

ASA 8.x : Exemple de configuration d'autorisation de la transmission tunnel partagée pour un client VPN AnyConnect sur le dispositif ASA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration d'ASA utilisant l'ASDM 6.0\(2\)](#)

[Configuration de l'interface de ligne de commande ASA](#)

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

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit des instructions pas à pas sur la façon de permettre l'accès de Cisco AnyConnect VPN Client à Internet tandis qu'ils sont reliés par tunnel à un appliance de sécurité adaptable Cisco (ASA) 8.0.2. Cette configuration permet l'accès client sécurisé aux ressources de l'entreprise par l'intermédiaire du SSL tout en donnant l'accès non sécurisé à Internet en utilisant le split tunnelling.

[Conditions préalables](#)

[Conditions requises](#)

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

- L'appliance de sécurité ASA doit exécuter une version 8.x
- Cisco AnyConnect VPN Client 2.x **Remarque** : Téléchargez le package AnyConnect VPN Client (anyconnect-win*.pkg) à partir du [téléchargement de logiciels](#) Cisco (clients [enregistrés](#) uniquement). Copiez le client VPN d'AnyConnect 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 l'ASA. Référez-vous à la section [Installer le client d'AnyConnect du guide de configuration d'ASA pour plus d'informations](#).

Components Used

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

- ASA de la gamme Cisco 5500 qui exécute le logiciel version 8.0(2)
- Client VPN SSL Cisco AnyConnect version pour Windows 2.0.0343
- PC qui exécute Microsoft Vista, Windows XP SP2 ou Windows 2000 Professionnel SP4 avec Microsoft Installer version 3.1
- Cisco Adaptive Security Device Manager (ASDM) version 6.0(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 Cisco AnyConnect VPN Client fournit les connexions sécurisées SSL au dispositif de sécurité pour des utilisateurs distants. Sans client installé précédemment, les utilisateurs distants saisissent dans leur navigateur l'adresse IP d'une interface configurée pour accepter les connexions VPN SSL. À moins que le dispositif de sécurité soit configuré pour rediriger des demandes de http:// à https://, les utilisateurs doivent saisir l'URL sous la forme https://<adresse>.

Après avoir saisi l'URL, le navigateur se connecte à cette interface et affiche l'écran d'ouverture de connexion. Si la connexion et l'authentification de l'utilisateur sont acceptées, et que l'appareil de sécurité identifie que l'utilisateur demande le client, il télécharge le client correspondant au système d'exploitation de l'ordinateur distant. Après téléchargement, le client s'installe et se configure automatiquement, établit une connexion SSL sécurisée et reste ou se désinstalle automatiquement (selon la configuration du dispositif de sécurité) quand la connexion se termine.

Avec un client installé précédemment, quand l'utilisateur s'authentifie, le dispositif de sécurité examine la révision du client et met à niveau le client selon les besoins.

Quand le client négocie une connexion VPN SSL avec le dispositif de sécurité, il se connecte en utilisant la Transport Layer Security (TLS), et sur option, la Datagram Transport Layer Security (DTLS). La DTLS permet d'éviter les problèmes de latence et de bande passante associés à certaines connexions SSL et d'améliorer les performances des applications en temps réel qui sont sensibles aux retards de paquet.

Le client d'AnyConnect peut être téléchargé depuis le dispositif de sécurité ou il peut être installé manuellement sur le PC distant par l'administrateur système. Référez-vous au [Guide d'administration du client VPN Cisco AnyConnect](#) pour plus d'informations sur l'installation

manuelle du client.

Le dispositif de sécurité télécharge le client en fonction de la stratégie de groupe ou des attributs du nom d'utilisateur de l'utilisateur établissant la connexion. Vous pouvez configurer le dispositif de sécurité pour qu'il télécharge automatiquement le client ou vous pouvez le configurer pour qu'il demande à l'utilisateur distant s'il souhaite télécharger le client. Dans le dernier cas, si l'utilisateur ne répond pas, vous pouvez configurer le dispositif de sécurité pour qu'il télécharge le client après un délai d'attente ou qu'il présente la page de connexion.

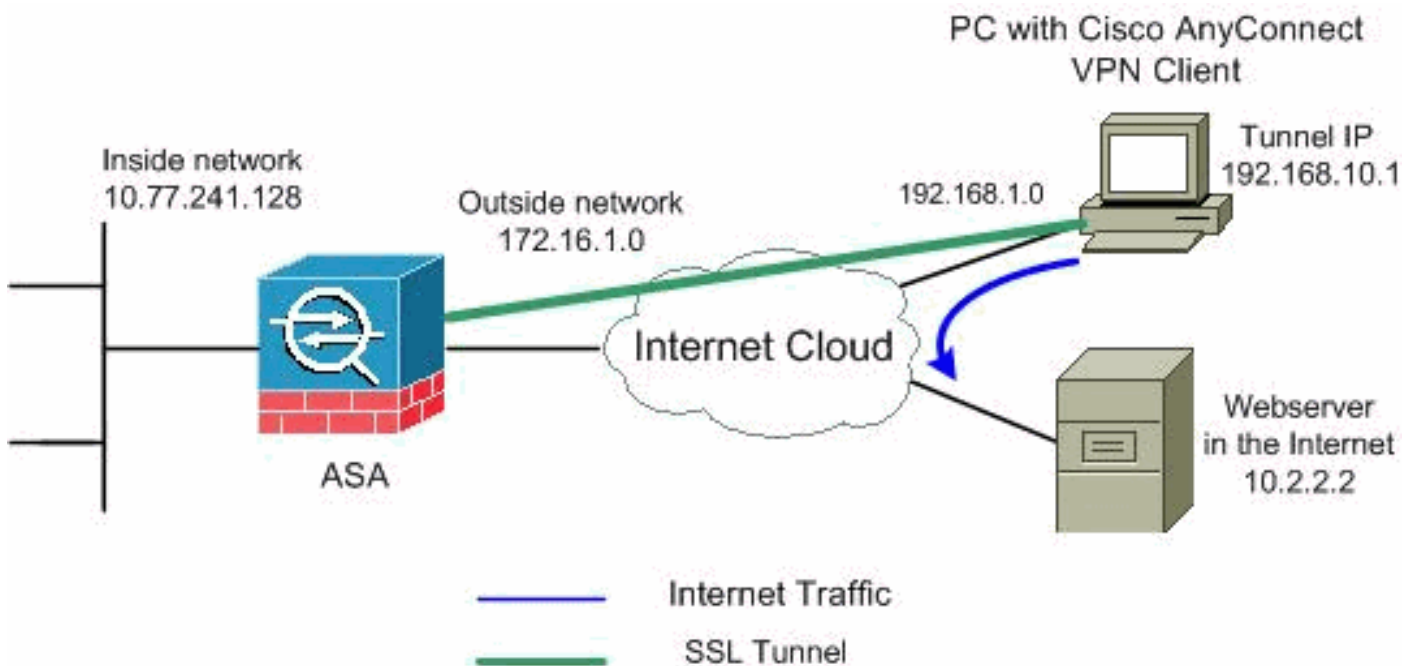
Configuration

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

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



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 utilisés dans un environnement de laboratoire](#).

Configuration d'ASA utilisant l'ASDM 6.0(2)

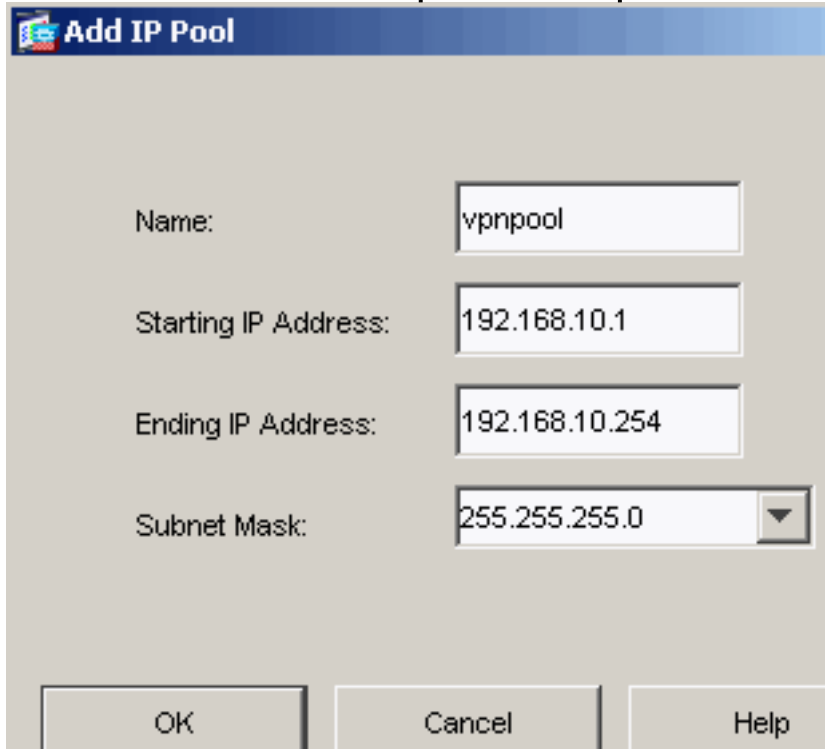
Ce document suppose que la configuration de base, telle que la configuration d'interface, est déjà faite et fonctionne correctement.

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.](#)

Exécutez ces étapes afin de configurer le VPN SSL sur l'ASA avec le split tunneling :

1. Choisissez **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add** pour créer un pool d'adresses IP



The screenshot shows a dialog box titled "Add IP Pool" with the following fields and values:

Field	Value
Name:	vpnpool
Starting IP Address:	192.168.10.1
Ending IP Address:	192.168.10.254
Subnet Mask:	255.255.255.0

Buttons: OK, Cancel, Help

vpnpool.

2. Cliquez sur Apply. Configuration CLI équivalente :
3. Activez WebVPN. Choisissez **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** et sous **Access Interfaces**, cliquez les cases à cocher **Allow Access** et **Enable DTLS** pour l'interface externe. En outre, cliquez la case à cocher **Enable Cisco AnyConnect VPN Client** ou **legacy SSL VPN Client access on the interface selected in the table below** afin d'activer le VPN SSL sur l'interface externe.

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at [Client Settings](#))

Access Interfaces

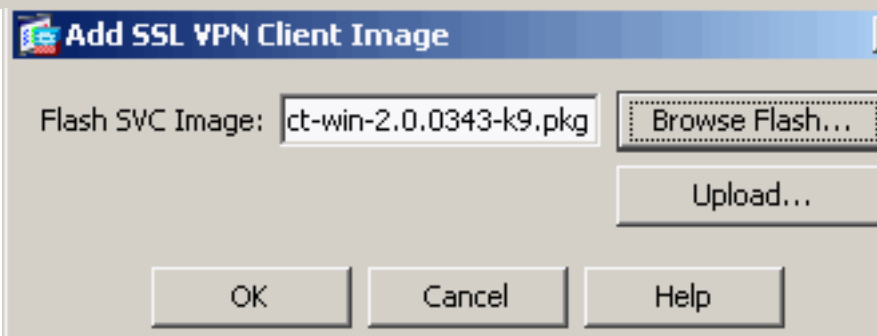
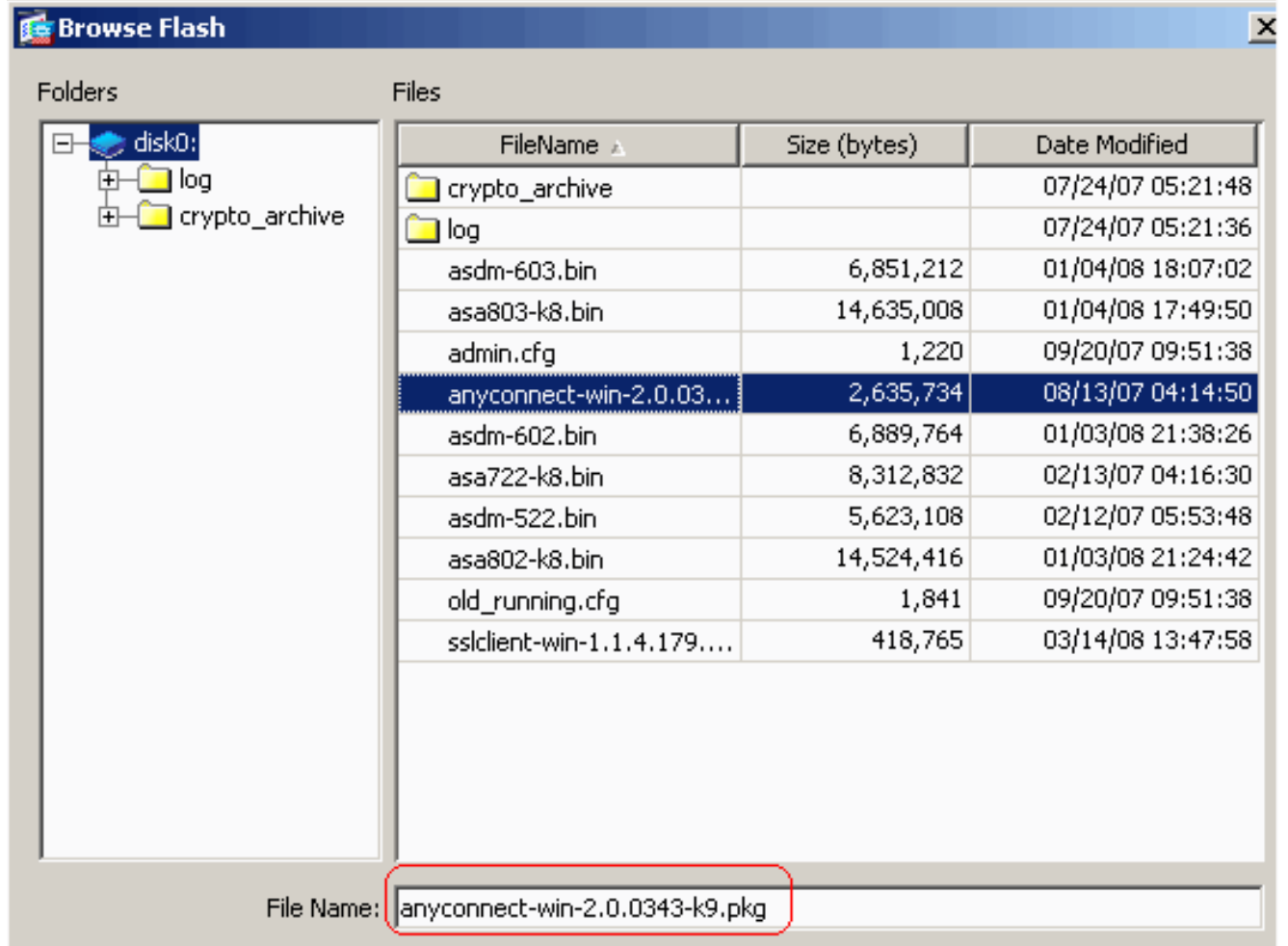
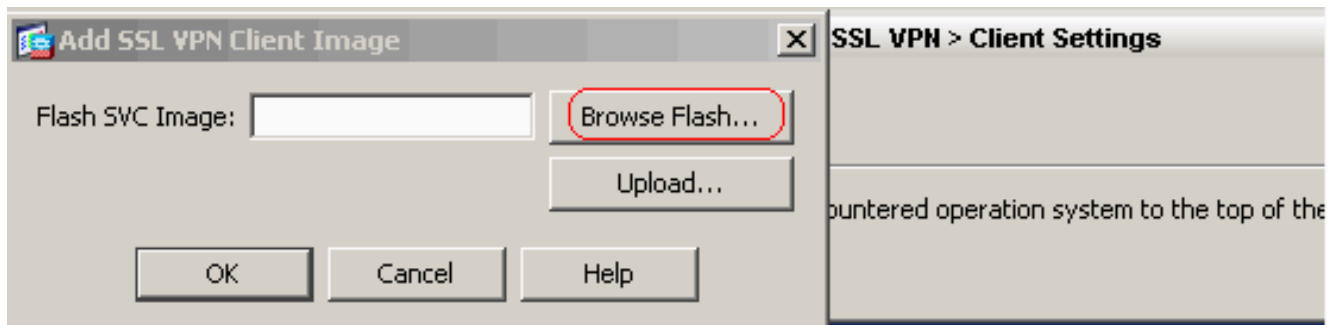
Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Access Port: DTLS Port:

Click here to [Assign Certificate to Interface](#).

Cliquez sur Apply. Choisissez **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add** afin d'ajouter l'image de Cisco AnyConnect VPN Client depuis la mémoire flash de l'ASA comme indiqué.



Click OK.

Cliquez sur

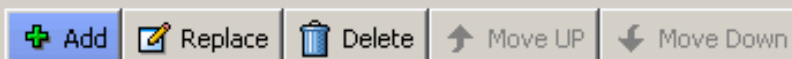
Add.

Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings

Identify SSL VPN Client (SVC) related files.

SSL VPN Client Images

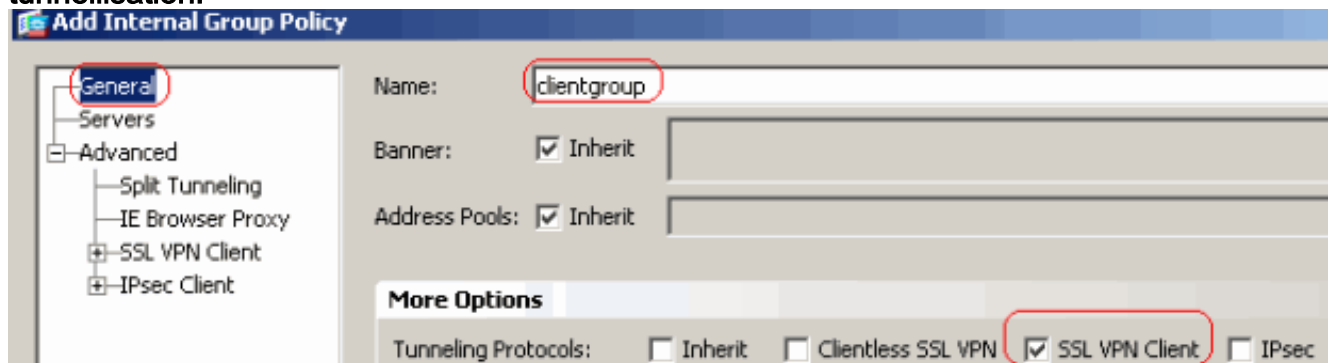
Minimize connection setup time by moving the image used by the most commonly encountered operation system to t



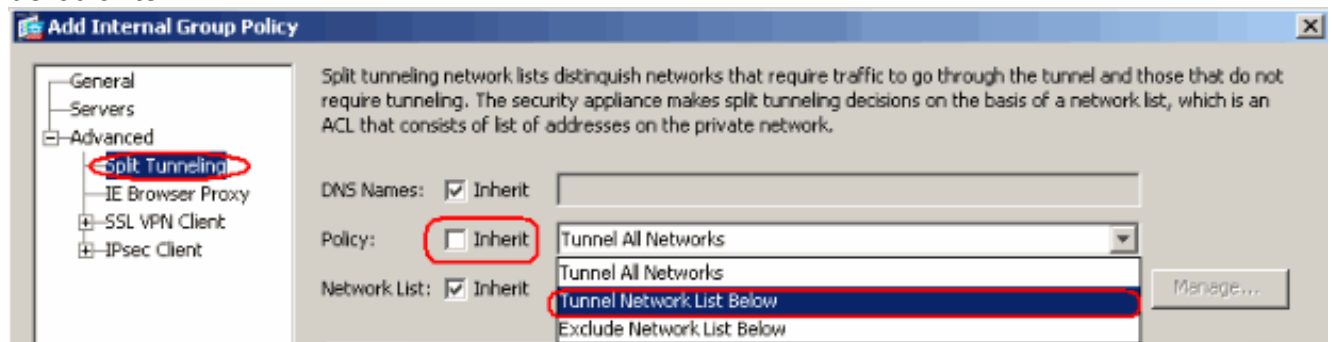
disk0:/anyconnect-win-2.0.0343-k9.pkg

Configuration CLI équivalente :

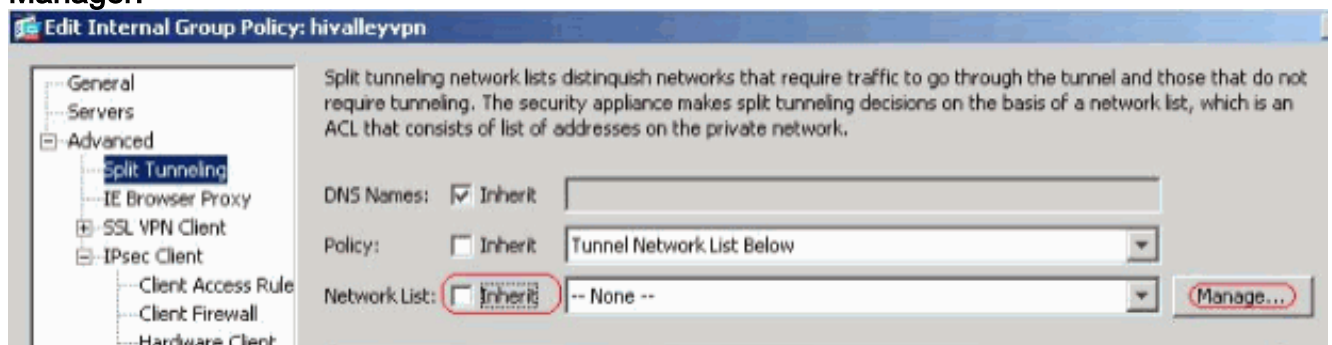
4. Configurez la stratégie de groupe. Choisissez **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** afin de créer une stratégie de groupe interne clientgroup. Sous l'onglet **General**, sélectionnez la case à cocher **SSL VPN Client** afin d'activer le WebVPN comme protocole de tunnellation.



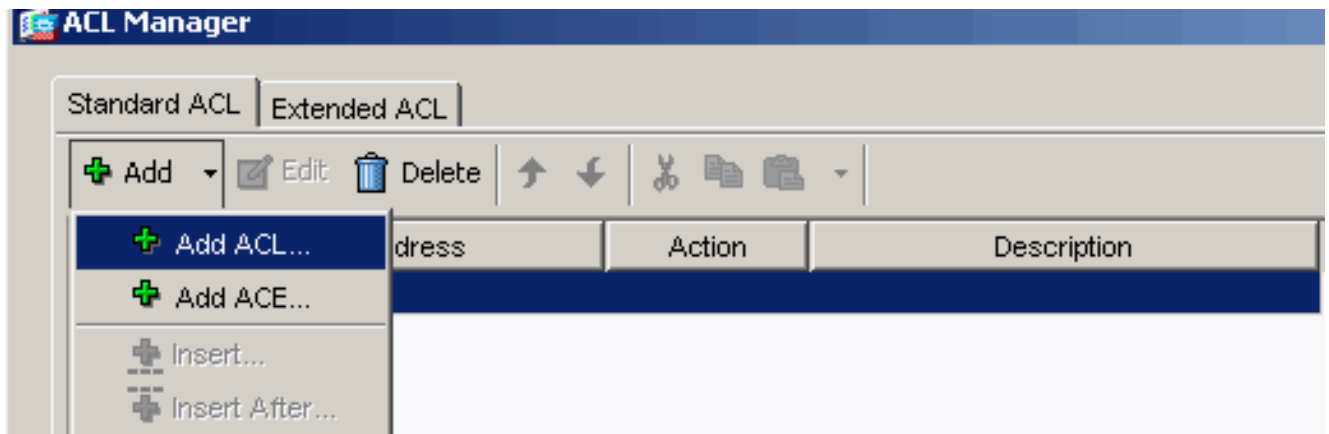
Dans l'onglet **Advanced > Split Tunneling**, décochez la case à cocher **Inherit** pour la stratégie de split tunneling et choisissez **Tunnel Network List Below** dans la liste déroulante.



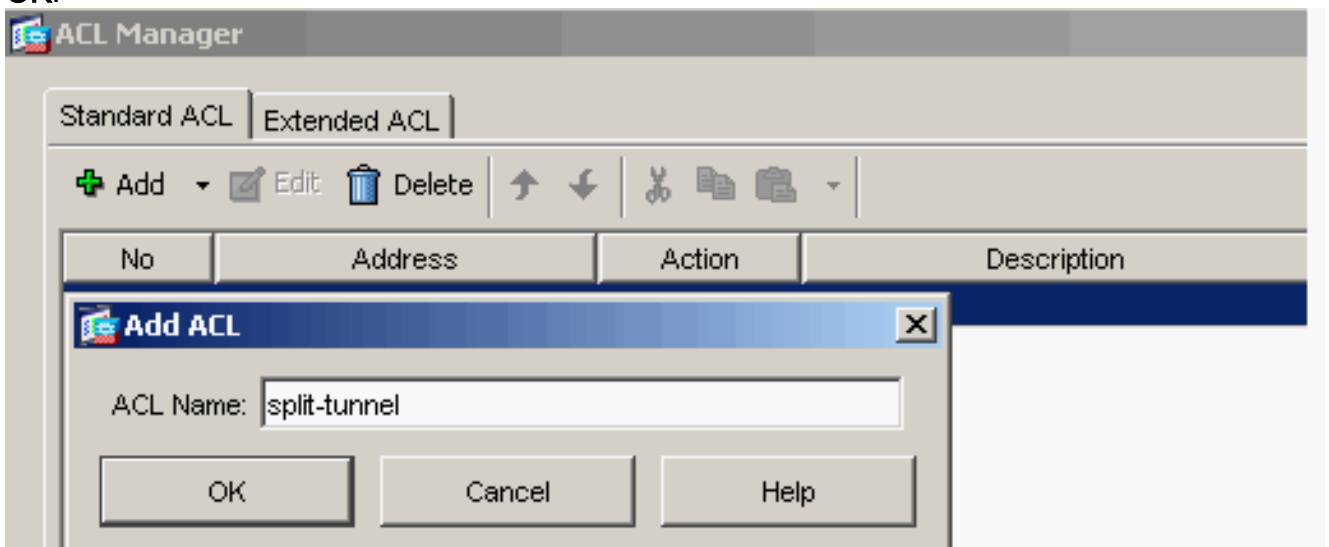
Décochez la case à cocher **Inherit** pour **Split Tunnel Network List** et cliquez ensuite sur **Manage** afin de lancer l'ACL Manager.



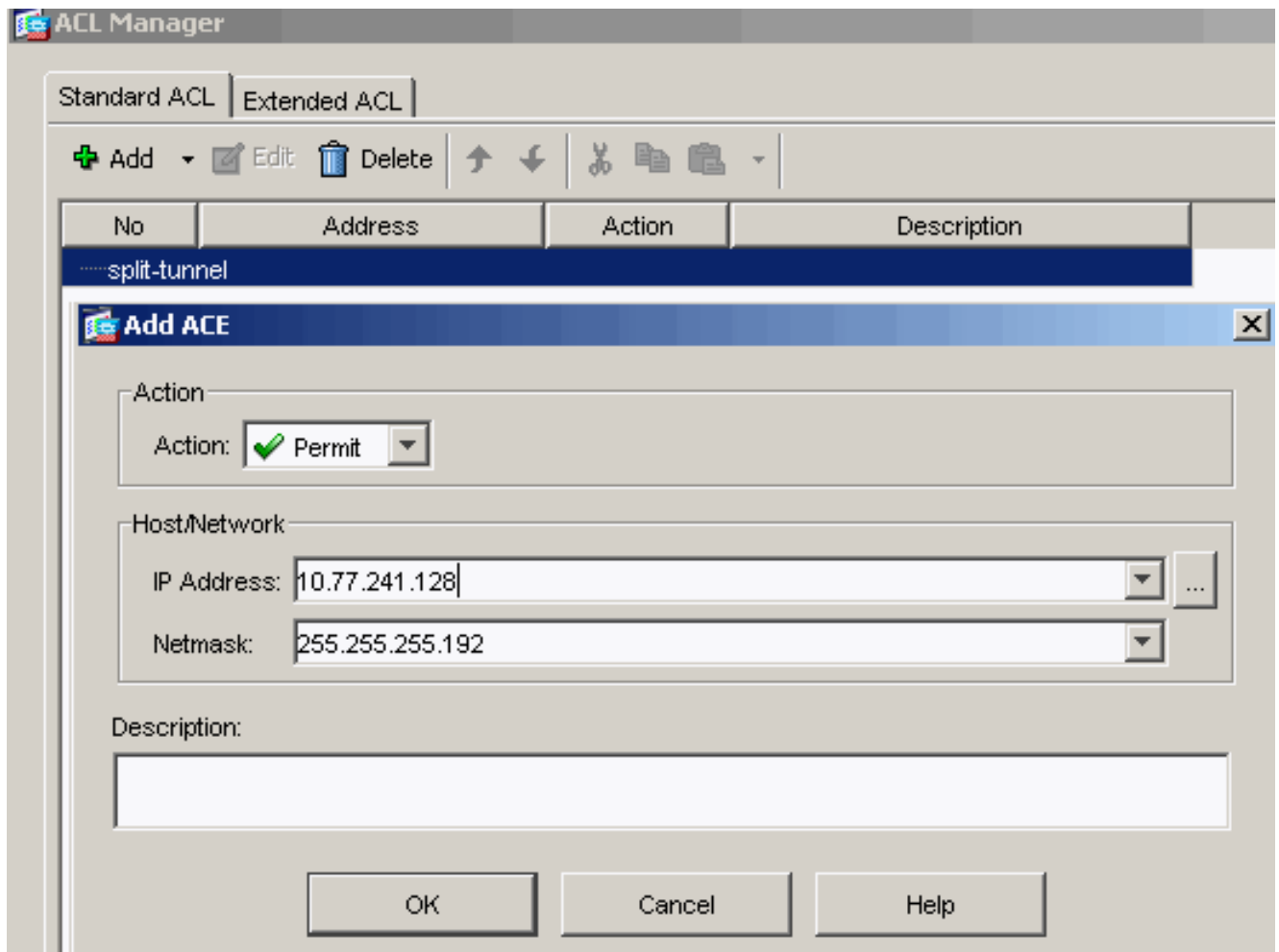
Dans le gestionnaire ACL, choisissez **Ajouter > Ajouter une ACL...** afin de créer une nouvelle liste d'accès.



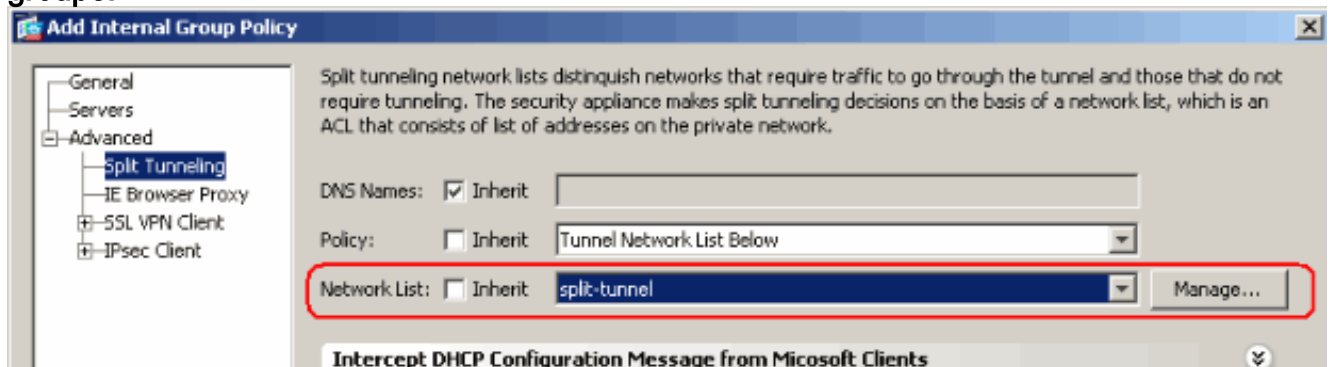
Fournissez un nom pour l'ACL et cliquez sur OK.



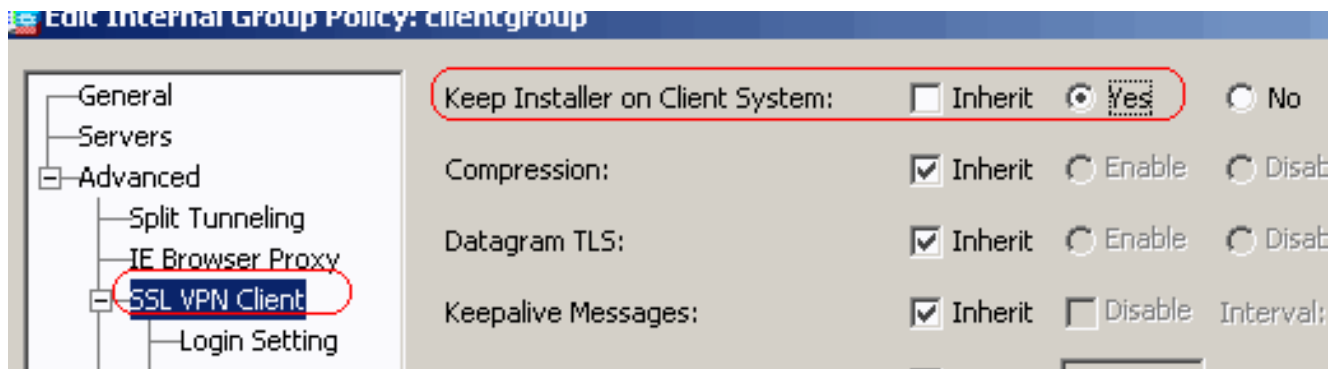
Une fois le nom de l'ACL créé, choisissez **Add > Add ACE** afin d'ajouter une entrée de **contrôle d'accès (ACE)**. Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est 10.77.241.128/26 et sélectionnez **Permit** comme action. Cliquez sur **OK** afin de quitter l'ACL Manager.



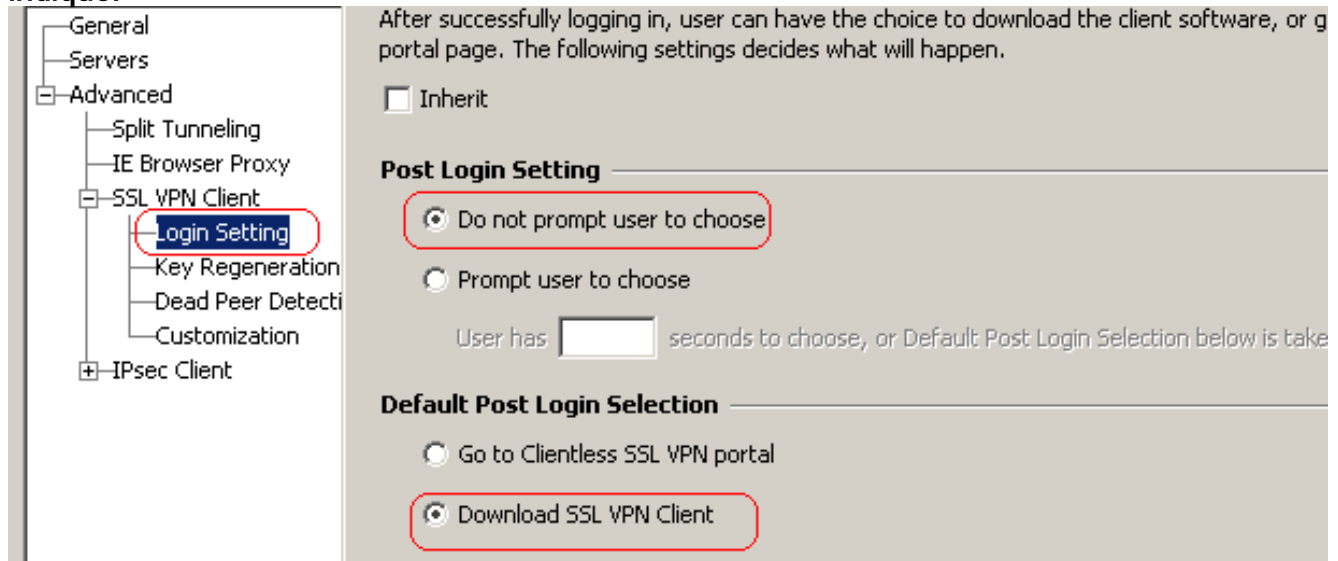
Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste de réseaux à split tunneling. Cliquez sur **OK** afin de retourner à la configuration de la stratégie de groupe.



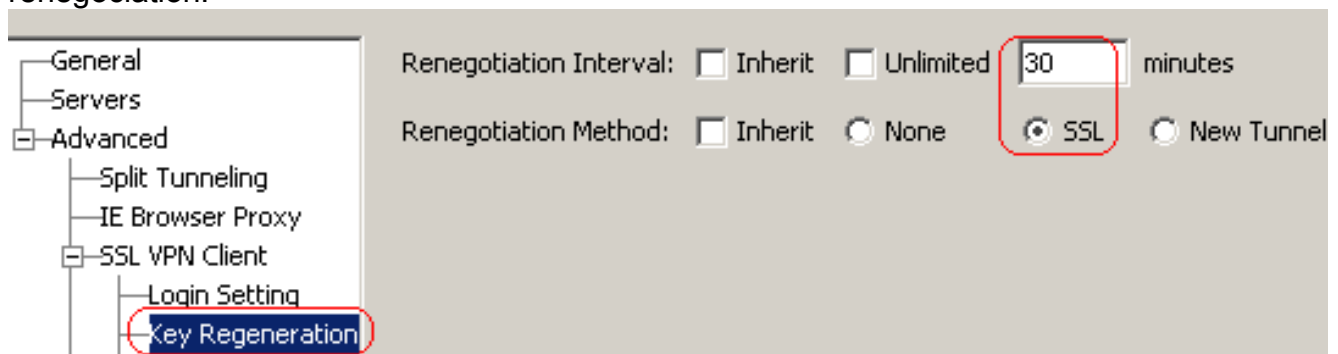
Sur la page principale, cliquez sur **Apply**, puis sur **Send** (s'il y a lieu) afin d'envoyer les commandes à l'ASA. Configurez les paramètres de VPN SSL en mode **Stratégie de groupe**. Pour l'option Keep Install on Client System, désélectionnez la case à cocher **Inherit**, puis cliquez sur le bouton radio **Yes**. Cette action permet au logiciel de SVC pour 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.



Cliquez sur **Login Setting** afin de paramétrer Post Login Setting et Default Post Login Selection comme indiqué.






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 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 sur la case d'option **SSL**. La renégociation peut utiliser le tunnel SSL actuel ou un nouveau tunnel créé expressément pour la renégociation.



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

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

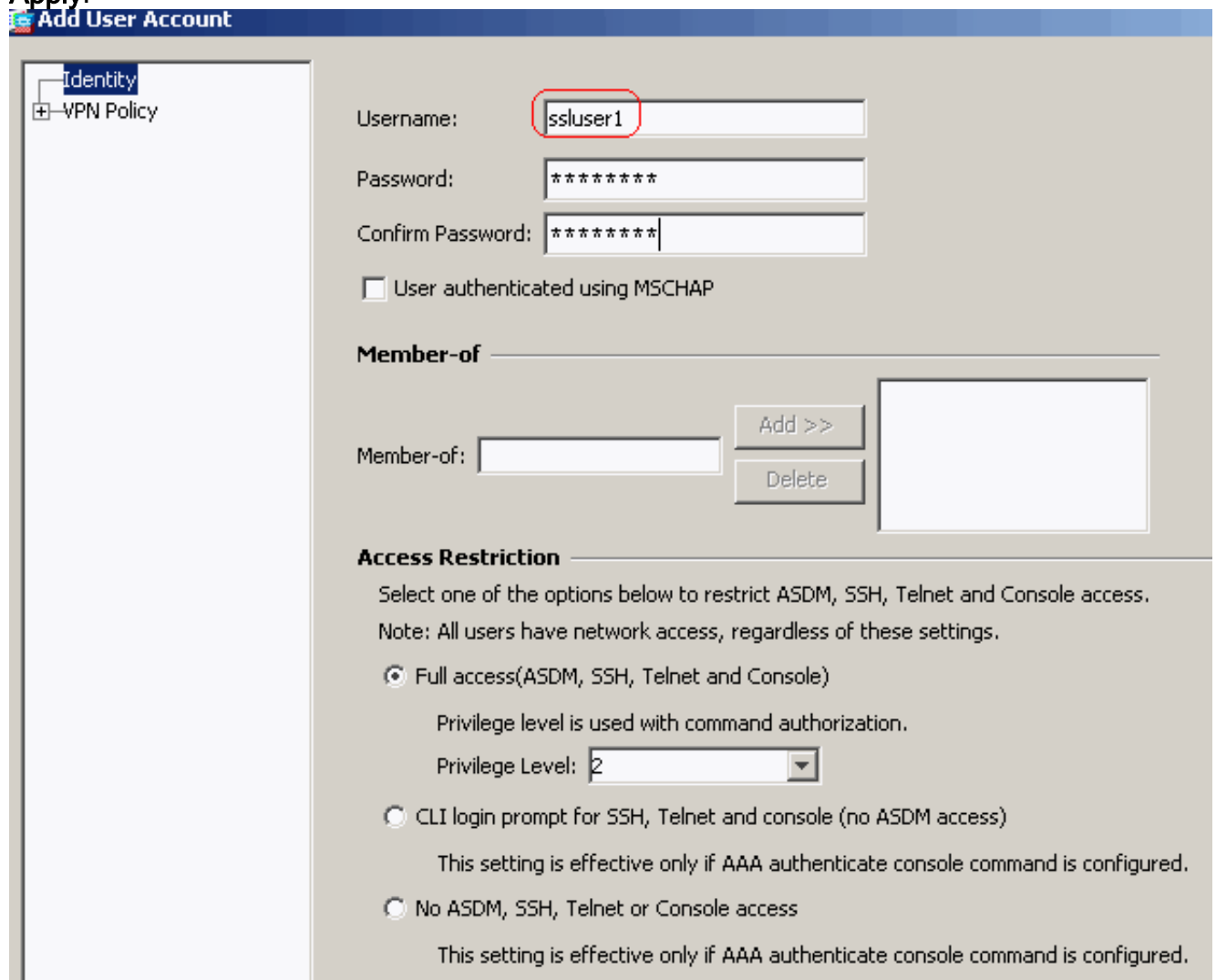
 Add  Edit  Delete

Name	Type	Tunneling Protocol	
clientgroup	Internal	svc	-- N/A -
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,IPSec,webvpn	-- N/A -

Configuration CLI équivalente :

5. Choisissez **Configuration > Remote Access VPN > AAA Setup > Local Users > Add** afin de créer un nouveau compte utilisateur **ssluser1**. Cliquez sur **OK**, puis sur

Apply.



Add User Account

Identity

- VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

Member-of

Member-of:

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

Configuration CLI équivalente :

6. Choisissez **Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit** afin de modifier le groupe de serveurs par défaut LOCAL en cochant la case à cocher **Enable Local User Lockout** avec comme valeur de tentatives maximale 16.

Configuration > Remote Access VPN > AAA Setup > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		

Edit LOCAL Server Group

This feature allows you to specify the maximum number of failed attempts to allow before locking out and denying access to the user. This limit is applicable only when the local database is used for authentication.

Enable Local User Lockout

Maximum Attempts:

OK

Cancel

Help

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

8. Configurez le groupe de tunnels. Choisissez Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles > Add afin de créer un nouveau groupe de tunnels sslgroup. Dans l'onglet Basic, vous pouvez exécuter la liste des configurations indiquée : Donnez au groupe de tunnels le nom sslgroup. Sous Client Address Assignment, choisir le pool d'adresses vpnpool dans la liste déroulante. Sous Default Group Policy, choisir la stratégie de groupe clientgroup dans la liste déroulante.

Add SSL VPN Connection Profile

Basic
Advanced

Name:

Aliases:

Authentication

Method: AAA Certificate Both

AAA Server Group:

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools:

Default Group Policy

Group Policy:

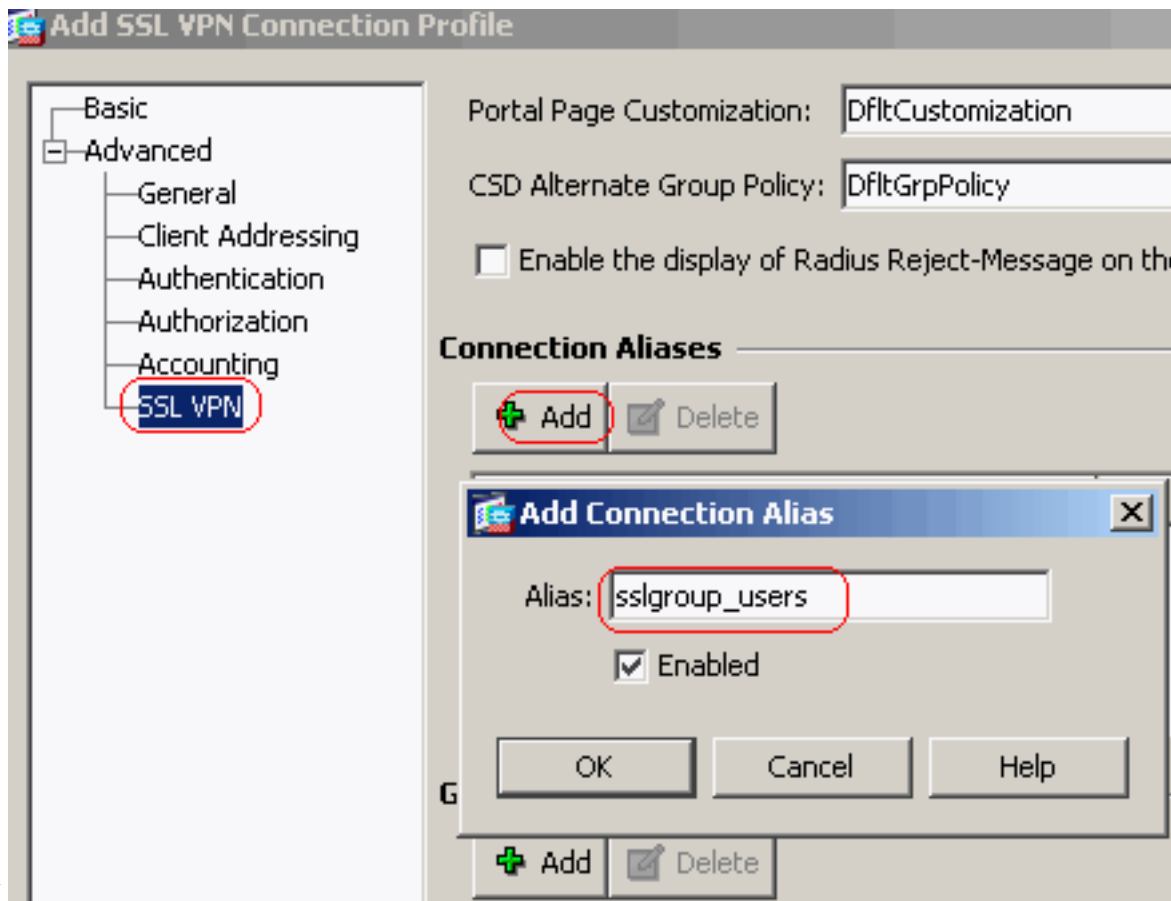
SSL VPN Client Protocol: Enabled

OK

Cancel

Help

Sous l'onglet SSL VPN > Connection Aliases, spécifiez sslgroup_users comme nom d'alias du groupe et cliquez sur

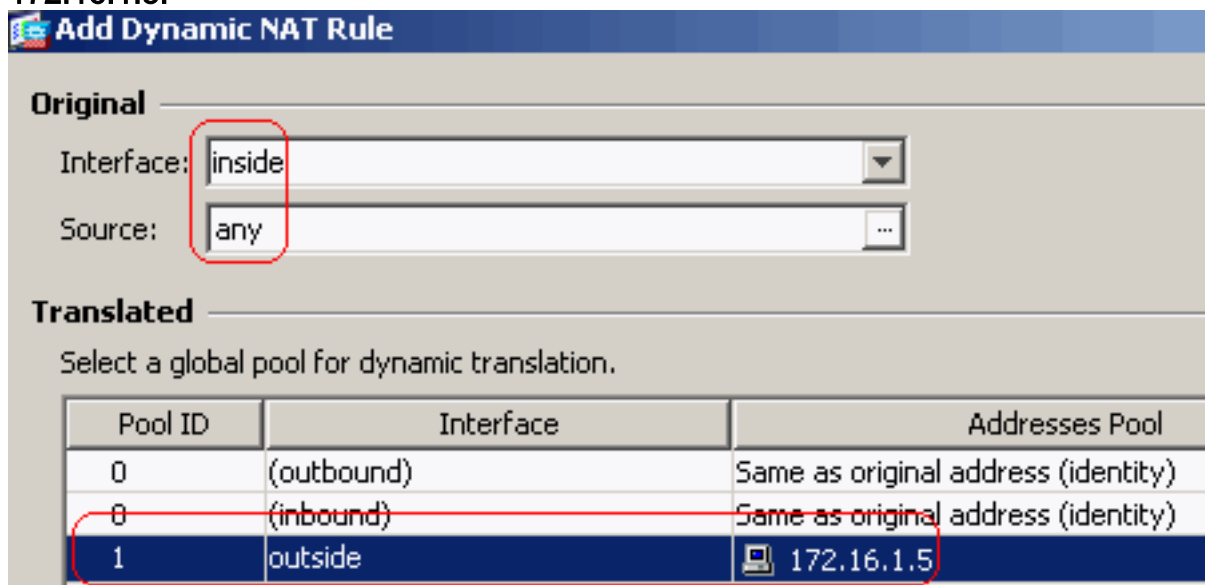


OK.

Clique

z sur OK, puis sur Apply. Configuration CLI équivalente :

- Configurez NAT. Choisissez Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule de façon à ce que le trafic venant de l'intérieur du réseau puisse être traduit avec l'adresse IP externe 172.16.1.5.



Click

OK. Click

OK.

Configuration > Firewall > NAT Rules						
#	Type	Original			Interface	
		Source	Destination	Service		
[-] inside (1 Dynamic rules)						
1	Dynamic	any			outside	

Cliquez sur Apply. Configuration CLI équivalente :

10. 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 de l'interface de ligne de commande ASA

Cisco ASA 8.0(2)

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name default.domain.invalid
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
boot system disk0:/asa802-k8.bin
```

```

ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
  domain-name default.domain.invalid
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 logging enable logging asdm informational
mtu inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN
Clients no failover icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-602.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

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 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
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
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios

```

```
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
webvpn
  enable outside

  !--- Enable WebVPN on the outside interface svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1

  !--- Assign an order to the AnyConnect SSL VPN Client
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 group-policy clientgroup internal

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

  !--- Specify SSL as a permitted VPN 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 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. svc ask none default svc

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

  !--- Create a user account "ssluser1" tunnel-group
sslgroup type remote-access

  !--- Create a tunnel group "sslgroup" with type as
remote access 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 prompt  
hostname context  
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end  
ciscoasa(config)#
```

Établir la connexion VPN SSL avec SVC

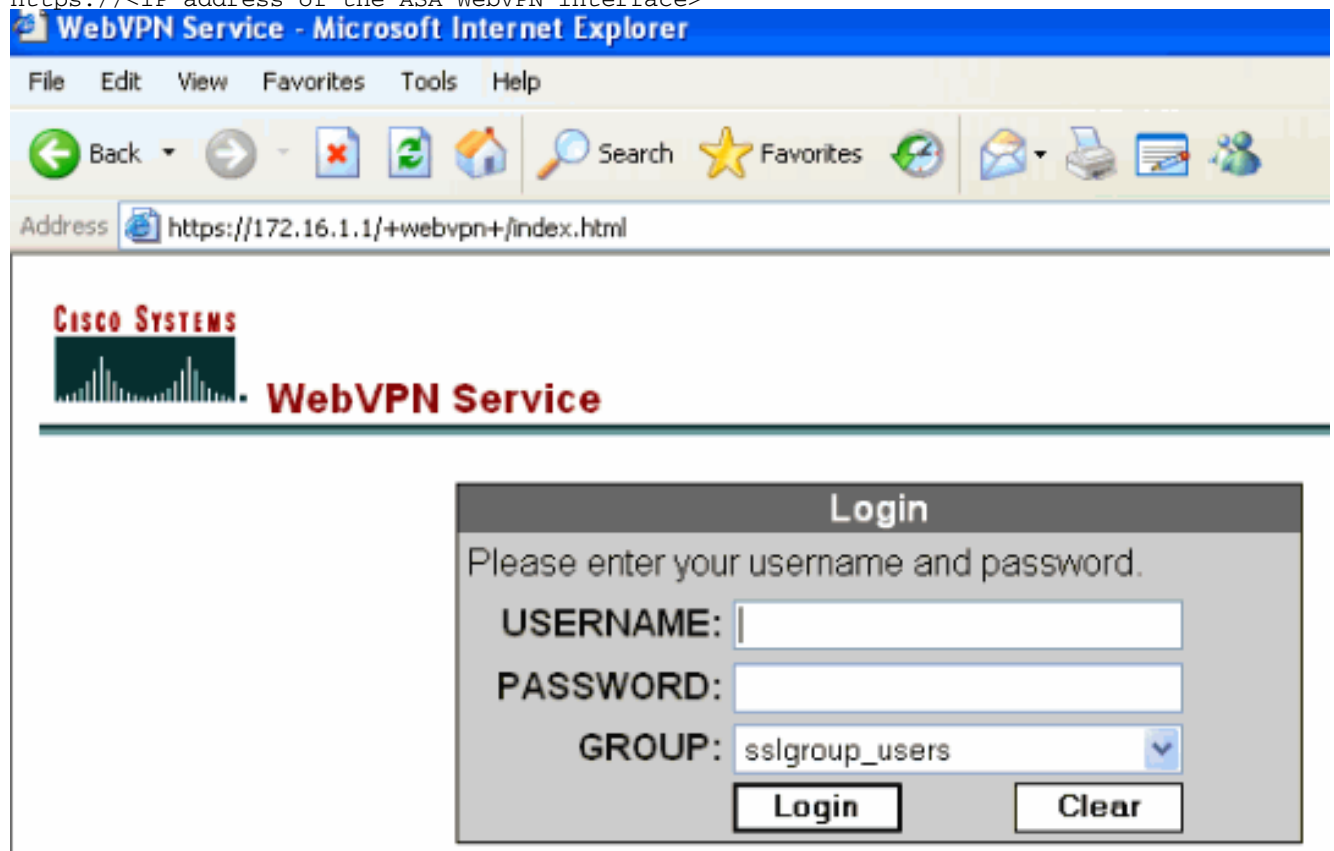
Exécutez ces étapes afin d'établir une connexion VPN SSL avec l'ASA :

1. Saisissez l'URL ou l'adresse IP de l'interface WebVPN de l'ASA dans votre navigateur Web avec le format indiqué.

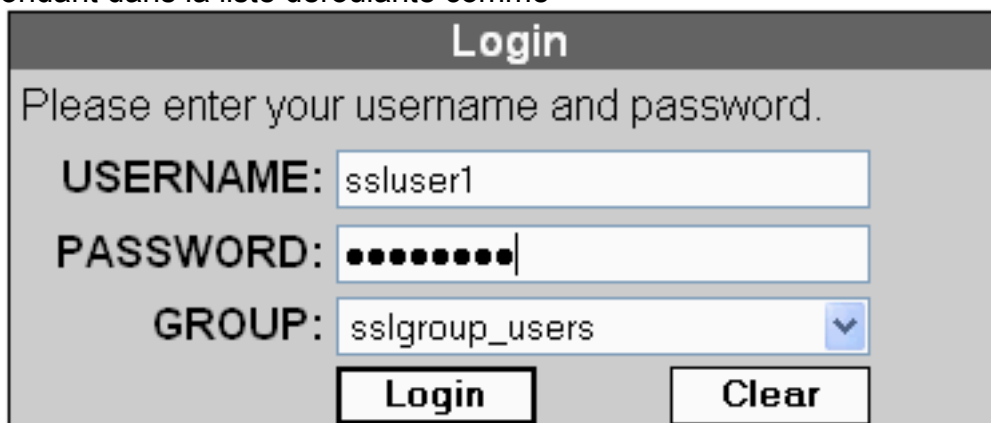
https://url

OU

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



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



indiqué.

apparaît avant que la connexion VPN SSL ne soit

Cette fenêtre

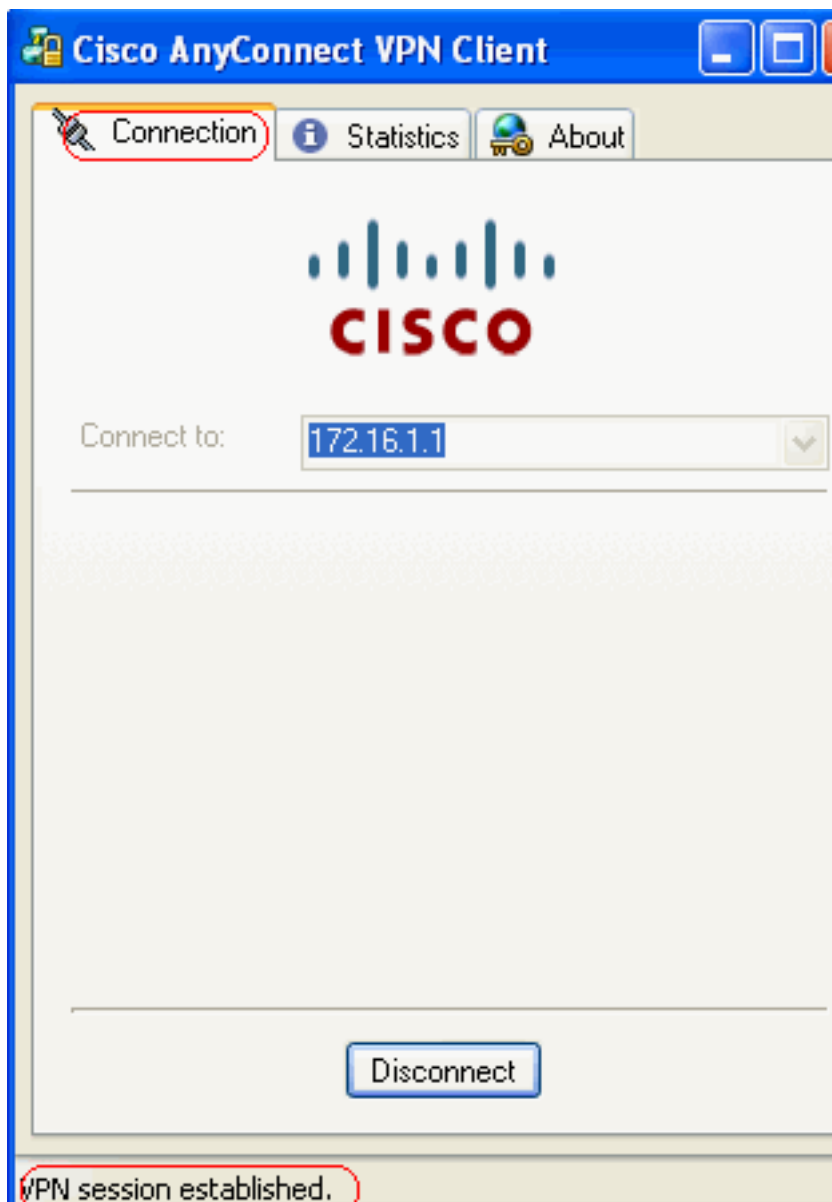
établie.



Remarque : le logiciel ActiveX doit être installé sur votre ordinateur avant de télécharger le SVC. Vous obtenez cette fenêtre une fois que la connexion est établie.

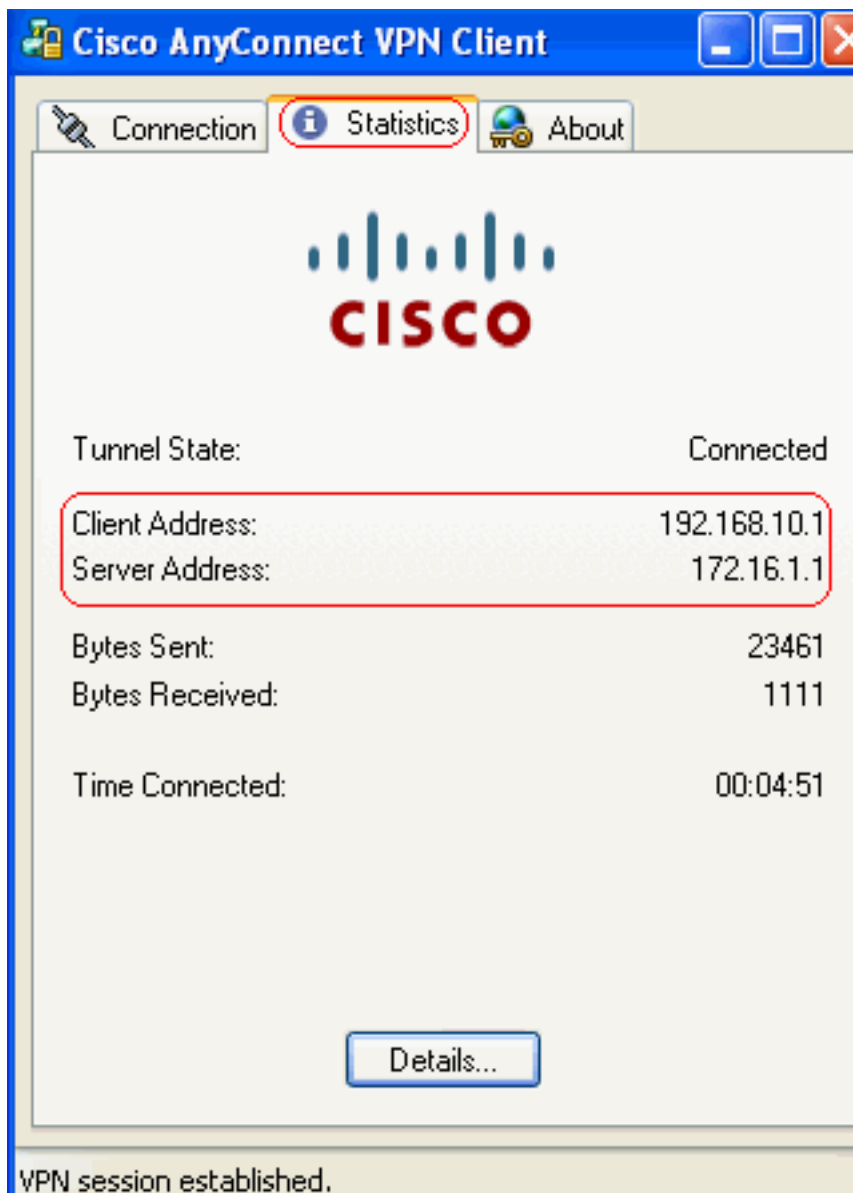


3. Cliquez sur le verrou qui apparaît dans la barre des tâches de votre



ordinateur. VPN session established.
et fournit des informations au sujet de la connexion SSL. Par exemple, 192.168.10.1 est l'adresse IP attribuée par l'ASA,

Cette fenêtre apparaît



etc. VPN session established.

informations sur la version de Cisco AnyConnect VPN

Cette fenêtre affiche les



Client: VPN session established

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:/anyconnect-win-2.0.0343-k9.pkg 1
   CISCO STC win2k+
   2,0,0343
   Mon 04/23/2007 4:16:34.63

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

: 12

```

Assigned IP   : 192.168.10.1           Public IP    : 192.168.1.1
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 194118                  Bytes Rx    : 197448
Group Policy : clientgroup             Tunnel Group : sslgroup
Login Time   : 17:12:23 IST Mon Mar 24 2008
Duration     : 0h:12m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                     VLAN        : none

```

- **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 la **Monitoring > VPN > VPN Statistics > Sessions** afin de connaître les sessions WebVPN actuelles dans l'ASA.

Remote Access	Site-to-Site	SSL VPN			E-mail Proxy	VPN Load Balancing
0	0	Clientless	With Client	Total	0	0
0	0	0	0	0	0	0

Username	IP Address	Group Policy Connection	Protocol Encryption	Login Time Duration	Bytes
ssluser1	192.168.10.1	clientgroup sslgroup	Clientless SSL-Tunnel DT... RC4 AES128	17:12:23 IST Mon Mar 24 2008 0h:03m:31s	194118 192474

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
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1

ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)

```

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

```

```
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xA000)
```

```
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.

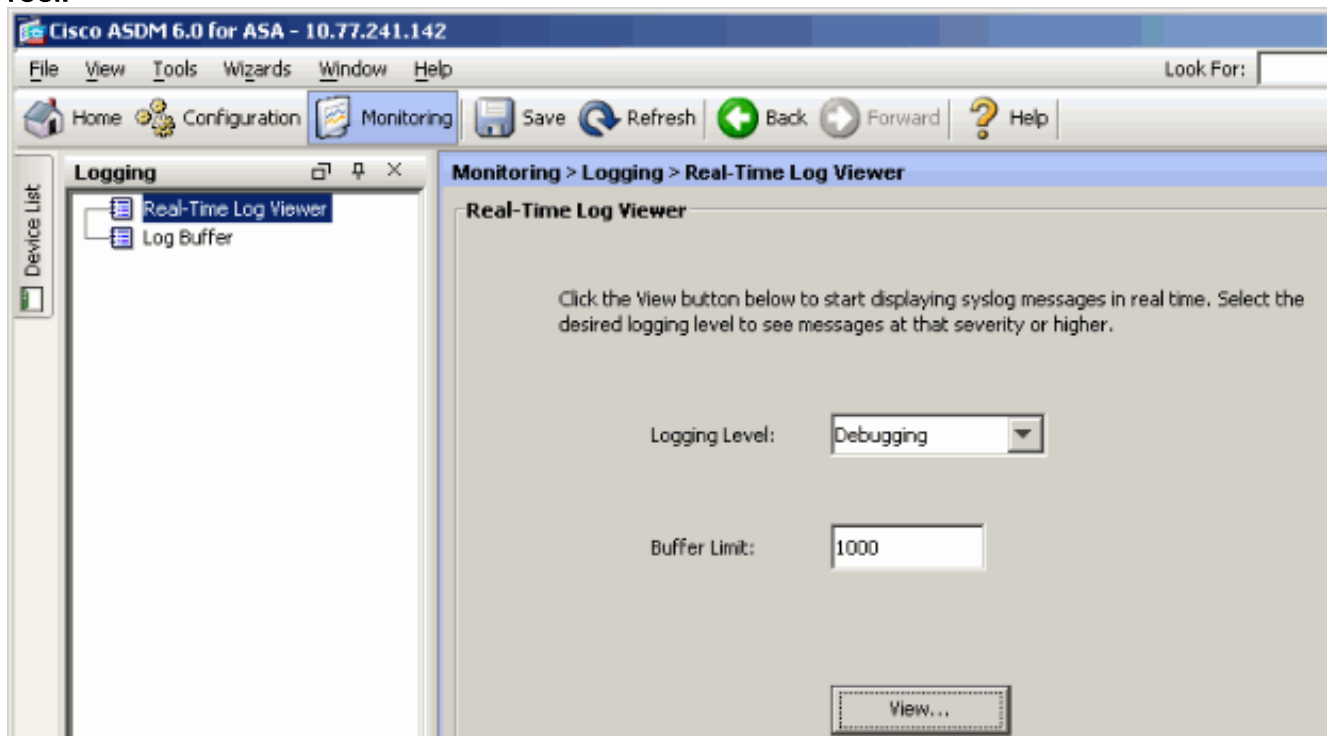
```
Ciscoasa#debug webvpn svc 7
```

```
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 AnyConnect VPN Client 2, 0, 0343'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
'
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26'
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: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
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
np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

4. Dans l'ASDM, choisissez **Monitoring > Logging > Real-time Log Viewer > View** afin de voir les événements en temps réel.



Cet exemple montre que la session SSL a été établie avec le périphérique de tête de réseau.

Real-Time Log Viewer - 10.77.241.142

File Tools Window Help

Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help

Filter By: Filter Show All Find:

Severity	Date	Time	Syslog ID	Source IP	Destination IP	
6	Mar 21 2008	20:03:36	725007	10.77.233.74		SSL session with client inside:10.77.233.74/1026 terminated.
6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44:
6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identit
6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enabl
6	Mar 21 2008	20:03:35	725002	10.77.233.74		Device completed SSL handshake with client inside:10.77.233.74/1026
6	Mar 21 2008	20:03:35	725003	10.77.233.74		SSL client inside:10.77.233.74/1026 request to resume previous session.
6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside:10.77.233.74/1026 for TL5v1 se
6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23

%ASA-6-725002: Device completed SSL handshake with remote_device_interface_name:IP_address/port

The SSL handshake has completed successfully with the remote device.

Informations connexes

- [Page de support pour appliances de sécurité adaptables de la gamme Cisco 5500](#)
- [Notes de publication relatives au client VPN d'AnyConnect, Version 2.0](#)
- [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](#)