

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations ASA utilisant ASDM 5.2\(2\)](#)

[Configuration ASA 7.2\(2\) à l'aide de l'interface de ligne de commande](#)

[Établir la connexion VPN SSL avec SVC](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit des instructions détaillées sur la façon d'autoriser les clients VPN SSL (Secure Socket Layer) à accéder à Internet lorsqu'ils sont connectés par tunnel à un appareil de sécurité adaptatif Cisco (ASA). Cette configuration permet un accès sécurisé SVC aux ressources de l'entreprise via SSL et donne un accès non sécurisé à Internet avec l'utilisation de la transmission tunnel partagée.

La possibilité de transmettre du trafic sécurisé comme du trafic non sécurisé sur la même interface est connue sous le nom de transmission tunnel partagée. La transmission tunnel partagée nécessite de spécifier exactement quel trafic est sécurisé et quelle est la destination de ce trafic, de sorte que seul le trafic spécifié entre dans le tunnel, tandis que le reste est transmis sans chiffrement sur 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 bloqué nulle part le long du chemin de connexion

Components Used

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

- Dispositif de sécurité adaptatif (ASA) de la gamme Cisco 5500 qui exécute la version logicielle 7.2(2)
- Version du client VPN SSL Cisco pour Windows 1.1.4.179**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, qui doit être téléchargée sur les ordinateurs des utilisateurs distants afin d'établir la connexion VPN SSL avec ASA. Référez-vous à [Installation du logiciel SVC](#) dans le guide de configuration ASA pour plus d'informations.
- PC exécutant Windows 2000 Professionnel SP4 ou Windows XP SP2
- Cisco Adaptive Security Device Manager (ASDM) version 5.2(2)

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.

Afin d'établir une session SVC, l'utilisateur distant entre l'adresse IP d'une interface WebVPN de l'appliance de sécurité dans le navigateur, et le navigateur se connecte à cette interface et affiche l'écran de connexion WebVPN. Si vous répondez aux critères de connexion et d'authentification et que le dispositif de sécurité vous identifie comme nécessitant le SVC, le dispositif de sécurité télécharge le SVC sur l'ordinateur distant. Si l'appliance de sécurité vous identifie avec l'option d'utilisation du SVC, l'appliance de sécurité télécharge le SVC sur l'ordinateur distant alors qu'il présente un lien dans la fenêtre pour ignorer l'installation du SVC.

Après le téléchargement, le SVC s'installe et se configure, puis le SVC reste ou se désinstalle lui-même, selon la configuration, à partir de l'ordinateur distant lorsque la connexion se termine.

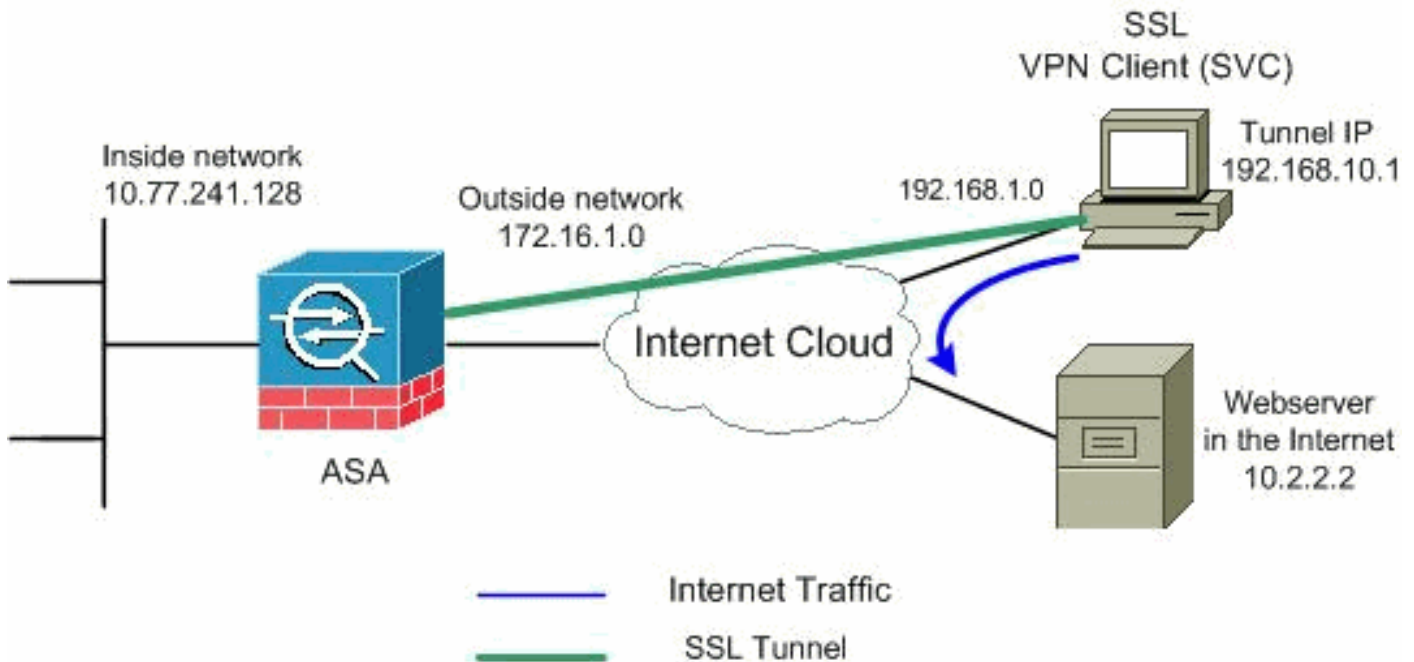
Configuration

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) afin d'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 IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Ce sont des adresses [RFC 1918 qui ont été utilisées dans un environnement de laboratoire](#).

[Configurations ASA utilisant ASDM 5.2\(2\)](#)

Complétez ces étapes afin de configurer le VPN SSL sur ASA avec la transmission tunnel partagée comme indiqué :

1. Le document suppose que la configuration de base, telle que la configuration d'interface, etc., est déjà faite et fonctionne correctement. **Remarque** : référez-vous à [Autoriser l'accès HTTPS pour ASDM](#) afin 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](#).
2. Choisissez **Configuration > VPN > IP Address Management > IP Pools** afin de créer un pool d'adresses IP : **vpnpool** pour les clients

Add IP Pool

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

VPN.

Cliquez sur Apply.

3. **Activez WebVPN** Choisissez **Configuration > VPN > WebVPN > WebVPN Access** et mettez en surbrillance l'interface externe avec la souris et cliquez sur **Enable**. Cochez la case **Activer la liste déroulante Groupe de tunnels** sur la page de connexion WebVPN afin d'activer la liste déroulante s'affiche dans la page de connexion des utilisateurs, pour choisir leurs groupes respectifs.

Configuration > VPN > WebVPN > WebVPN Access

WebVPN Access

Configure access parameters for WebVPN.

Interface	WebVPN Enabled
inside	No
outside	Yes

Port Number:

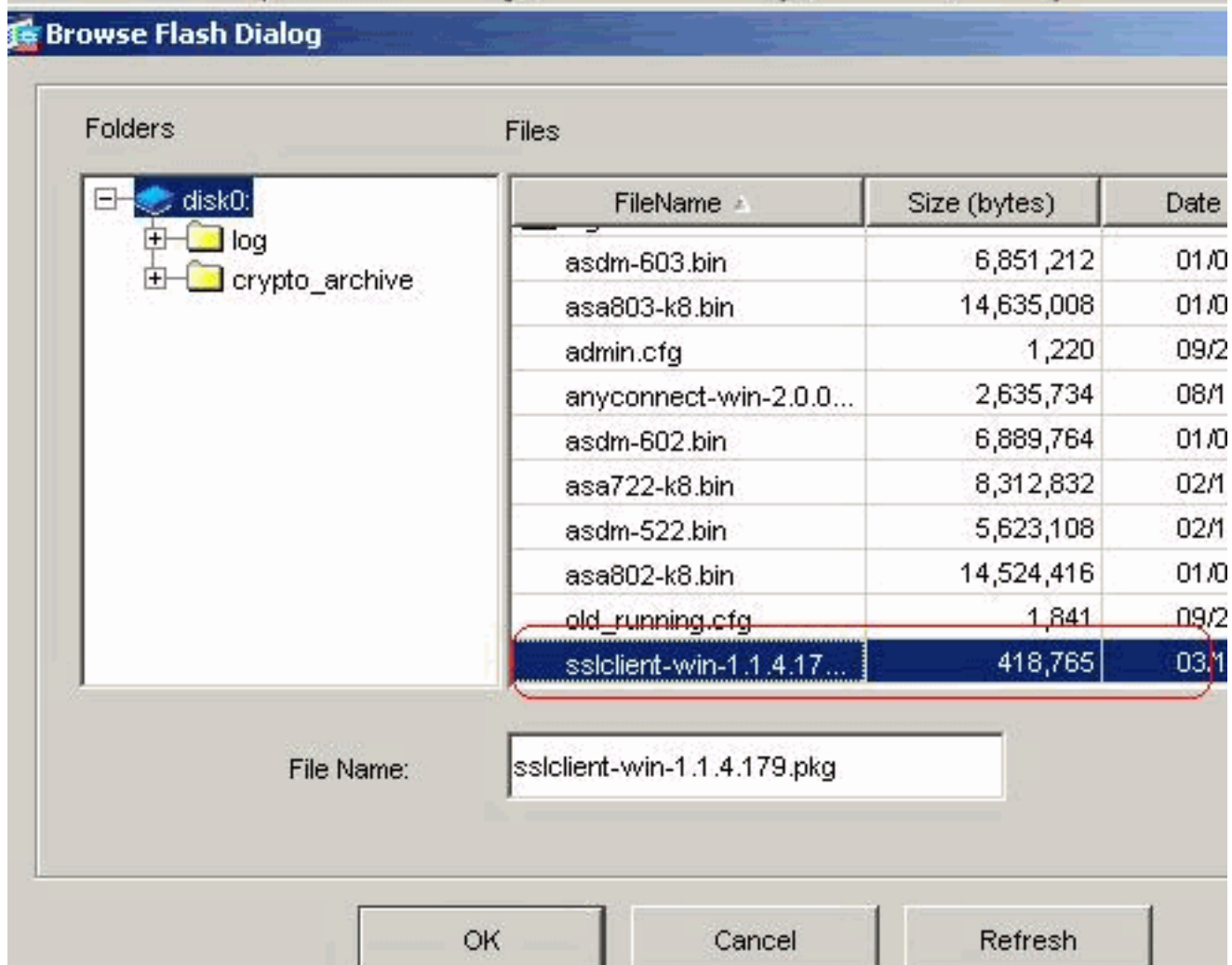
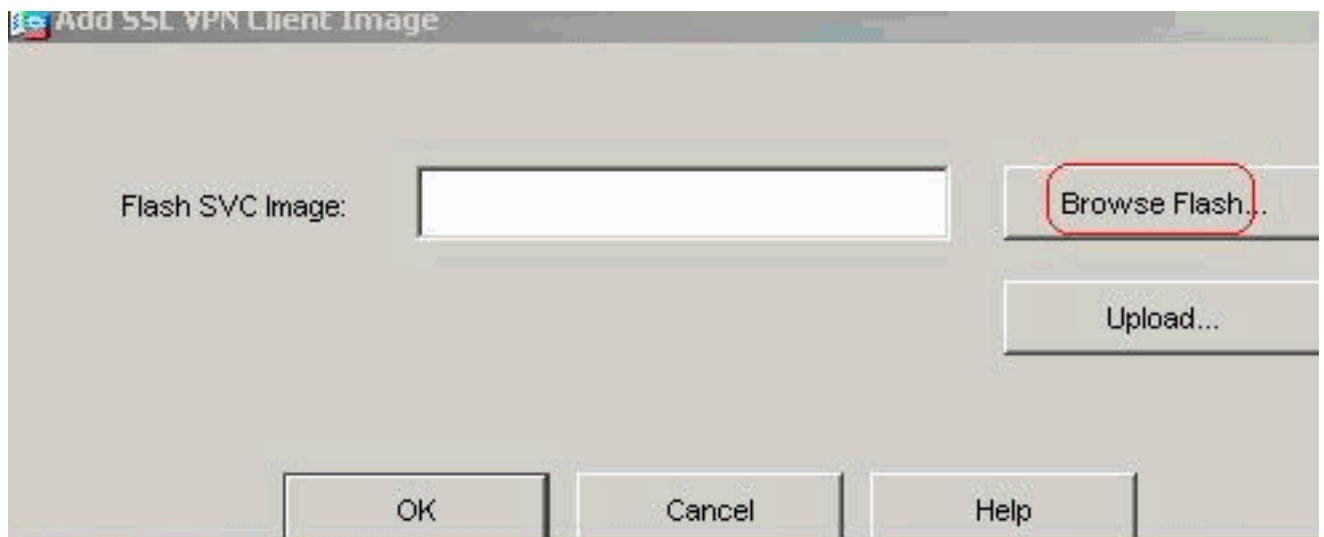
Default Idle Timeout: seconds

Max. Sessions Limit:

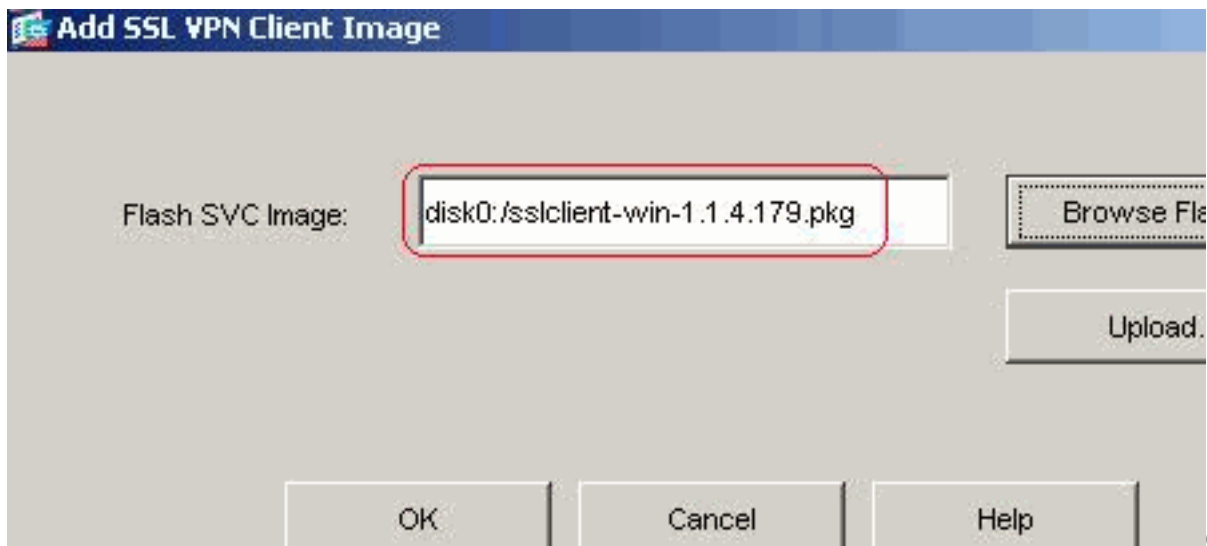
WebVPN Memory Size: % of total physical memory

Enable Tunnel Group Drop-down List on WebVPN Login Page

Cliquez sur Apply. Choisissez **Configuration > VPN > WebVPN > SSL VPN Client > Add** afin d'ajouter l'image du client VPN SSL à partir de la mémoire flash d'ASA comme indiqué.

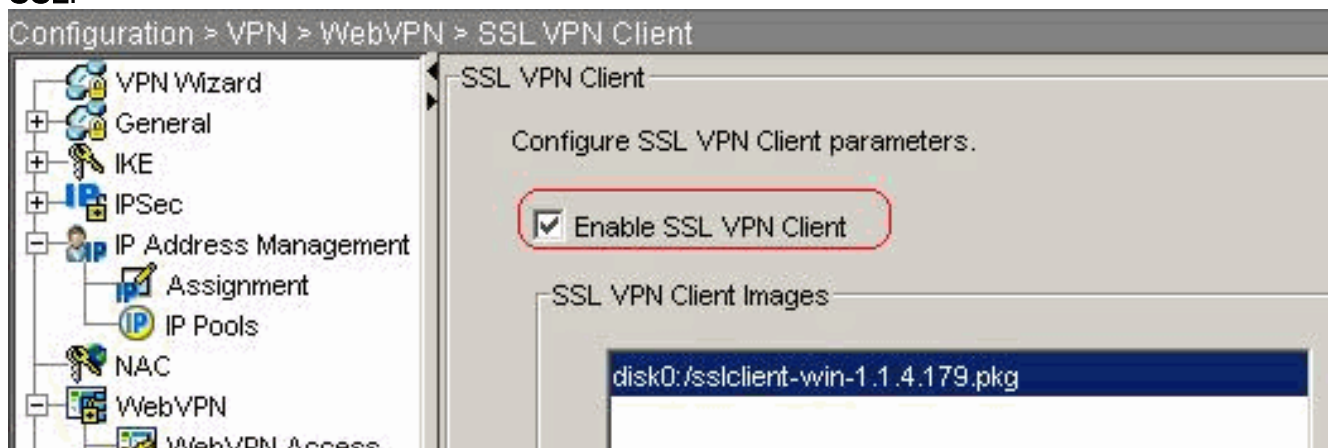


Click



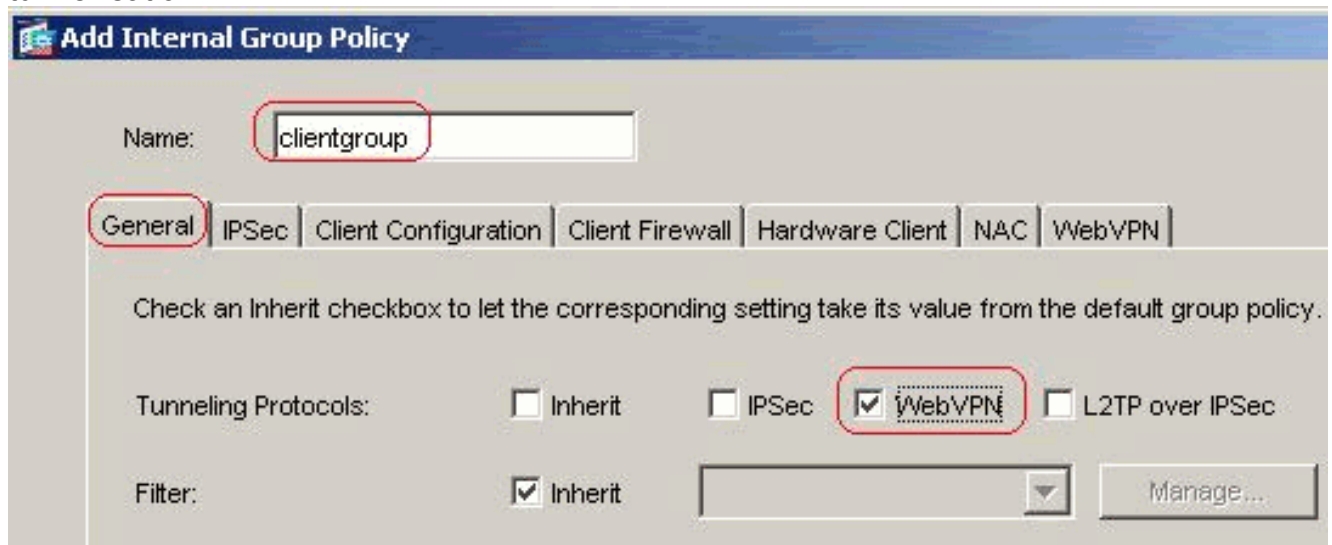
OK.

Cochez la case **Client VPN SSL**.



Cliquez sur Apply. Configuration CLI équivalente :

- Configurez la stratégie de groupe. Choisissez **Configuration > VPN > General > Group Policy > Add (Internal Group Policy)** afin de créer un groupe de clients de stratégie de groupe interne. Sous **General**, activez la case à cocher **WebVPN** afin d'activer le WebVPN en tant que protocole de tunnellation.



Dans l'onglet **Configuration du client > Paramètres généraux du client**, décochez la case **Hériter** pour la stratégie de tunnel partagé et choisissez **Tunnel Network List Below** dans la liste déroulante. Désactivez la case **Inherit** pour la liste **Split Tunnel Network List**, puis cliquez

sur Manage pour lancer l'ACL Manager.

Name:

General | IPsec | **Client Configuration** | Client Firewall | Hardware Client | NAC | WebVPN

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

General Client Parameters | Cisco Client Parameters | Microsoft Client Parameters

Banner: Inherit

Default Domain: Inherit

Split Tunnel DNS Names (space delimited): Inherit

Split Tunnel Policy: Inherit

Split Tunnel Network List: Inherit

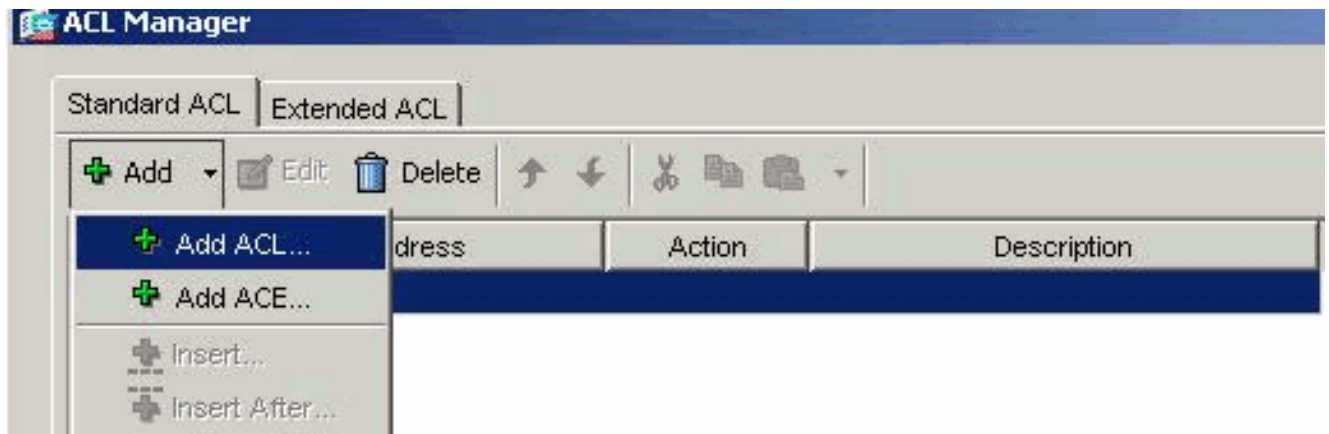
Address pools

Inherit

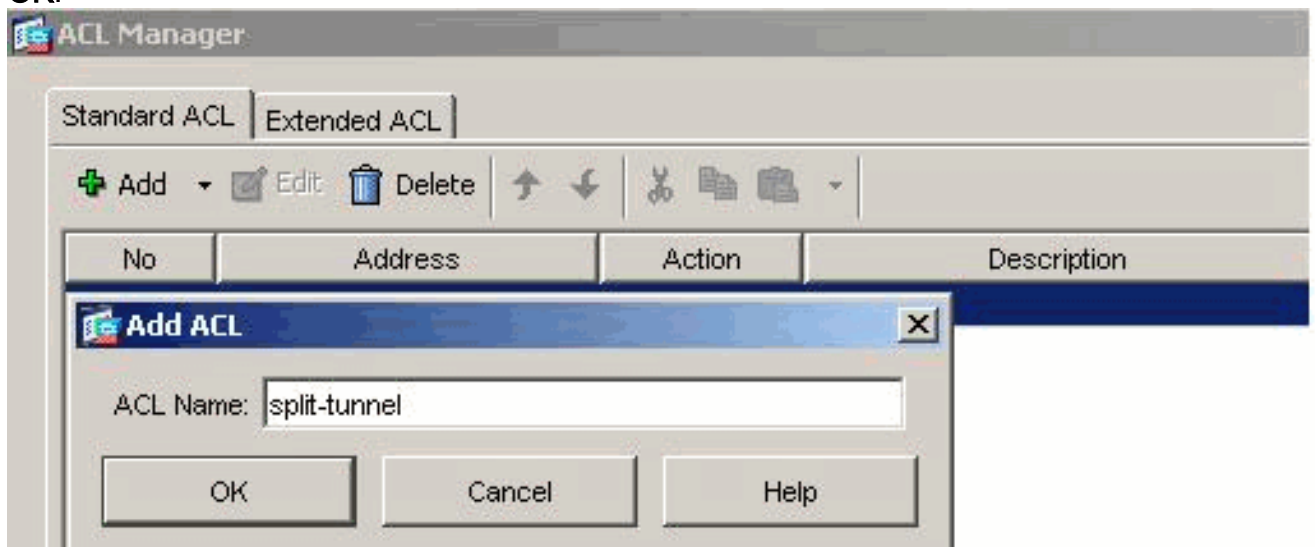
Available Pools:

Assigned Pools (up to 6 entries):

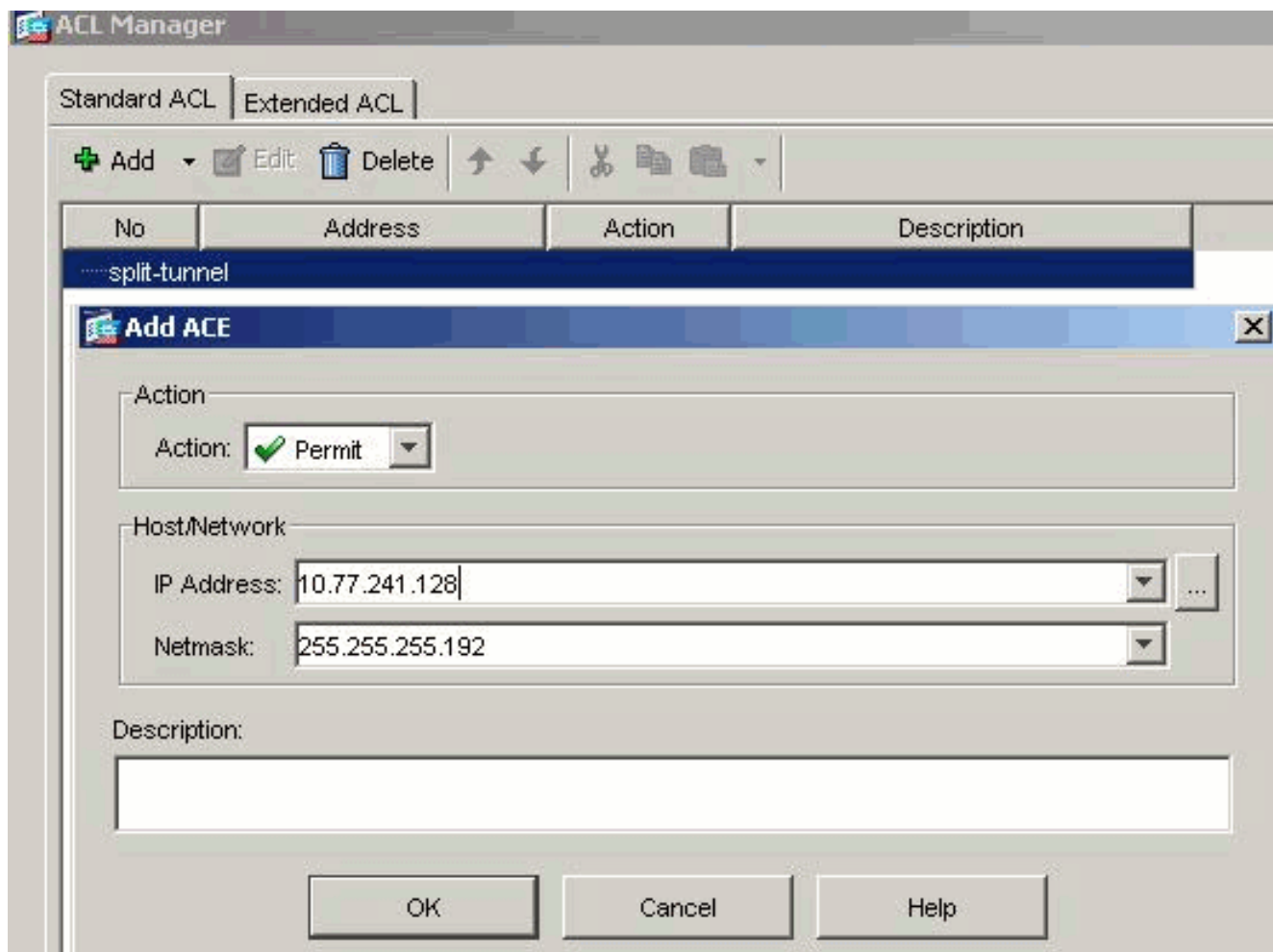
Dans le gestionnaire ACL, choisissez **Ajouter > Ajouter une ACL...** afin de créer une nouvelle liste d'accès.



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 sélectionnez **Autoriser**. 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.

Edit Internal Group Policy: clientgroup

Name:

General | IPsec | **Client Configuration** | Client Firewall | Hardware Client | NAC | WebVPN

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

General Client Parameters | Cisco Client Parameters | Microsoft Client Parameters

Banner: Inherit

Default Domain: Inherit

Split Tunnel DNS Names (space delimited): Inherit

Split Tunnel Policy: Inherit

Split Tunnel Network List: Inherit

Address pools

Inherit

Available Pools:

Assigned Pools (up to 6 entries):

Dans la page principale, cliquez sur **Apply**, puis **Send** (si nécessaire) afin d'envoyer les commandes à l'ASA. Pour l'option Utiliser le client VPN SSL, décochez la case **Hériter** et cliquez sur la case d'option **Facultatif**. Ce choix permet au client distant de choisir s'il doit cliquer sur l'onglet **WebVPN > SSLVPN Client**, et de choisir les options suivantes : 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 Install 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

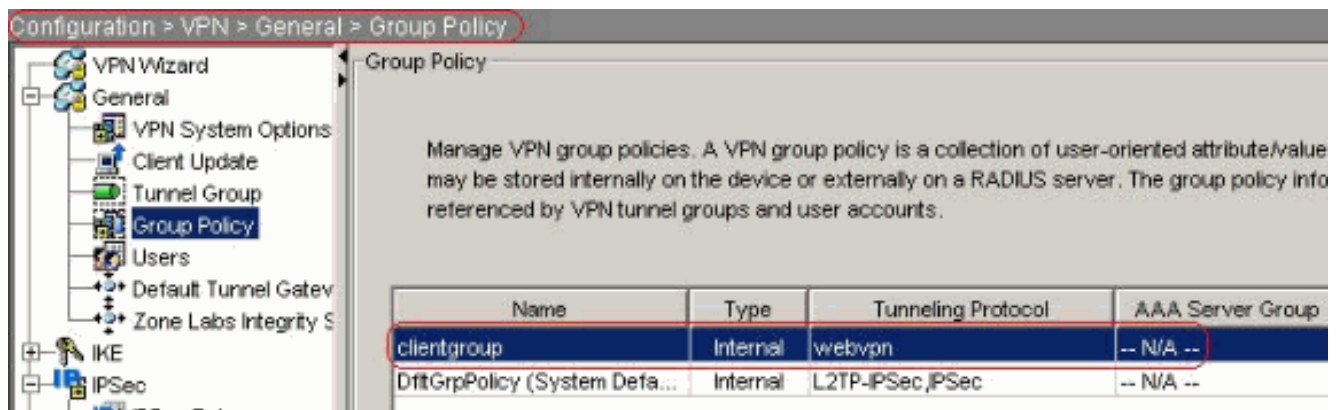
case **Inherit**, décochez la case à cocher **Unlimited** et saisissez le nombre de minutes jusqu'à une nouvelle saisie. La sécurité est renforcée lorsque vous définissez les limites sur la durée de validité d'une clé. Pour l'option Renegotiation Method, décochez la case à cocher **Inherit** et cliquez sur 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

The screenshot shows the 'Edit Internal Group Policy: clientgroup' dialog box. The 'Name' field contains 'clientgroup'. The 'WebVPN' tab is selected. Below the tabs, there is a section for 'Configure WebVPN attributes using the following tabs'. The 'SSL VPN Client' sub-tab is selected. The settings are as follows:

Setting	Inherit	Option 1	Option 2	Option 3
Use SSL VPN Client:	<input type="checkbox"/>	<input type="radio"/> Always	<input checked="" type="radio"/> Optional	<input type="radio"/> Never
Keep Installer on Client System:	<input type="checkbox"/>	<input checked="" type="radio"/> Yes	<input type="radio"/> No	
Compression:	<input checked="" type="checkbox"/>	<input type="radio"/> Enable	<input type="radio"/> Disable	
Keepalive Messages:	<input checked="" type="checkbox"/>	<input type="checkbox"/> Enable	Interval: <input type="text"/>	seconds
Key Renegotiation Settings				
Renegotiation Interval:	<input type="checkbox"/>	<input type="checkbox"/> Unlimited	<input type="text" value="30"/> minutes	
Renegotiation Method:	<input type="checkbox"/>	<input type="radio"/> None	<input checked="" type="radio"/> SSL	<input type="radio"/> New tunnel
Dead Peer Detection				
Gateway Side Detection:	<input checked="" type="checkbox"/>	<input type="checkbox"/> Enable	Interval: <input type="text"/>	seconds
Client Side Detection:	<input checked="" type="checkbox"/>	<input type="checkbox"/> Enable	Interval: <input type="text"/>	seconds

At the bottom of the dialog box, there are three buttons: 'OK', 'Cancel', and 'Help'.

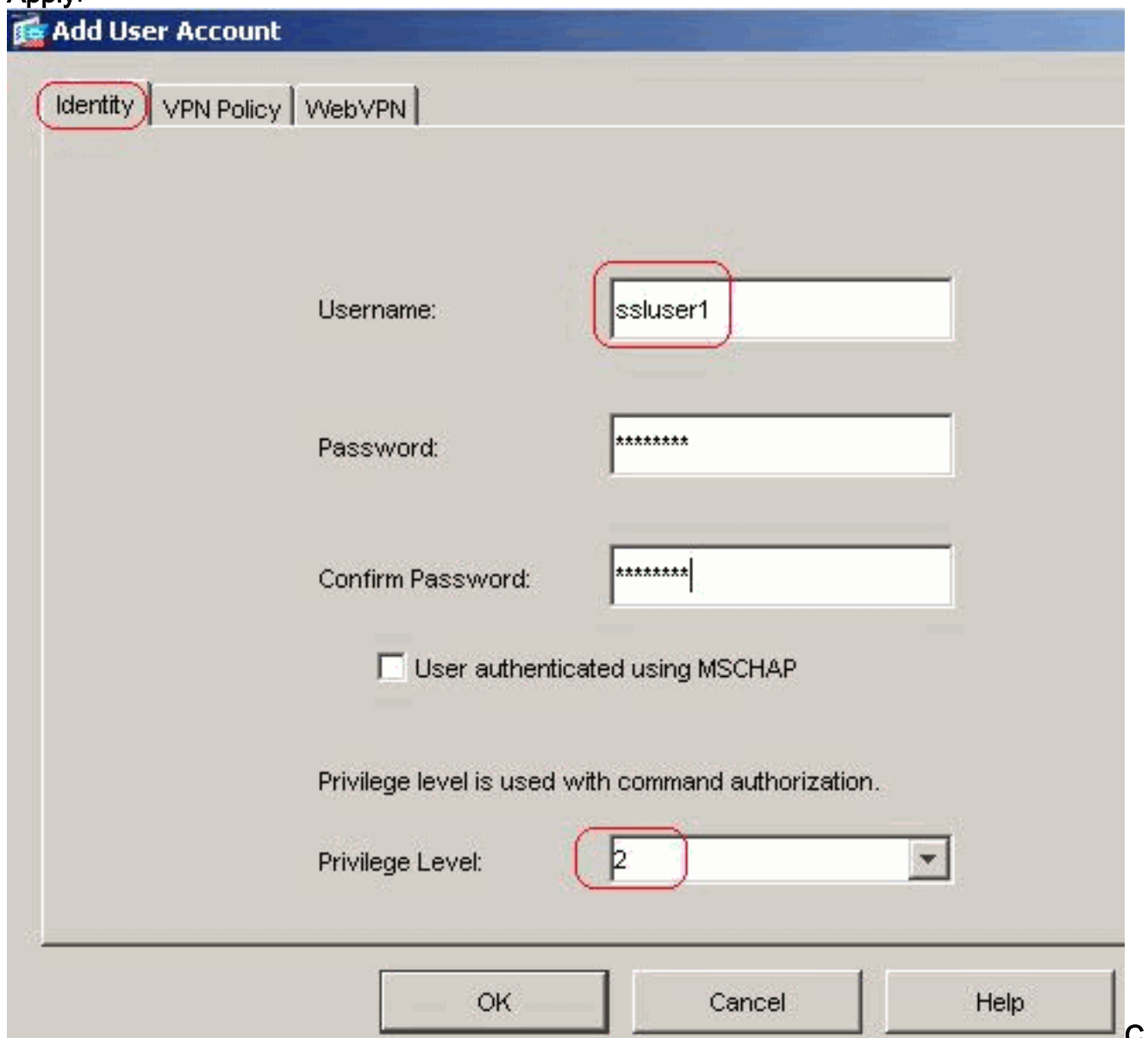
Cliquez sur **OK**, puis sur **Apply**.



Configuration CLI équivalente :

5. Choisissez **Configuration > VPN > General > Users > Add** afin de créer un nouveau compte d'utilisateur **ssluser1**. Cliquez sur **OK**, puis sur

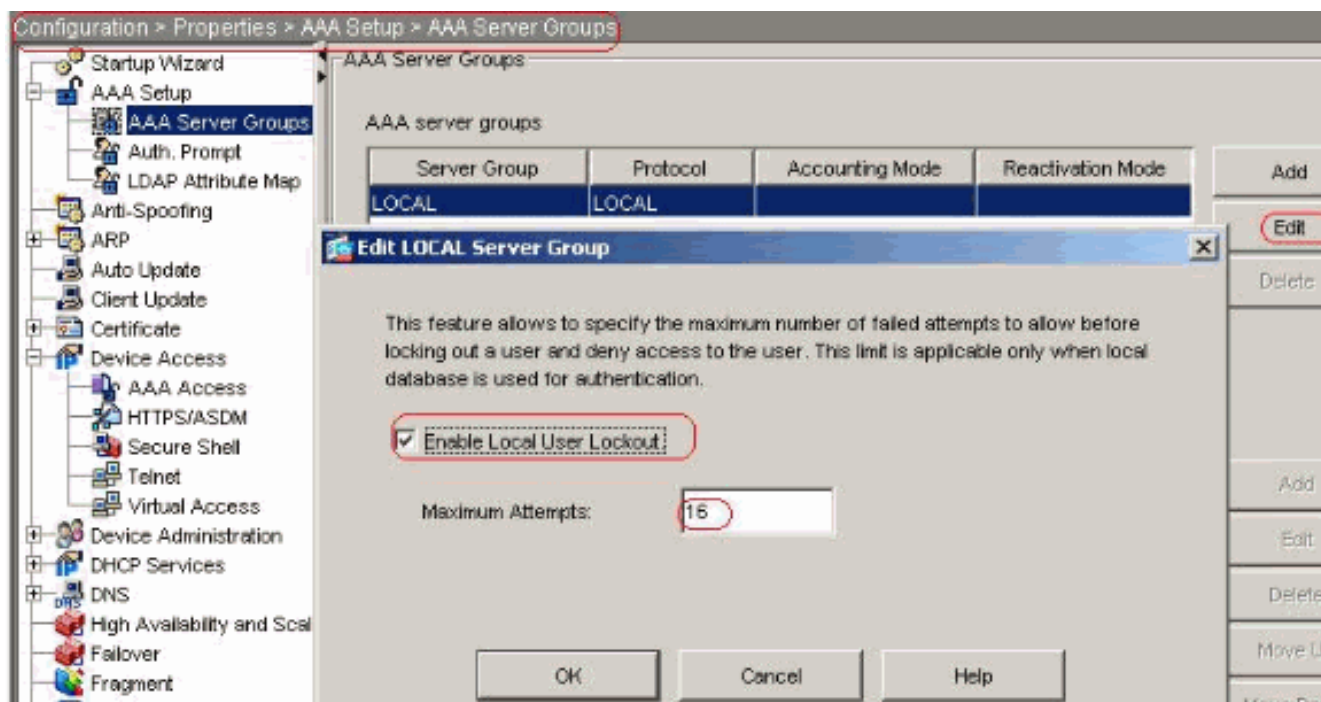
Apply.



onfiguration CLI équivalente :

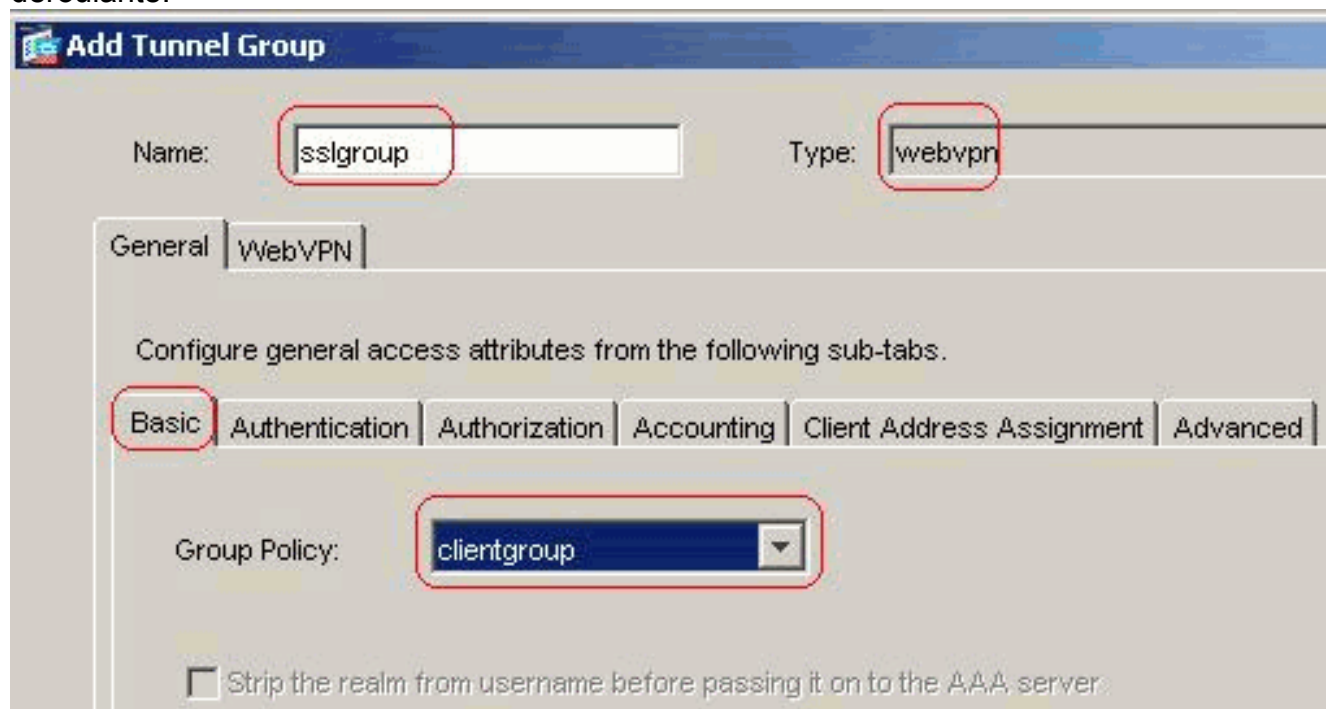
6. Choisissez **Configuration > Properties > AAA Setup > AAA Servers Groups > Edit** afin de modifier le groupe de serveurs par défaut **LOCAL** et activez la case à cocher **Enable Local User Lockout** avec la valeur maximale de tentatives

16.



Configuration CLI équivalente :

- Configurez le groupe de tunnels. Choisissez Configuration > VPN > General > Tunnel Group > Add (WebVPN access) afin de créer un nouveau groupe de tunnels **sslgroup**. Dans l'onglet Général > Basique, sélectionnez la stratégie de groupe en tant que **groupe de clients** dans la liste déroulante.



Dans **General > Client Address Assignment**, sous Address Pools, cliquez sur **Add** » afin d'affecter le pool d'adresses disponible **vpnpool**.

Add Tunnel Group

Name: Type:

General | WebVPN

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | **Client Address Assignment** | Advanced

To specify whether to use DHCP or address pools for address assignment, go to Configuration > VPN > IP Address Management > Assignment.

DHCP Servers

IP Address:

Address Pools

To configure interface-specific address pools, go to the Advanced tab.

Available Pools

Assigned pools

vpnpool

Dans l'onglet **WebVPN > Alias de groupe et URL**, tapez le nom de l'alias dans la zone de paramètres et cliquez sur **Ajouter »** afin de le faire apparaître dans la liste des noms de groupe dans la page de connexion.

General | **WebVPN**

Configure WebVPN access attributes from the following sub-tabs.

Basic | NetBIOS Servers | **Group Aliases and URLs** | Web Page

Group Aliases

Alias:

Enable

Alias	Status
sslgroup_users	enable

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

8. **Configurer NAT** Choisissez **Configuration > NAT > Add > Add Dynamic NAT Rule** pour le

trafic provenant du réseau interne qui peut être traduit avec l'adresse IP externe

Select	Pool ID	Addresses Pool
<input checked="" type="checkbox"/>	1	172.16.1.5

172.16.1.5.

Cliquez sur OK et

sur **Appliquer** dans la page principale. **Configuration CLI équivalente :**

9. Configurez l'exemption nat pour le trafic de retour du réseau interne vers le 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\(2\) à l'aide de l'interface de ligne de commande](#)

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 0:05:00
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
esmtip 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

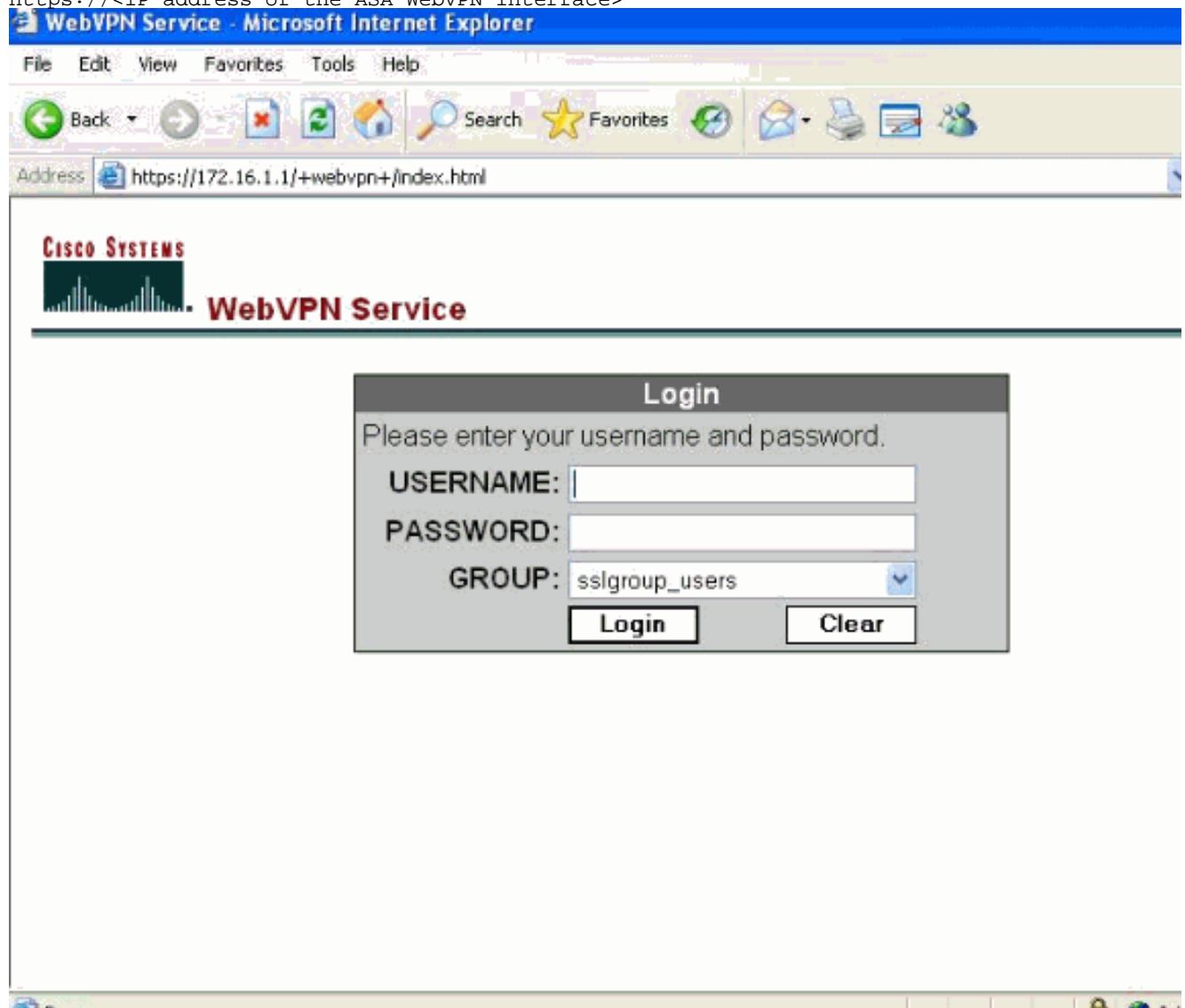
Exécutez ces étapes afin d'établir une connexion VPN SSL avec l'ASA .

1. Tapez l'URL ou l'adresse IP de l'interface WebVPN de l'ASA dans votre navigateur Web au format indiqué.

https://url

OU

https://<IP address of the ASA WebVPN interface>



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

Login

Please enter your username and password.

USERNAME:

PASSWORD:

GROUP: ▼

indiqué.

3. Le logiciel ActiveX doit être installé sur votre ordinateur avant de télécharger le



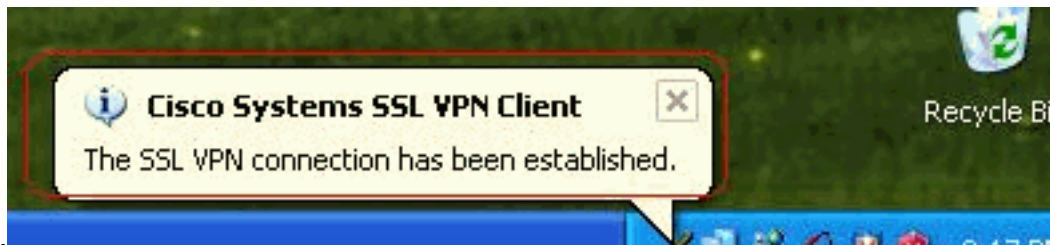
SVC.

4. Ces fenêtres apparaissent avant l'établissement de la connexion VPN



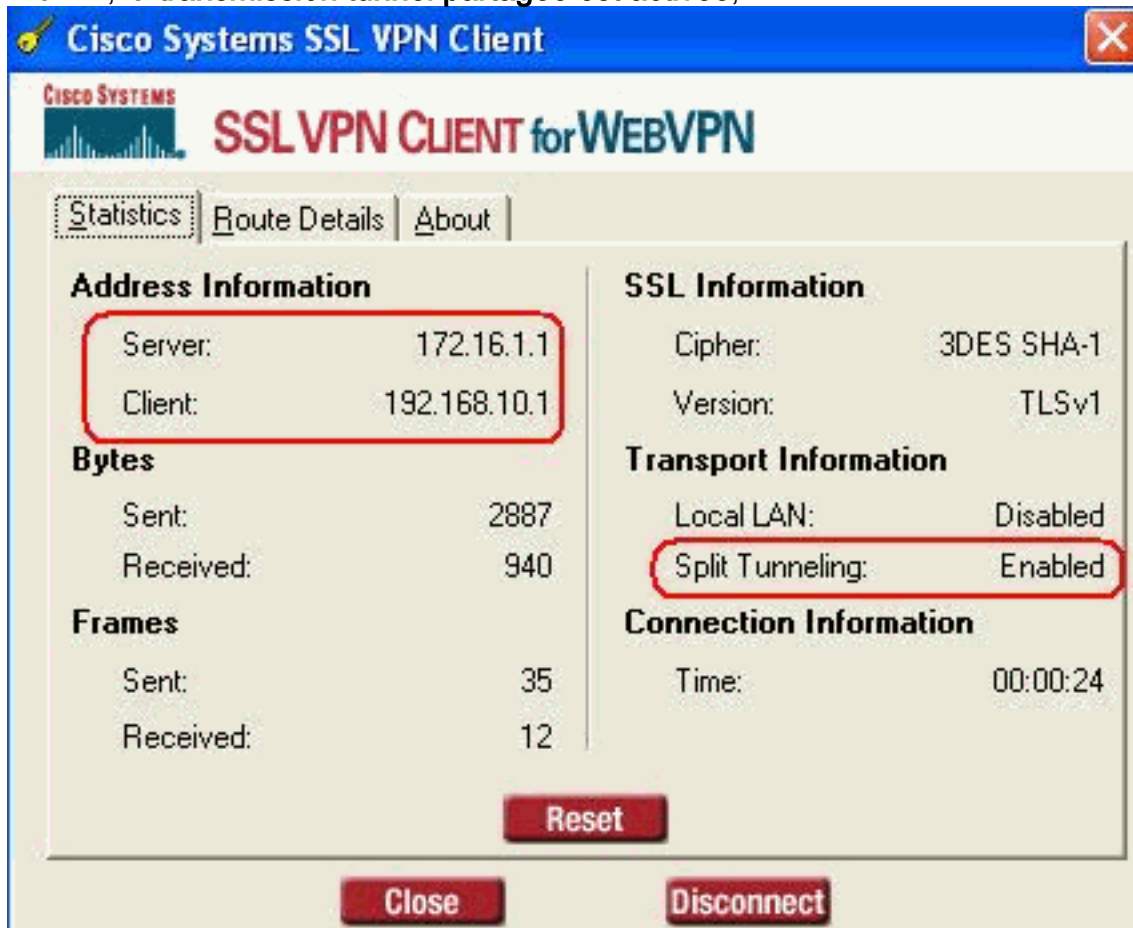
SSL.

5. Vous pouvez obtenir ces fenêtres une fois la connexion



établie.

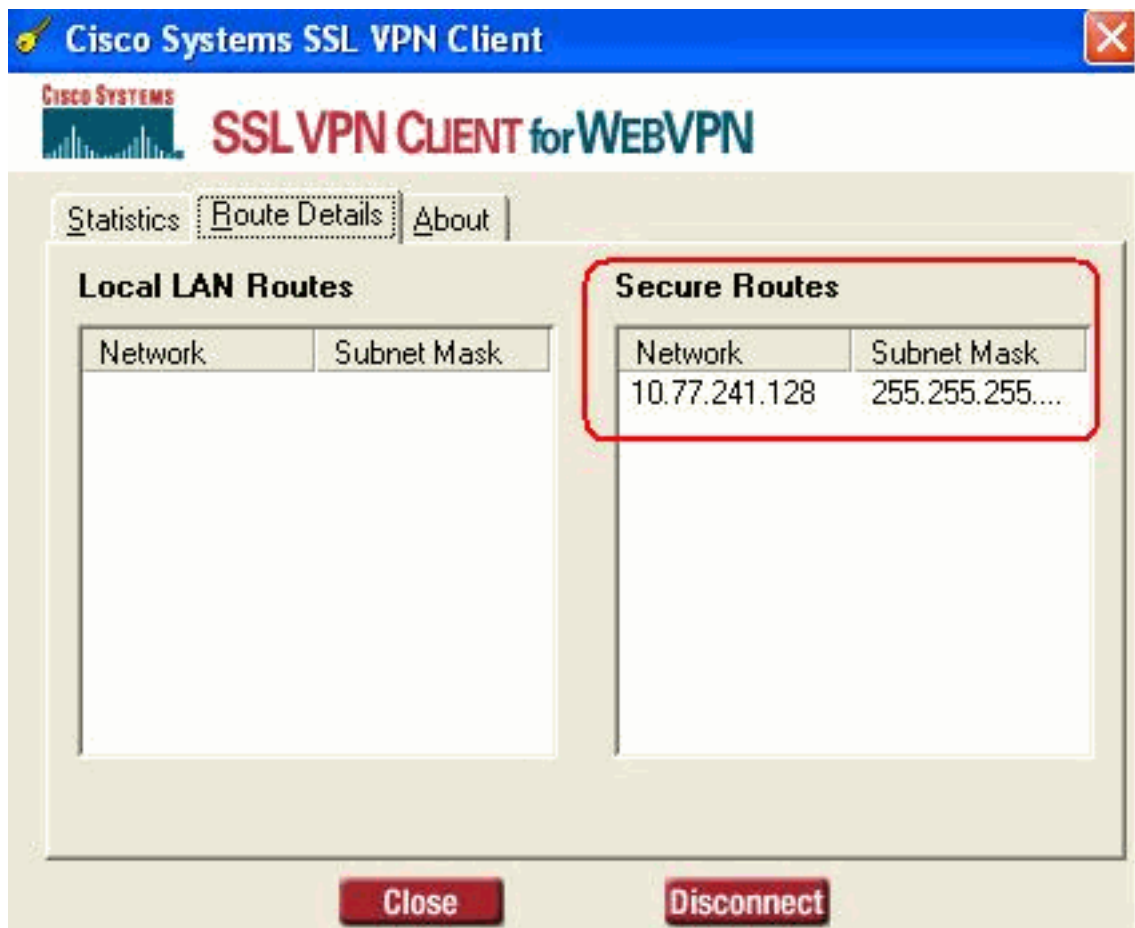
6. Cliquez sur la touche jaune qui apparaît dans la barre des tâches de votre ordinateur. Ces fenêtres s'affichent et fournissent des informations sur la connexion SSL. Par exemple, **192.168.10.1** est l'adresse IP attribuée pour l'adresse IP du client et du serveur est 172.16.1.1, la **transmission tunnel partagée est activée**,



etc.

Vous

pouvez également vérifier le réseau sécurisé qui doit être chiffré par SSL, la liste de réseau est téléchargée à partir de la liste d'accès à tunnel partagé configurée dans ASA. Dans cet exemple, le client 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.



Vérification

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 ASDM, choisissez **Monitoring > VPN > VPN Statistics > Sessions** afin de connaître les sessions WebVPN actuelles dans l'ASA.

The screenshot shows the ASDM interface for monitoring VPN sessions. The left sidebar shows the navigation tree with 'Sessions' selected under 'VPN Statistics'. The main window displays a summary table and a detailed table of sessions.

Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
0	0	1	0	0	1	12

Filter By: WebVPN -- All Sessions -- Filter

Username	IP Address	Group Policy	Tunnel Group	Protocol	Encryption	Login Time	Duration	Details	Logout	Ping
ssluser1	192.168.1.1	clientgroup	sslgroup	WebVPN	3DES	08:49:52 UTC Thu Mar 20 2008	0h:08m:14s			

Dépannage

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_uauth: success!
webvpn_svc_np_tear_down: no ACL
INFO: 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, la connexion VPN SSL peut être interrompue.

```
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
```

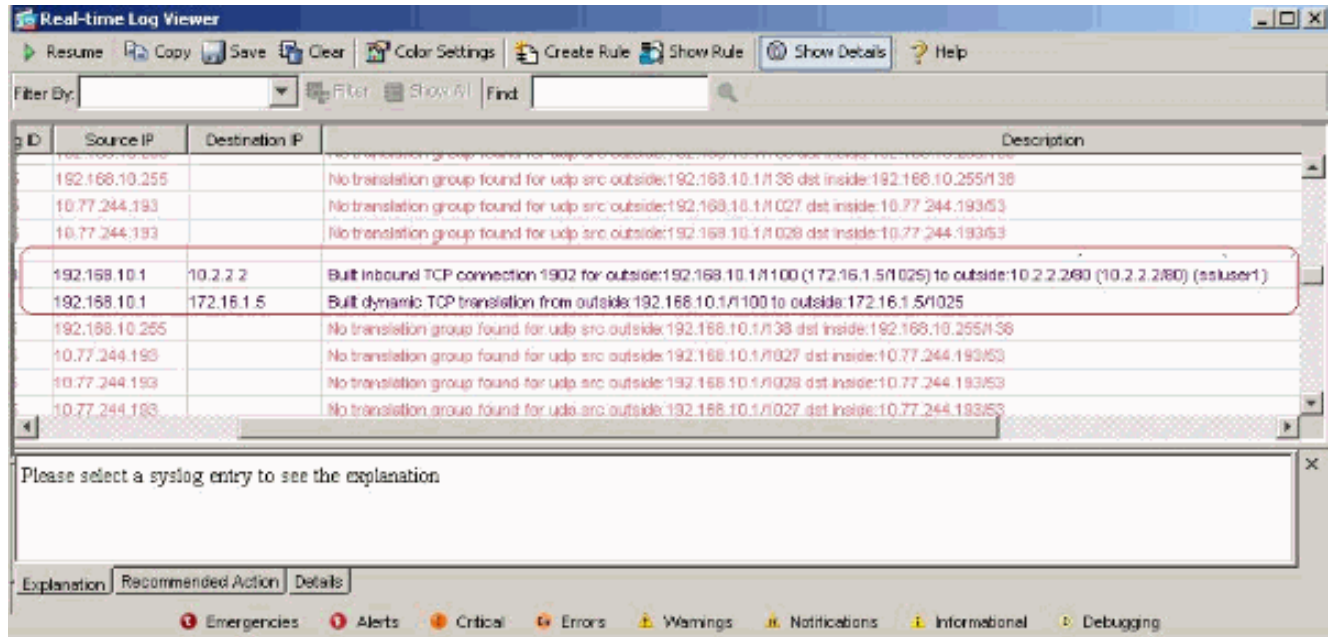
```
ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
..input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
..input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
..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@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2'
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. Cet exemple montre les informations de session entre le SVC 192.168.10.1 et le Webserver 10.2.2.2 dans Internet via ASA 172.16.1.5.



Informations connexes

- [Assistance produit des appareils de sécurité adaptatifs de la 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](#)