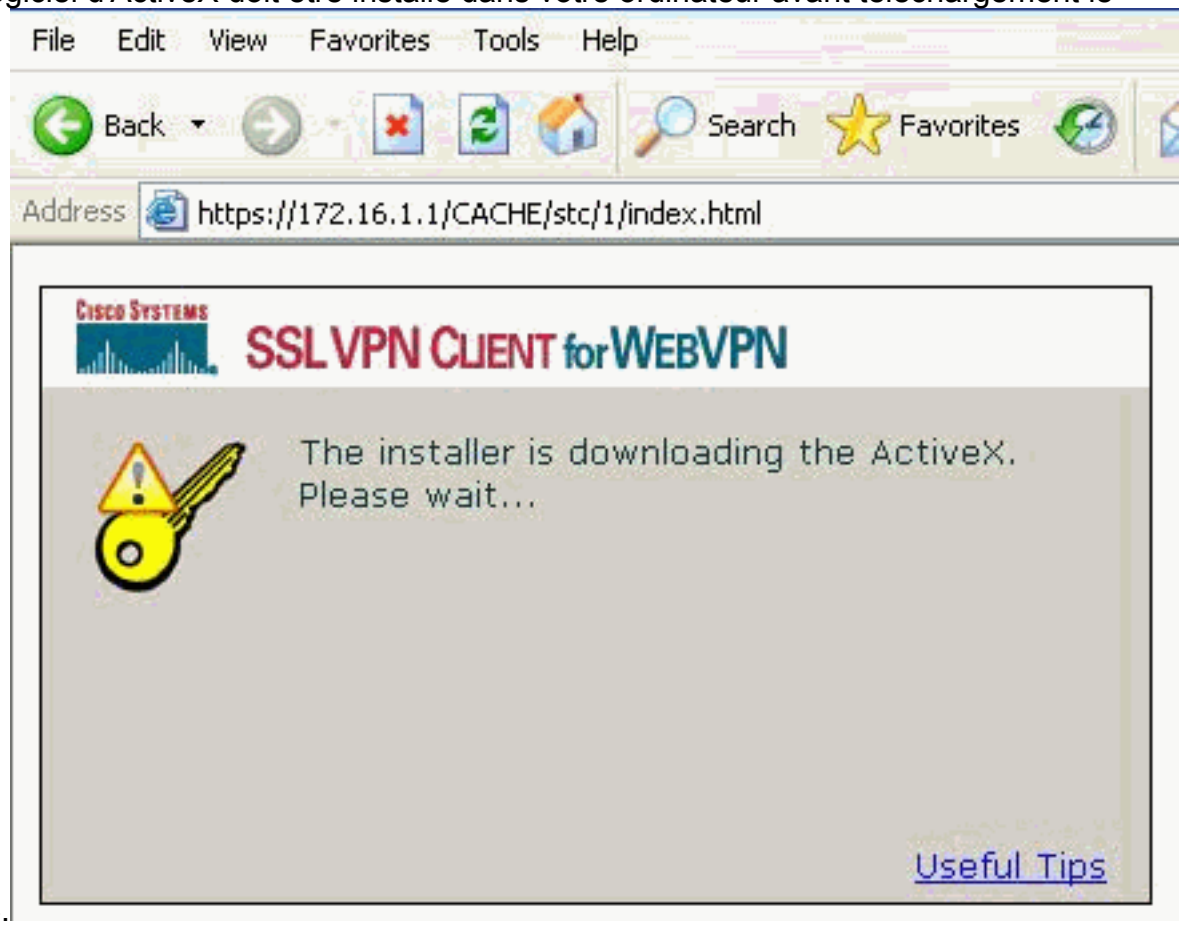
1. Tapez l'URL ou l'adresse IP de l'interface de webvpn de l'ASA en votre navigateur Web dans le format comme affiché.`https://url` OU `https://<IP address of the ASA WebVPN interface>`



2. Écrivez votre nom d'utilisateur et mot de passe et puis choisissez votre groupe respectif de la liste déroulante comme affichée.

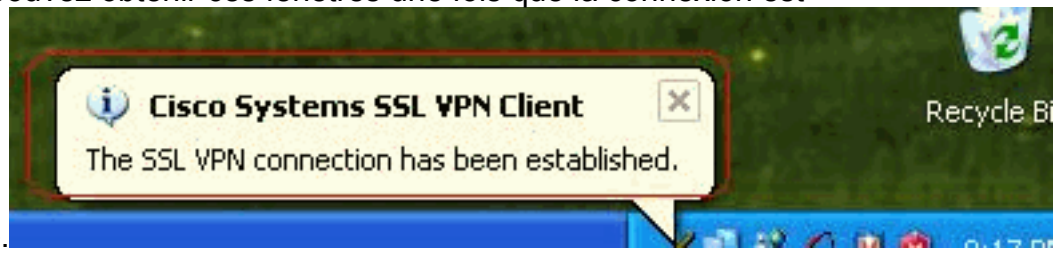


3. Le logiciel d'ActiveX doit être installé dans votre ordinateur avant téléchargement le SVC.

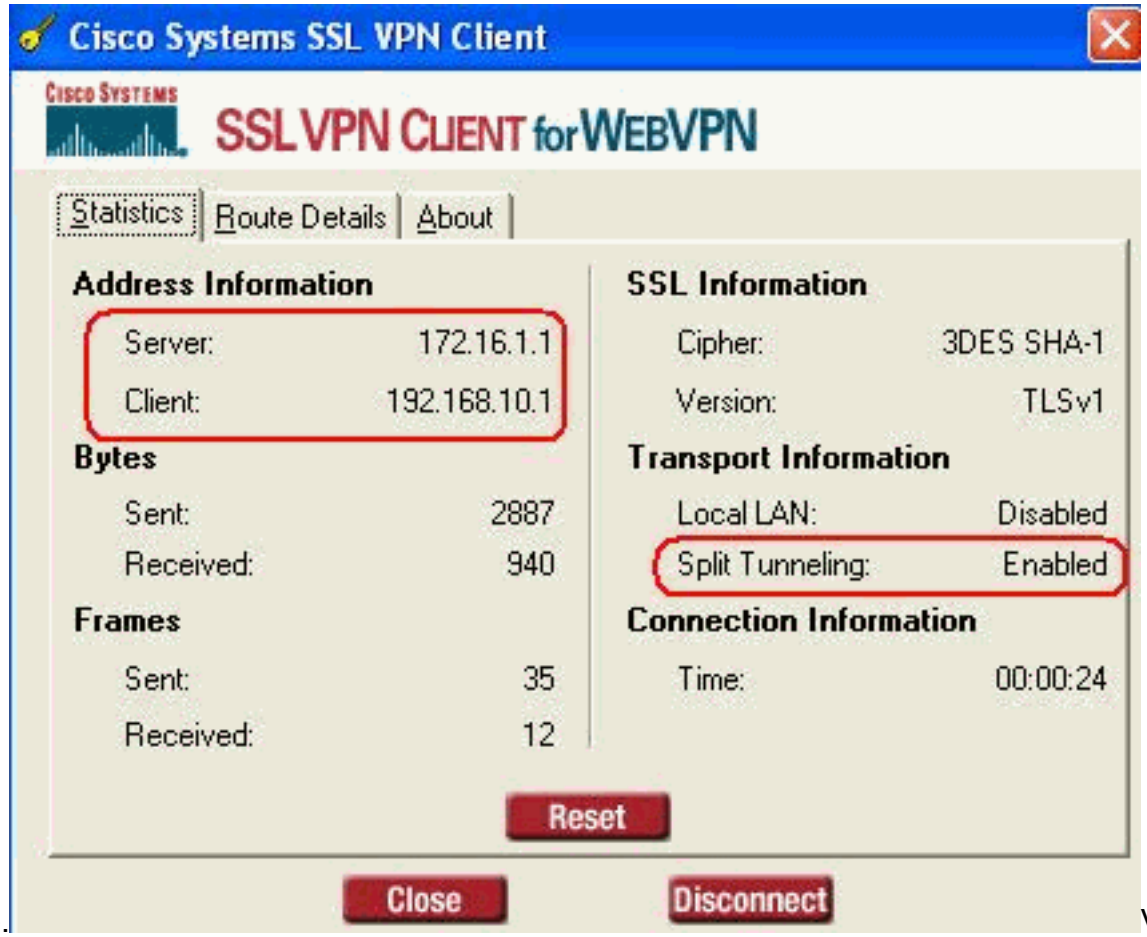


4. Ces fenêtres apparaissent avant que la connexion de VPN SSL soit établie.

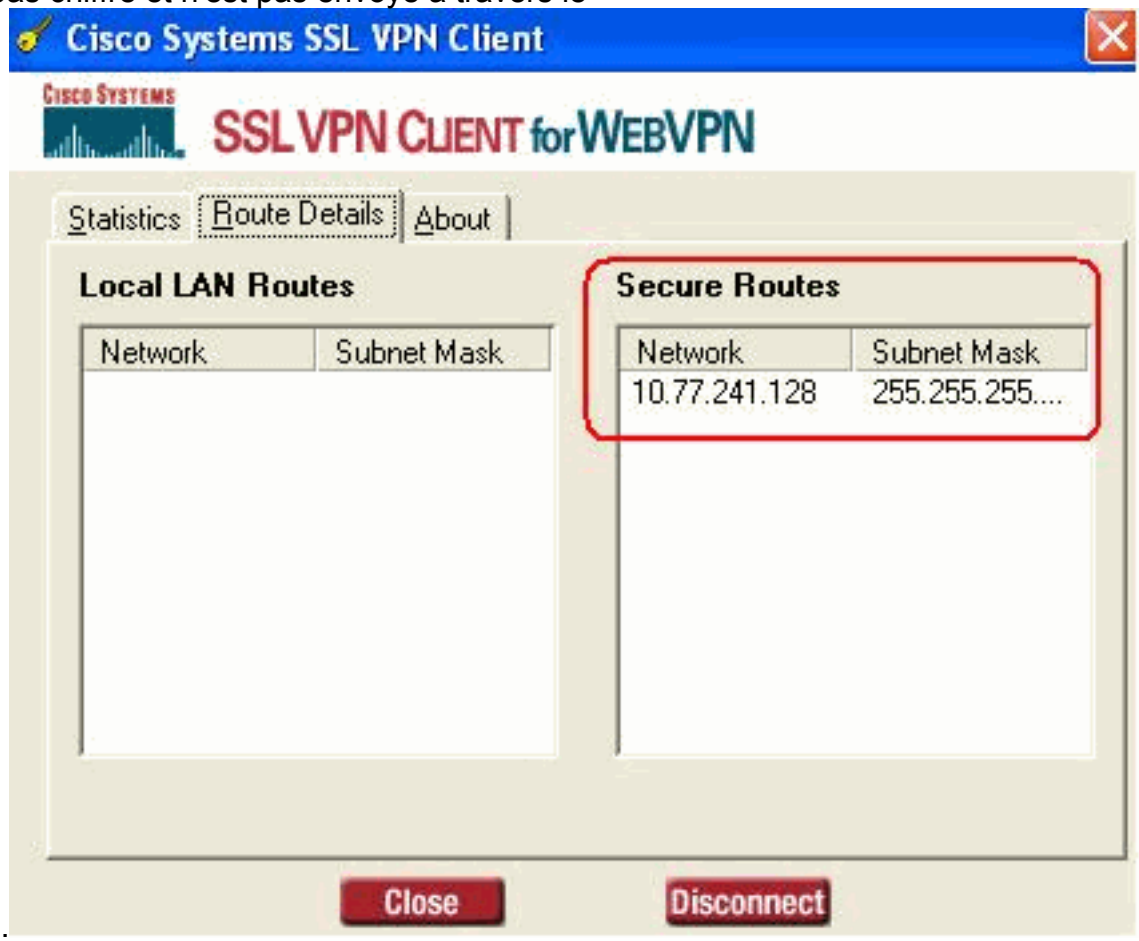
5. Vous pouvez obtenir ces fenêtres une fois que la connexion est établie.



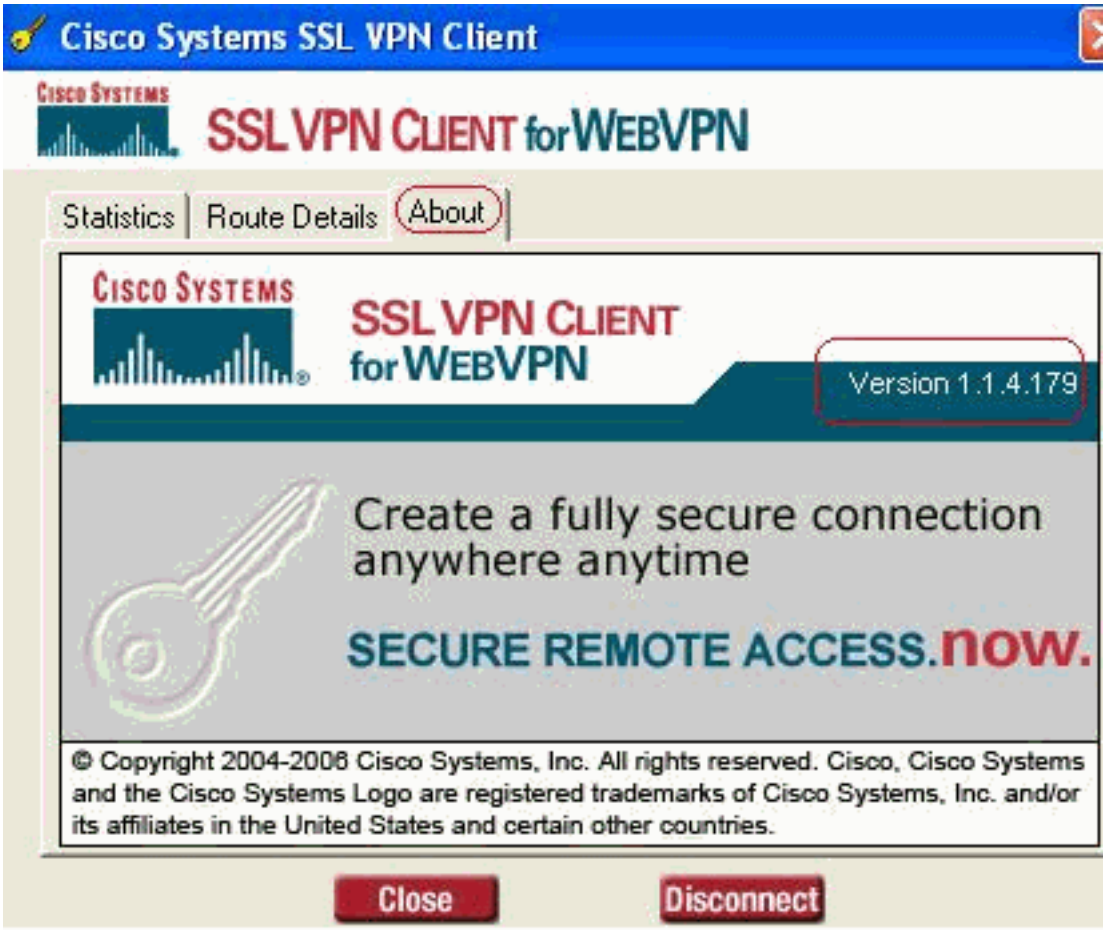
6. Cliquez sur la clé jaune qui apparaît dans la barre des tâches de votre ordinateur. Ces fenêtres apparaît qui fournit des informations sur la connexion SSL. Par exemple, **192.168.10.1** est l'adresse IP attribuée pour le client et serveur que l'adresse IP est 172.16.1.1, **Segmentation de tunnel est activé**, et ainsi de



suite. Vous pouvez également vérifier le réseau sécurisé qui doit être chiffré par le SSL, la liste des réseaux est téléchargé de la liste d'accès de tunnel partagé configurée dans l'ASA.Dans cet exemple, le client de VPN SSL sécurise l'accès à 10.77.241.128/24 alors que tout autre trafic n'est pas chiffré et n'est pas envoyé à travers le



tunnel.

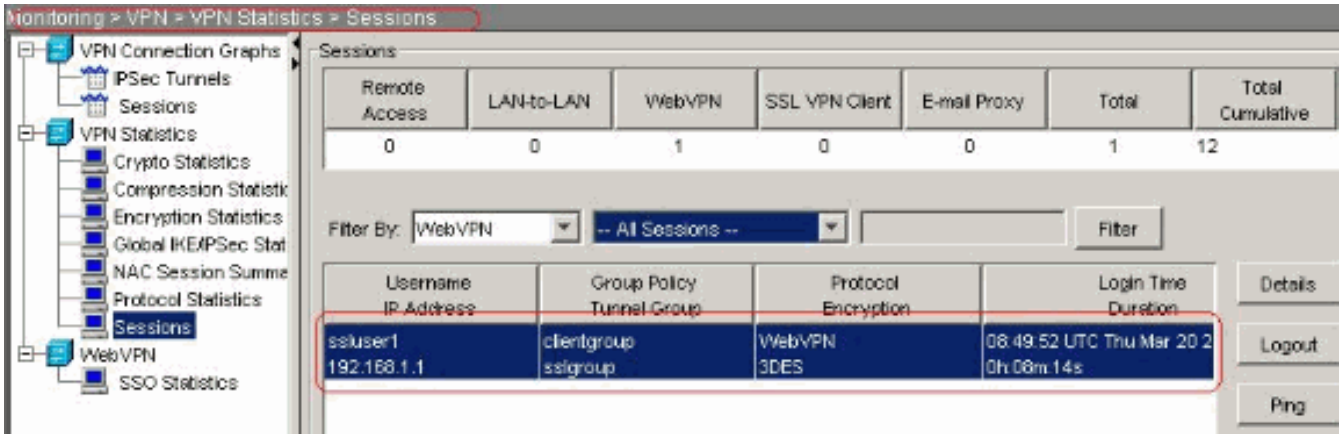


Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre 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** .

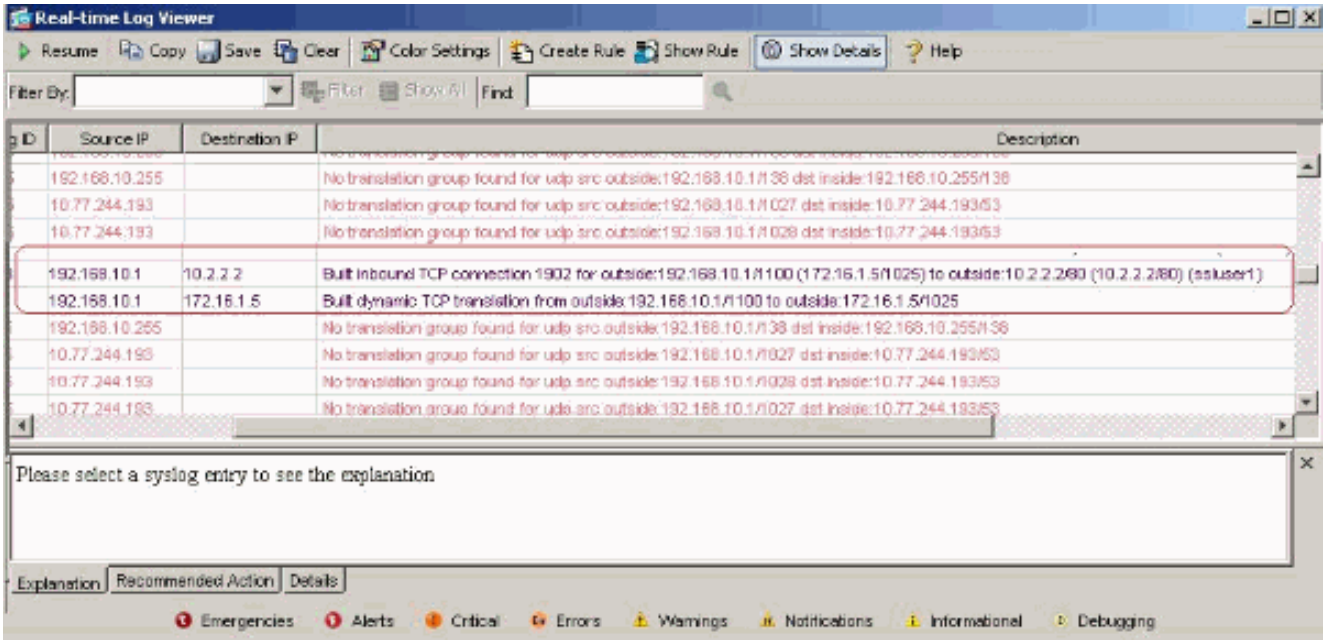
- **show webvpn svc** — Affiche les images de SVC enregistrées dans la mémoire flash de l'ASA.`ciscoasa#show webvpn svc 1. disk0:/sslclient-win-1.1.4.179.pkg 1 CISCO STC win2k+ 1.0.0 1,1,4,179 Fri 01/18/2008 15:19:49.43 1 SSL VPN Client(s) installed`
- **show vpn-sessiondb svc** — Affiche les informations 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 savoir les sessions en cours de webvpn dans l'ASA.



Dépannez

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

1. **vpn-sessiondb logoff name <username>** — Commande pour fermer la session VPN SSL pour le nom d'utilisateur particulier.`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 la commande **vpn-sessiondb logoff svc** afin de terminer toutes les sessions SVC.
2. **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`
3. **debug webvpn svc <1-255>** — Fournit les événements webvpn en temps réel 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
   ```
4. Dans l'ASDM, choisissez **Monitoring > Logging > Real-time Log Viewer > View** afin de voir les événements en temps réel. Ces expositions d'exemple au sujet des informations de session entre le SVC 192.168.10.1 et le web server 10.2.2.2 dans l'Internet par ASA 172.16.1.5.



Informations connexes

- Support de produit d'appliance de sécurité adaptable de gamme Cisco 5500
- ASA/PIX : Permettre le split tunneling pour des clients VPN sur l'exemple de configuration de l'ASA
- Exemple de configuration d'un routeur autorisant les clients VPN à se connecter à IPsec et à Internet via la transmission tunnel partagée
- 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