ASA 7.1/7.2: Split-tunneling voor SVC toestaan op het ASA Configuration-voorbeeld

Inhoud

Inleiding

Dit document bevat stap-voor-stap instructies over hoe u Secure Socket Layer (SSL) VPN-clients (SVC) toegang tot het internet kunt verlenen terwijl ze in een Cisco adaptieve security applicatie (ASA) zijn getunneld. Deze configuratie maakt SVC een veilige toegang tot bedrijfsmiddelen via SSL mogelijk en geeft onbeveiligde toegang tot het internet door het gebruik van gesplitste tunneling.

De mogelijkheid om zowel beveiligd als onbeveiligd verkeer op dezelfde interface te verzenden is bekend als gesplitste tunneling. Split-tunneling vereist dat u precies specificeert welk verkeer beveiligd is en wat de bestemming van dat verkeer is, zodat alleen het gespecificeerde verkeer de tunnel ingaat, terwijl de rest niet gecodeerd wordt door het openbare netwerk (Internet).

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Lokale beheerrechten op alle externe werkstations
- Java en ActiveX controleren het externe werkstation
- Port 443 (SSL) is nergens langs het verbindingspad geblokkeerd

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5500 Series adaptieve security applicatie (ASA) met softwareversie 7.2(2)
- Cisco SSL VPN-clientversie voor Windows 1.1.4.17.9**Opmerking:** Download het SSL VPN-clientpakket (slclient-win*.pkg) van de Cisco Software Download (alleen geregistreerde klanten). Kopieer de SVC naar het flash-geheugen van de ASA, dat gedownload moet worden naar de externe gebruikerscomputers om de SSL VPN-verbinding met ASA op te zetten. Raadpleeg het gedeelte SVC-software installeren van de ASA-configuratiegids voor meer informatie.
- PC die Windows 2000 Professional SP4 of Windows XP SP2 uitvoert
- Cisco Adaptieve Security Devices Manager (ASDM) versie 5.2(2)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

De SSL VPN Client (SVC) is een VPN-tunneling-technologie die externe gebruikers de voordelen van een IPsec VPN-client biedt zonder dat netwerkbeheerders IPsec VPN-clients op externe computers moeten installeren en configureren. SVC gebruikt de SSL-encryptie die reeds op de externe computer aanwezig is, evenals de inlognaam en verificatie van WebeVPN van het security apparaat.

Om een SVC-sessie te kunnen opzetten, gaat de externe gebruiker het IP-adres in van een WebVPN-interface van het security apparaat in de browser, en de browser sluit zich aan op die interface en geeft het inlogscherm van WebVPN weer. Als u voldoet aan de inlognaam en de verificatie en het beveiligingsapparaat u identificeert dat u de SVC nodig hebt, wordt de SVC op de externe computer gedownloads. Als het beveiligingsapparaat u identificeert met de optie om de SVC te gebruiken, wordt de SVC-installatie door het beveiligingsapparaat gedownload naar de externe computer terwijl er een link in het venster verschijnt om de SVC-installatie te overslaan.

Nadat u het downloaden, installeert en vormt SVC zichzelf, en dan blijft of oninstalleert de SVC, wat van de configuratie afhangt, van de afstandscomputer wanneer de verbinding wordt beëindigd.

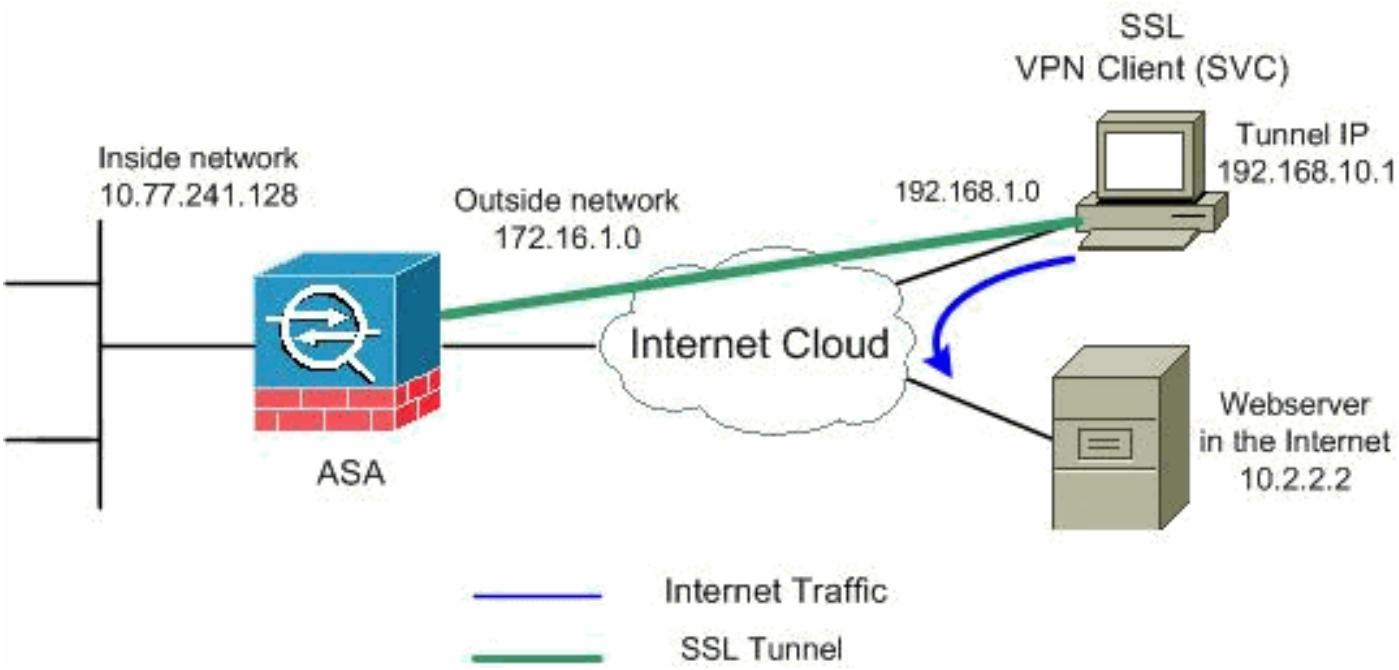
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

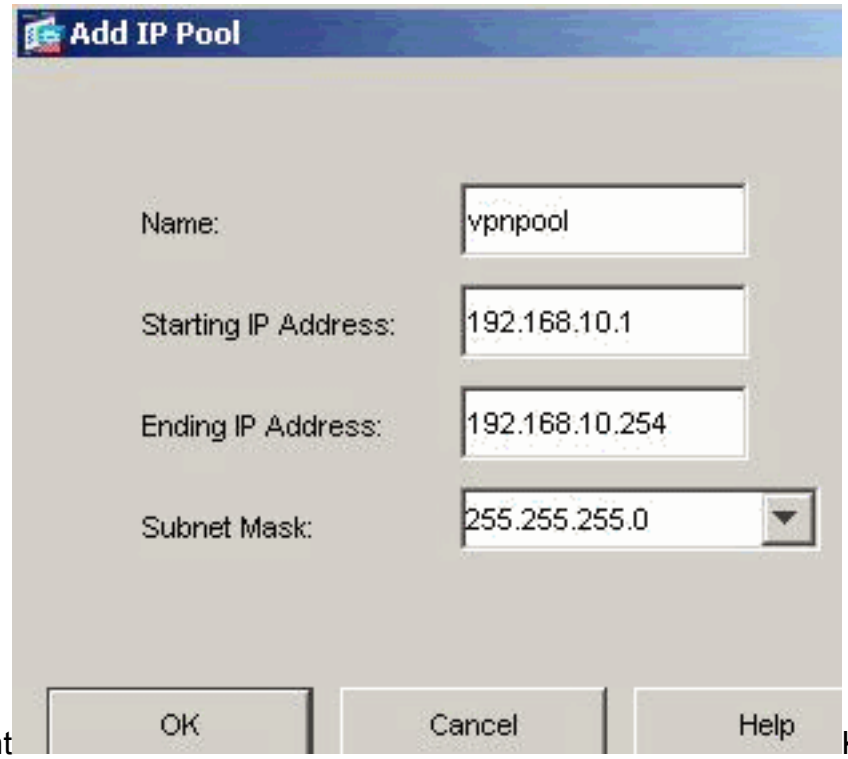


Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

ASA-configuraties met ASDM 5.2(2)

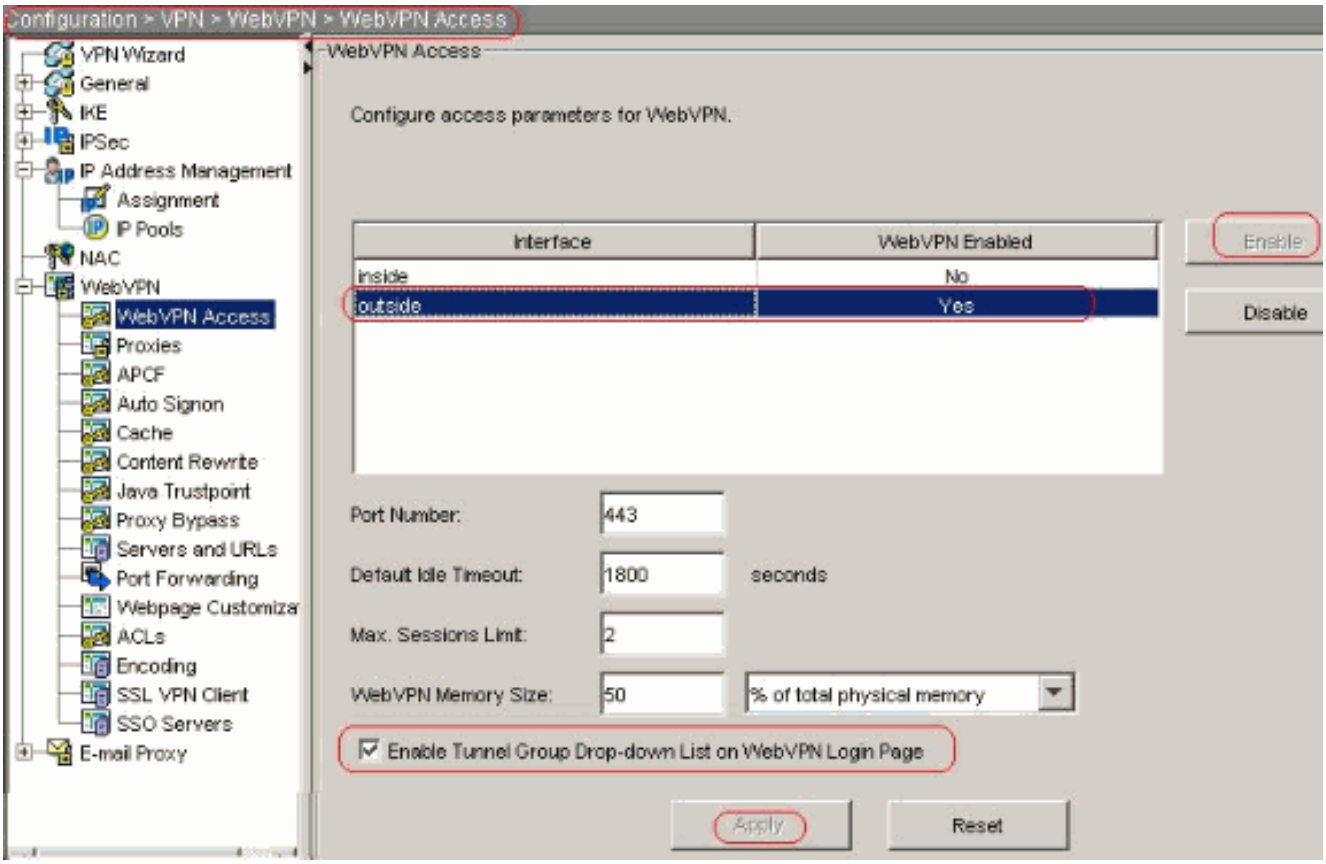
Voltooi deze stappen om SSL VPN op ASA met Split Tunneling zoals aangegeven te configureren:

1. Het document gaat uit van de basisconfiguratie, zoals de configuratie van de interface, enzovoort, die al gemaakt is en naar behoren werkt.**Opmerking:** Raadpleeg HTTPS-toegang voor ASDM om de ASA te kunnen configureren door de ASDM.**Opmerking:** WebVPN en ASDM kunnen niet op dezelfde ASA-interface worden ingeschakeld tenzij u de poortnummers wijzigt. Raadpleeg ASDM en WebVPN ingeschakeld op dezelfde interface van ASA voor meer informatie.
2. Kies **Configuration > VPN > IP-adresbeheer > IP-pools** om een IP-adrespool te maken: **VPN-**

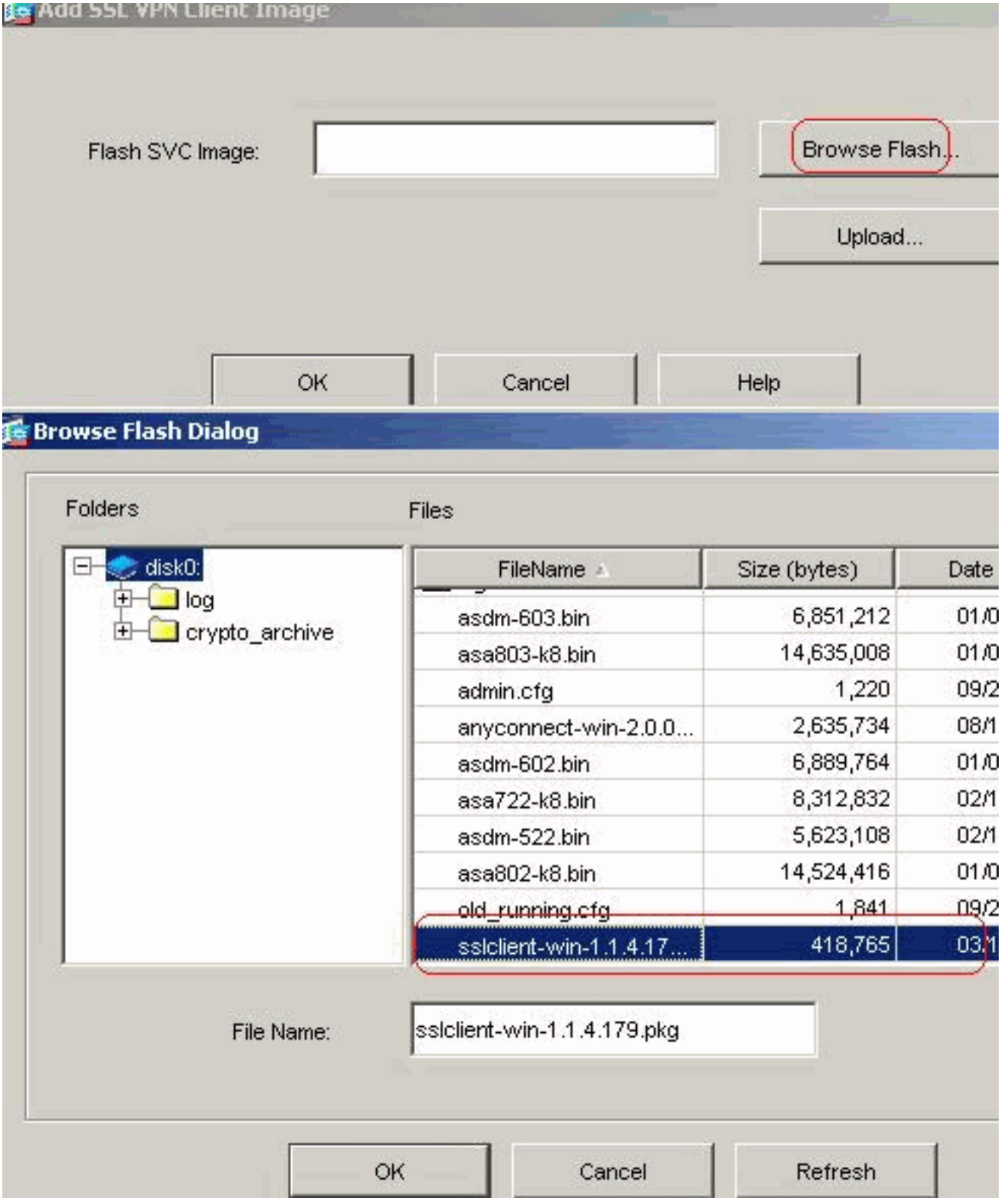


client Klik op **Apply** (Toepassen).

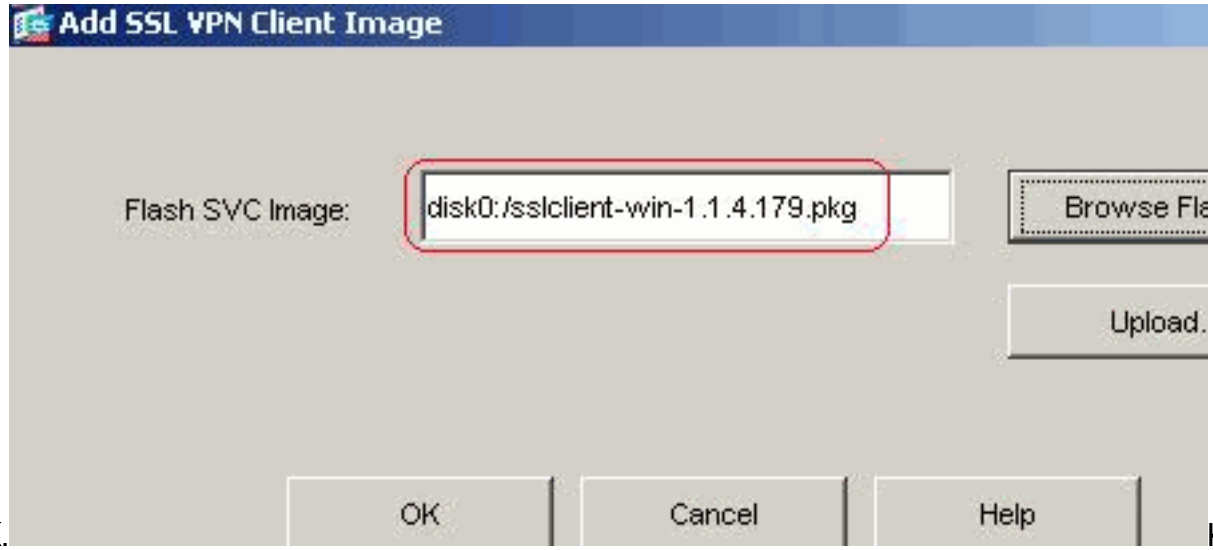
3. **WebVPN inschakelen**Kies **Configuration > VPN > WebeVPN > WebeVPN Access** en licht de externe interface met muis toe en klik op **Enable**. Selecteer **de vervolgkeuzelijst Tunnel groep inschakelen in het** dialoogvenster **Pagina voor vastlegging van WebVPN** om de uitrollijst in de inlogpagina voor gebruikers in staat te stellen hun respectievelijke groepen te kiezen.



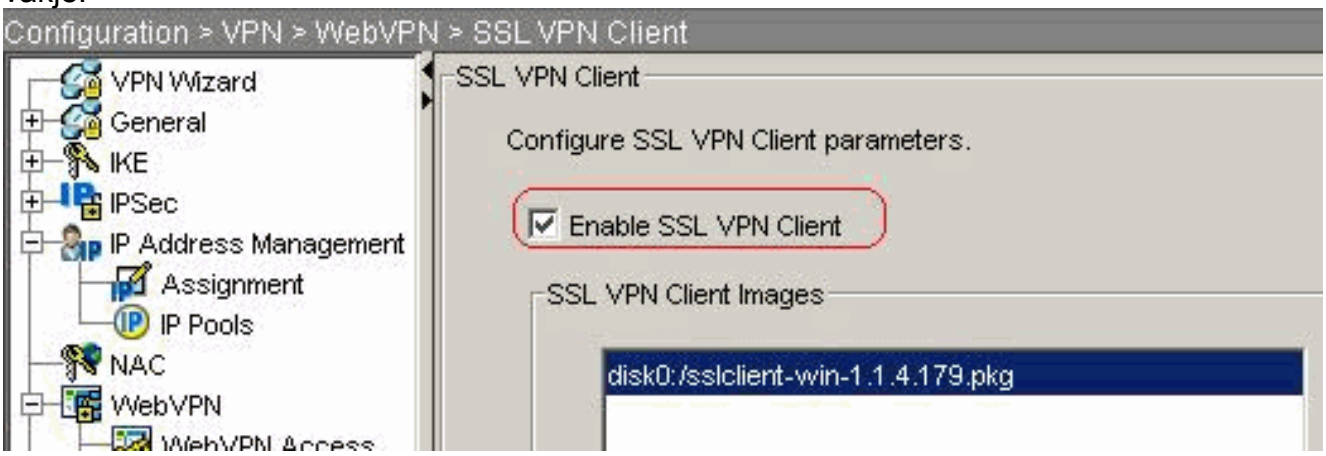
Klik op **Apply** (Toepassen).Kies **Configuratie > VPN > WebVPN > SSL VPN-client > Add** om het SSL VPN-clientbeeld uit het flash-geheugen van ASA zoals weergegeven toe te voegen.


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

Klik op

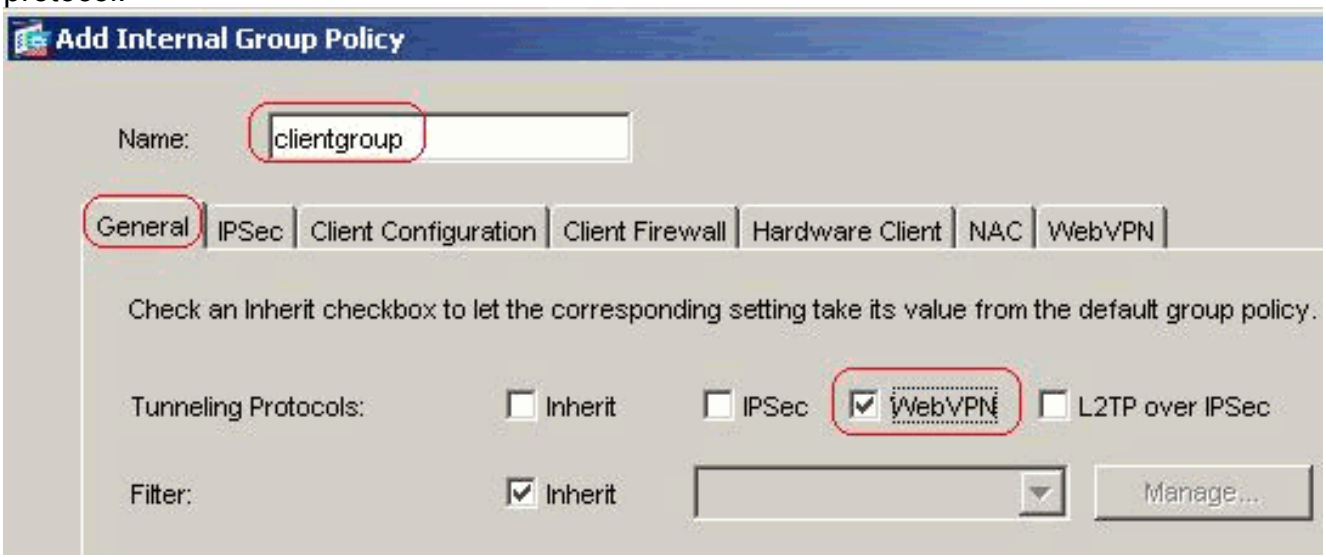


OK.Klik op **OK**.Klik op **SSL VPN-client** vakje.



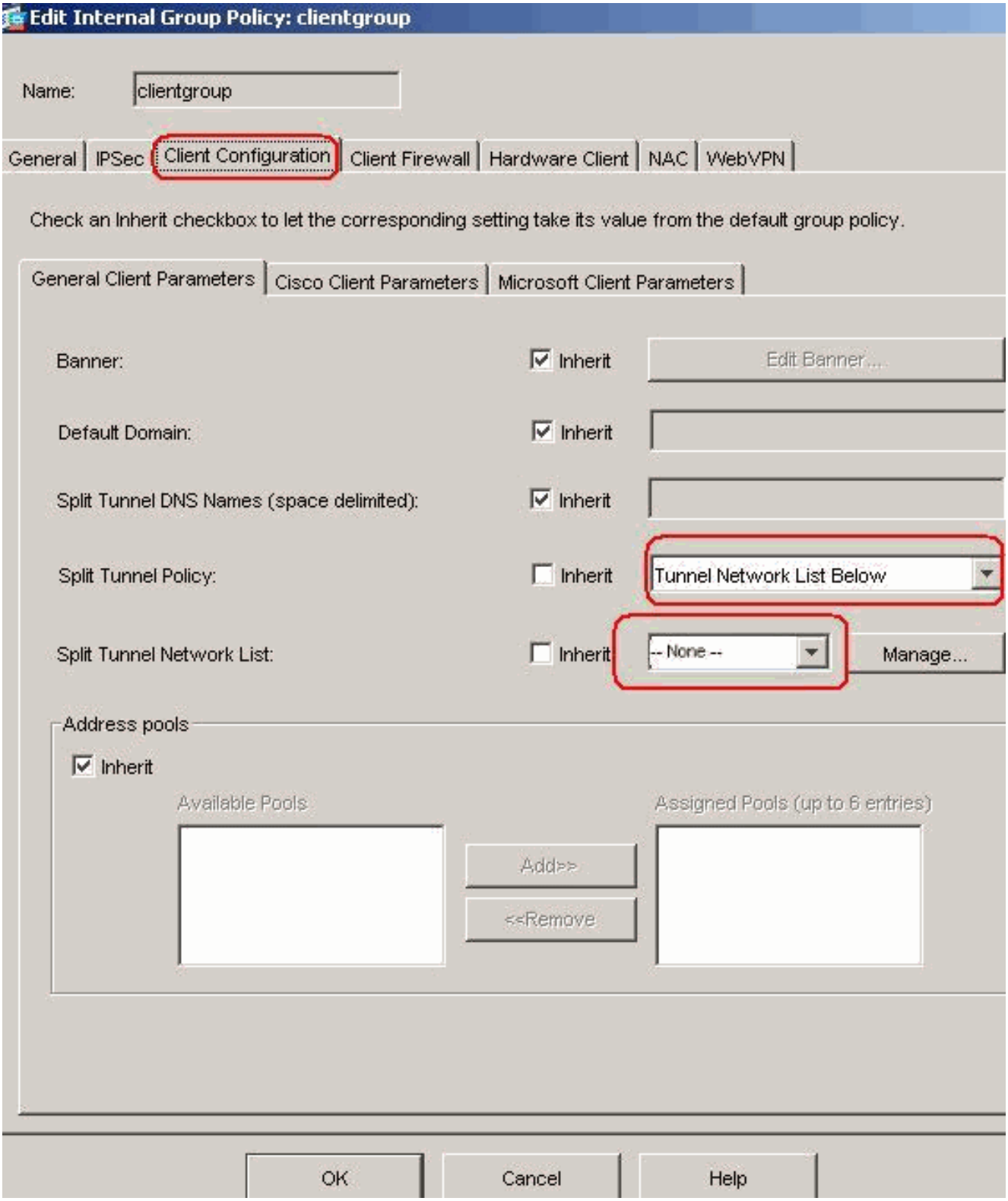
Klik op **Apply** (Toepassen).**Compatibele CLI-configuratie:**

4. **Groepsbeleid configurerenKies Configuratie > VPN > Algemeen > Groepsbeleid > Toevoegen (Intern Groepsbeleid)** om een interne **clientgroep** voor groepsbeleid te creëren. Selecteer onder **General** het aankruisvakje **WebVPN** om WebVPN in te schakelen als een tunneling-protocol.

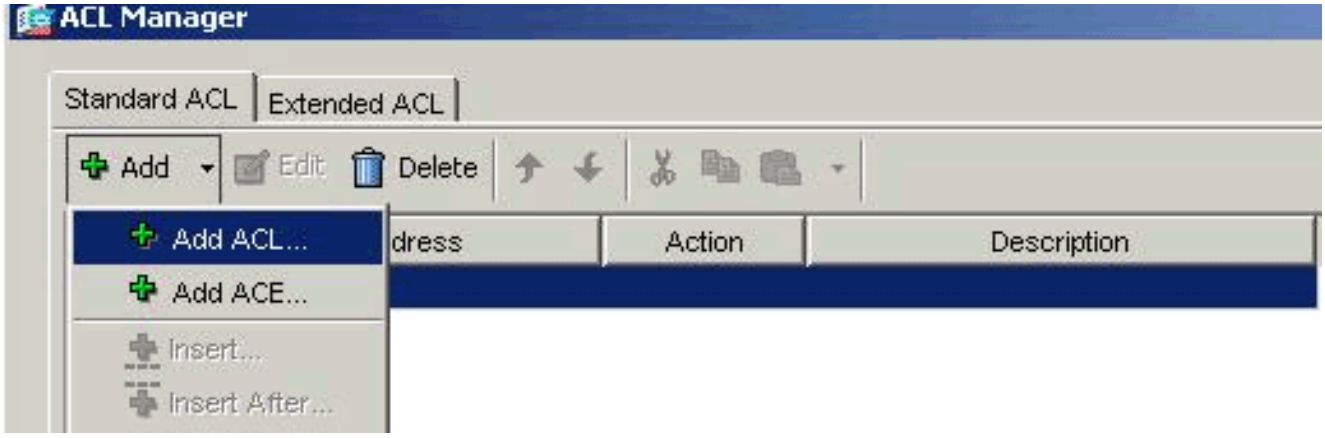


In het tabblad **Clientconfiguratie > Algemene clientparameters**, schakelt u het vakje **Inherit** uit voor Split-tunnelbeleid en kiest u **de onderstaande** lijst met **tunnelnetwerkbestanden** in de vervolgkeuzelijst.Schakel het vakje **Inherit** uit voor de **netwerklijst van splitter** en klik

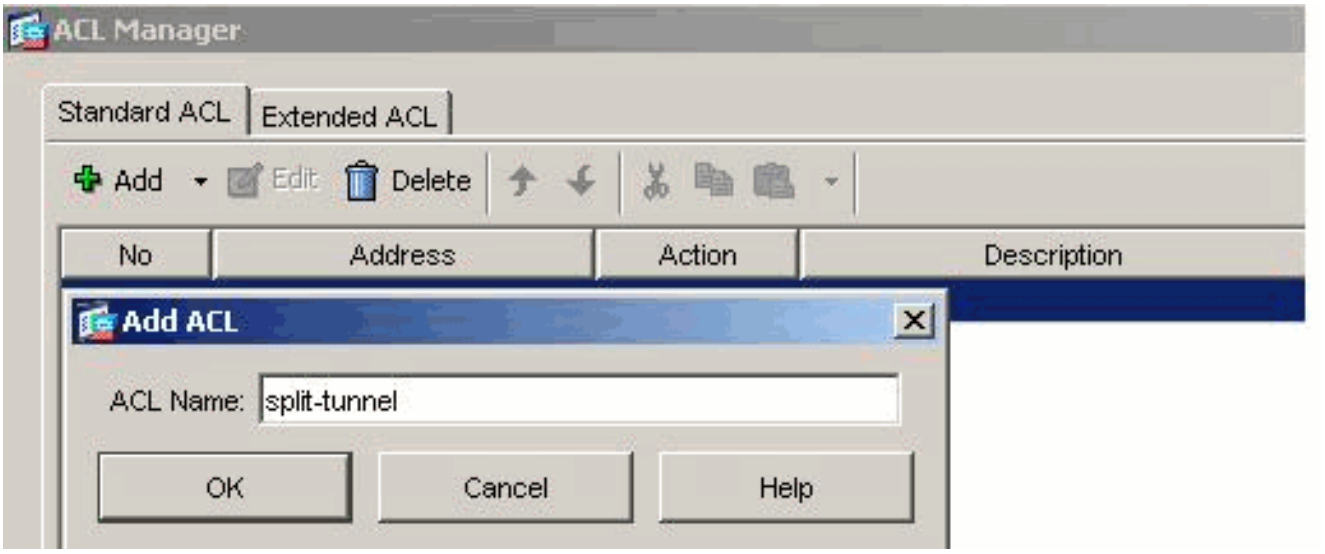
vervolgens op **Bewerken** om de ACL-Manager te starten.



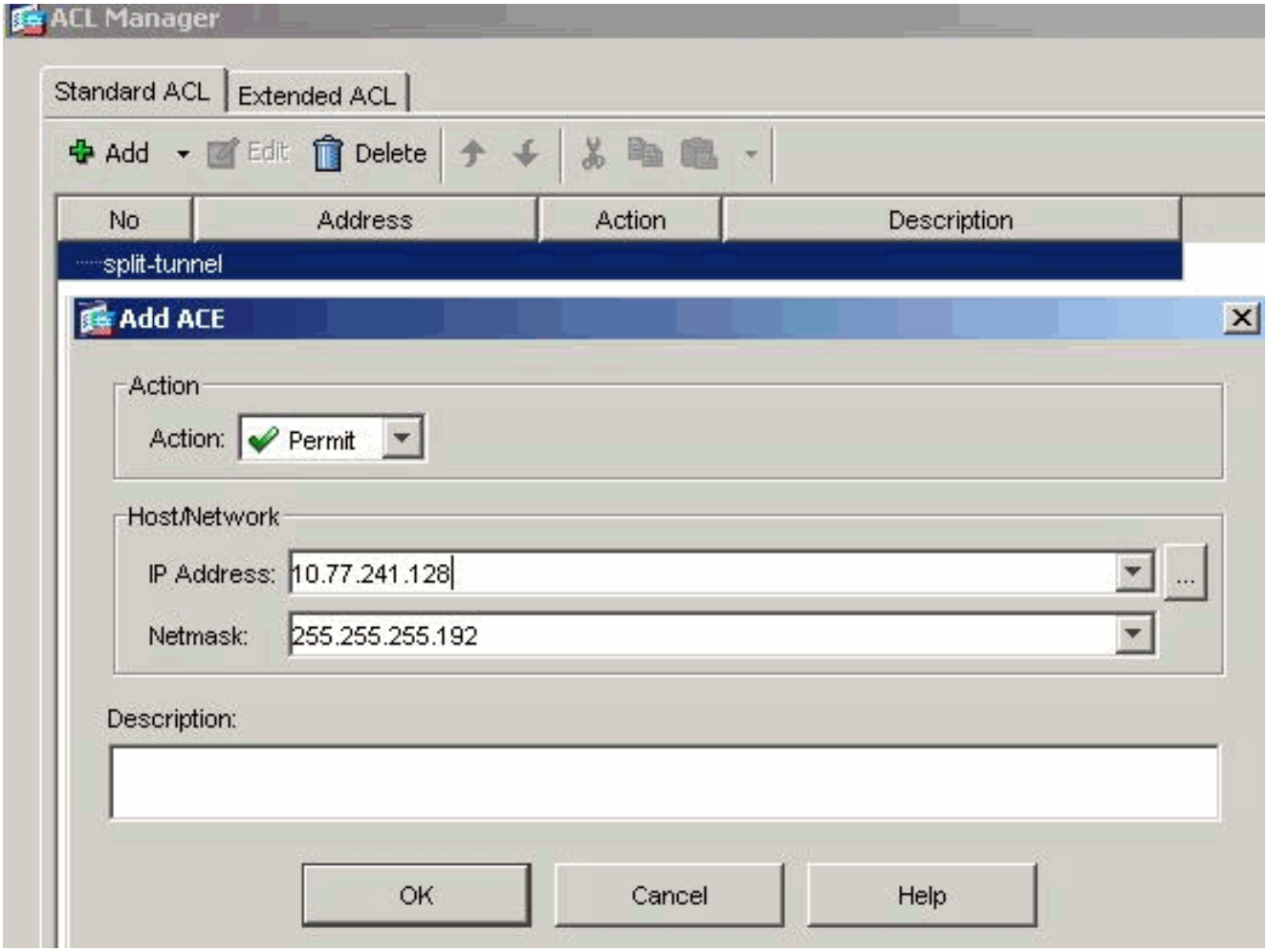
Kies in de ACL Manager **Add > Add ACL...** om een nieuwe toegangslijst te maken.



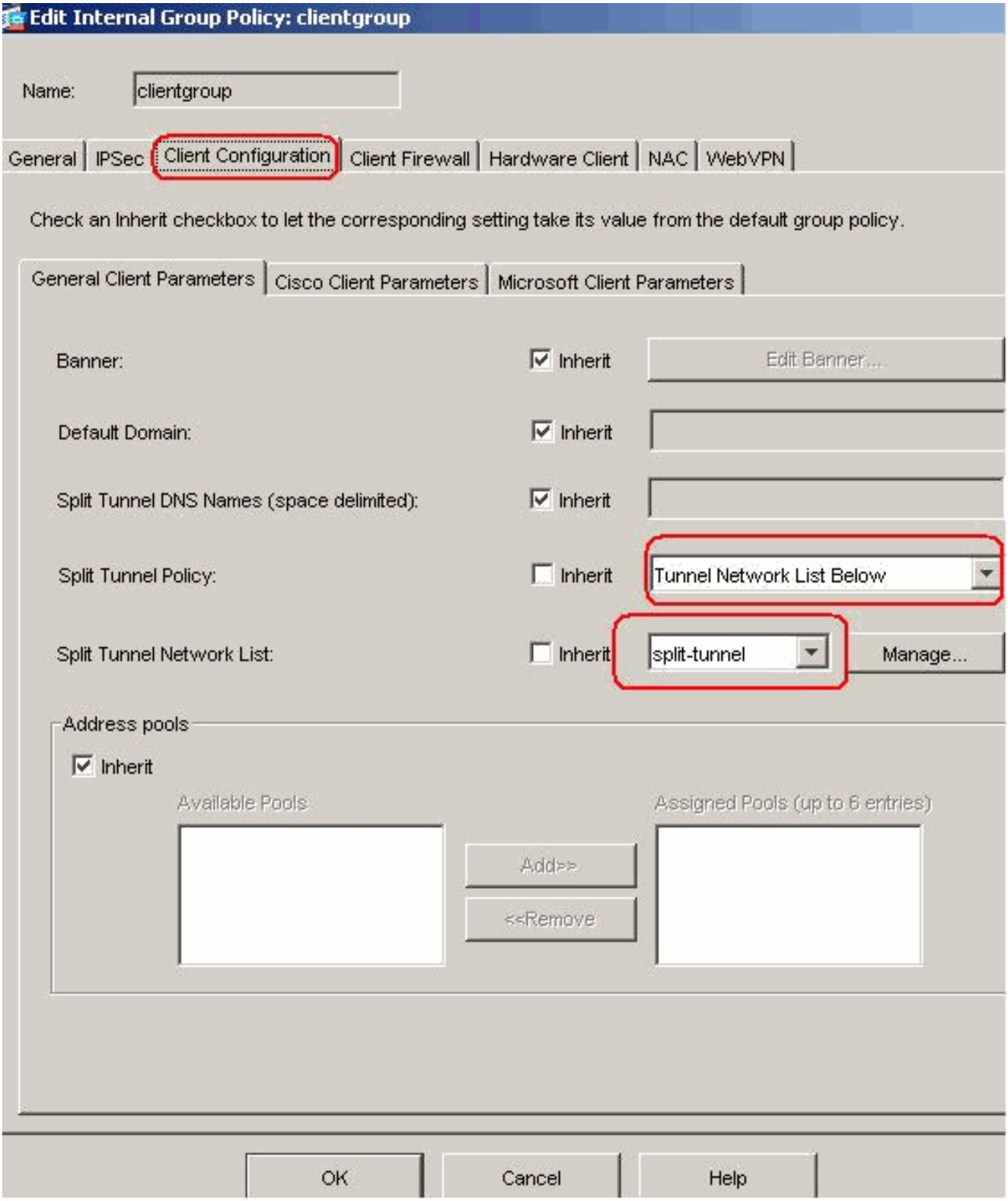
Typ een naam voor ACL en klik op **OK**.



Zodra de ACL-naam is gemaakt, kiest u **Add > Add ACE** om een Access Control Entry (ACE) toe te voegen.Defineer de ACE die overeenkomt met het LAN achter de ASA. In dit geval is het netwerk 10.77.241.128/26 en kiest u **Vergunning**.Klik op **OK** om de ACL-Manager te verlaten.

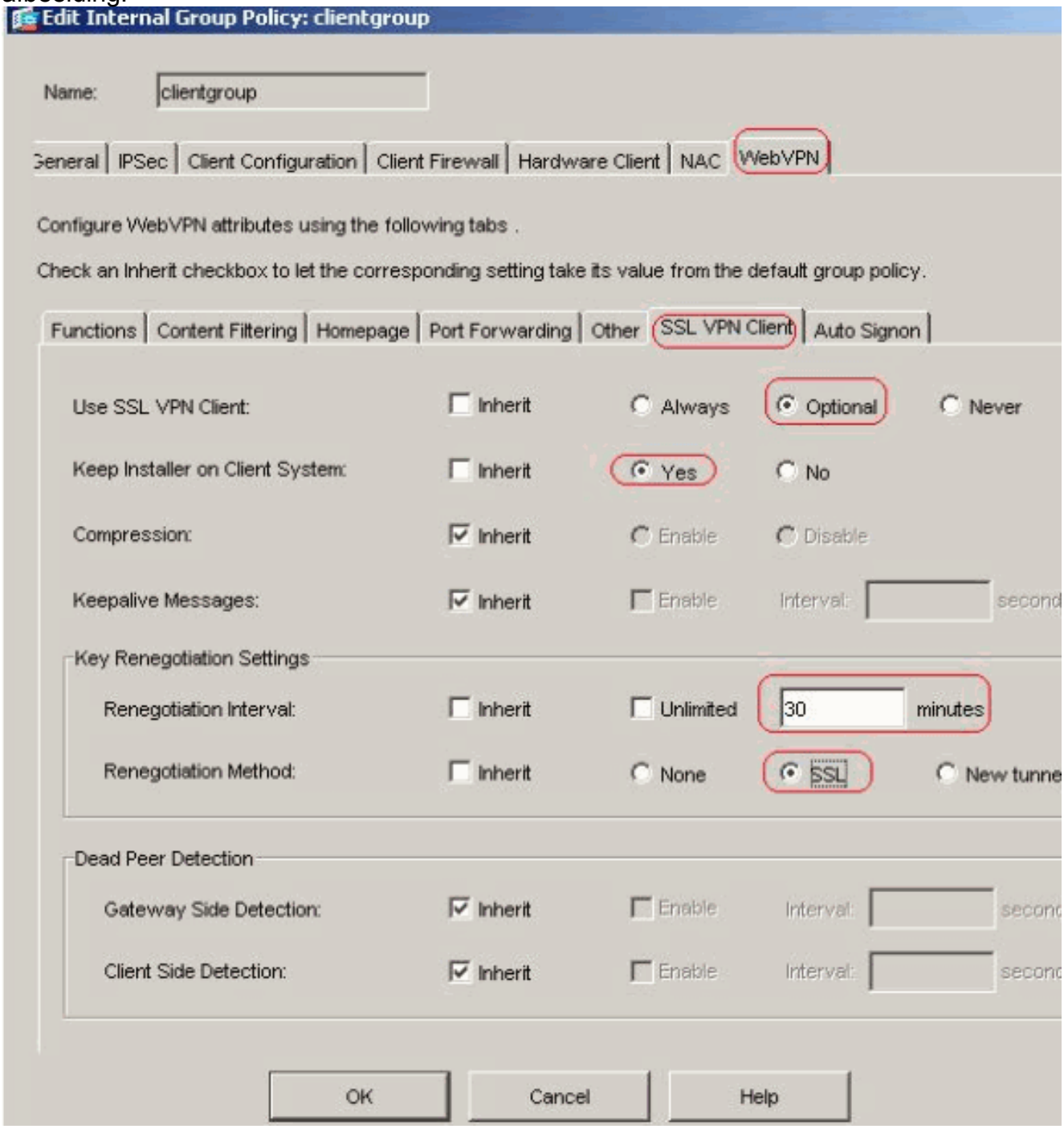


Verzeker u dat ACL die u zojuist hebt gemaakt, is geselecteerd voor Split Tunnel Network List.Klik op **OK** om naar de configuratie van het groepsbeleid terug te keren.

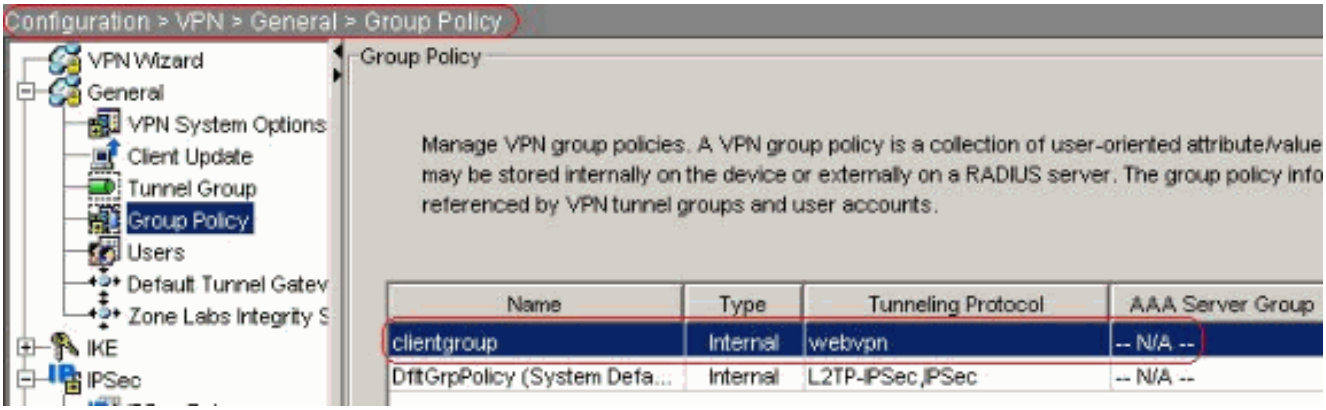


Klik in de hoofdpagina op **Toepassen** en **Verzend** (indien nodig) om de opdrachten naar de ASA te verzenden.Schakel voor de optie SSL VPN-client in het vakje Inherit uit en klik op het **optionele** radioknop.Met deze keuze kunt de externe client kiezen of u op het tabblad **WebVPN > SLB** klikt, en deze opties kiezen:Download de SVC niet. Kies altijd een optie die garandeert dat de SVC wordt gedownload naar het externe werkstation tijdens elke SSL VPN-verbinding.Schakel het vakje **Inherit uit** voor de optie Installeren bij clientsysteem en klik vervolgens op het radioknop **Ja**.Met deze actie kan de SVC-software op de clientmachine blijven staan; Daarom is de ASA niet verplicht de SVC-software aan de client te downloaden telkens wanneer een verbinding wordt gemaakt. Deze optie is een goede keuze voor externe gebruikers die vaak toegang hebben tot het bedrijfsnetwerk.Schakel het vakje **Inherit** uit, trek voor de optie Interval heronderhandelingen uit en geef het aantal minuten op tot het vakje

Onbeperkt is.De beveiliging wordt verbeterd wanneer u de limieten instelt op de tijdsduur die een toets geldig is.Schakel het vakje **Inherit uit** voor de optie Heronderhandelingsmethode en klik op de radioknop **SSL**. Heronderhandeling kan gebruik maken van de huidige SSL-tunnel of een nieuwe tunnel die uitdrukkelijk is gemaakt voor heronderhandeling.Uw SSL VPN-clienteigenschappen moeten worden geconfigureerd zoals in deze afbeelding:

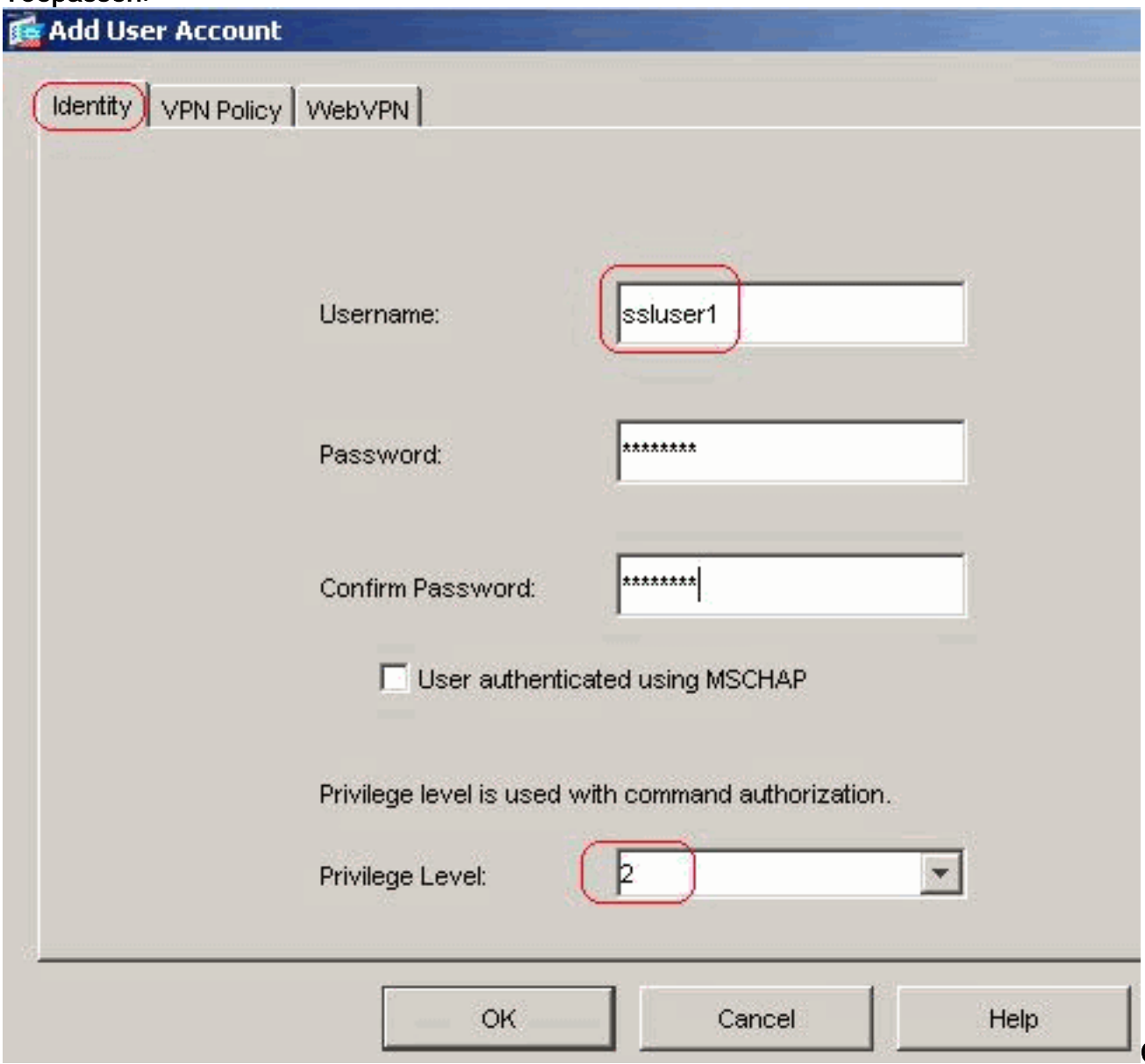


Klik op **OK** en vervolgens **op Toepassen**.



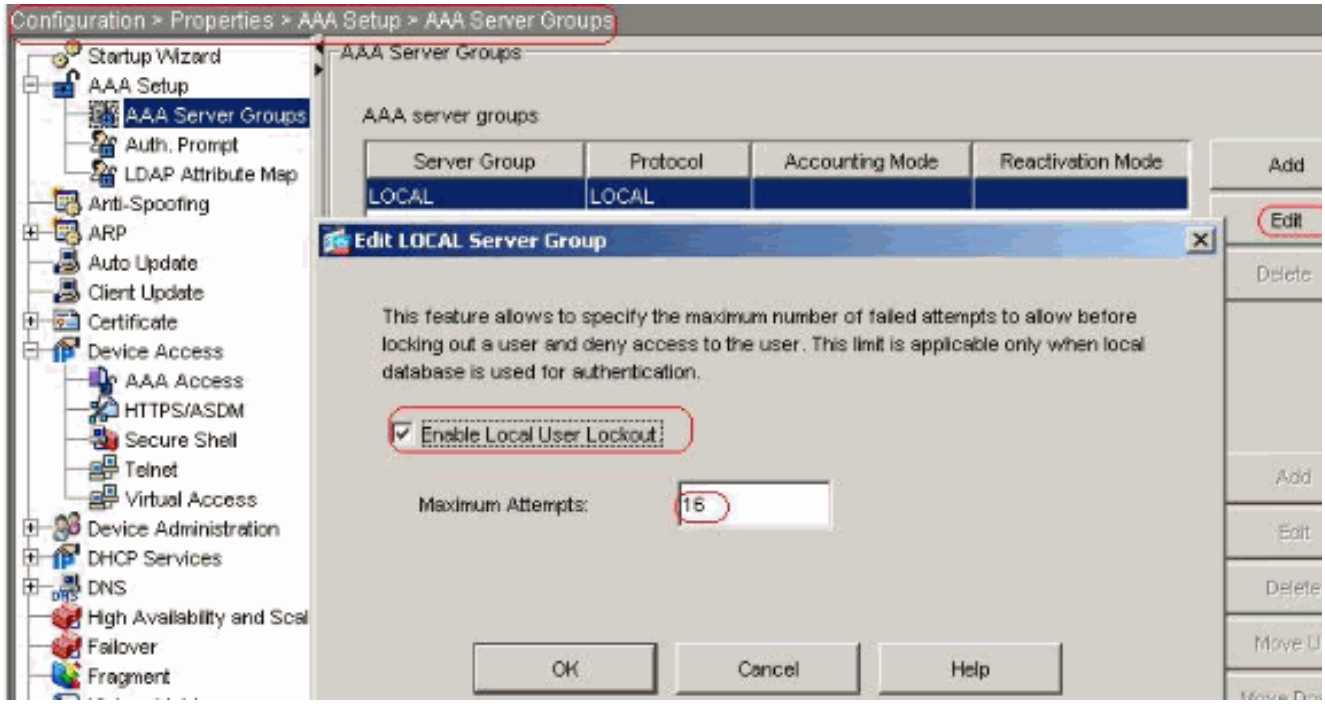
Compatibele CLI-configuratie:

5. Kies **Configuratie > VPN > Algemeen > Gebruikers > Toevoegen** om een nieuwe gebruikersaccount **te maken1**. Klik op **OK** en **Toepassen**.



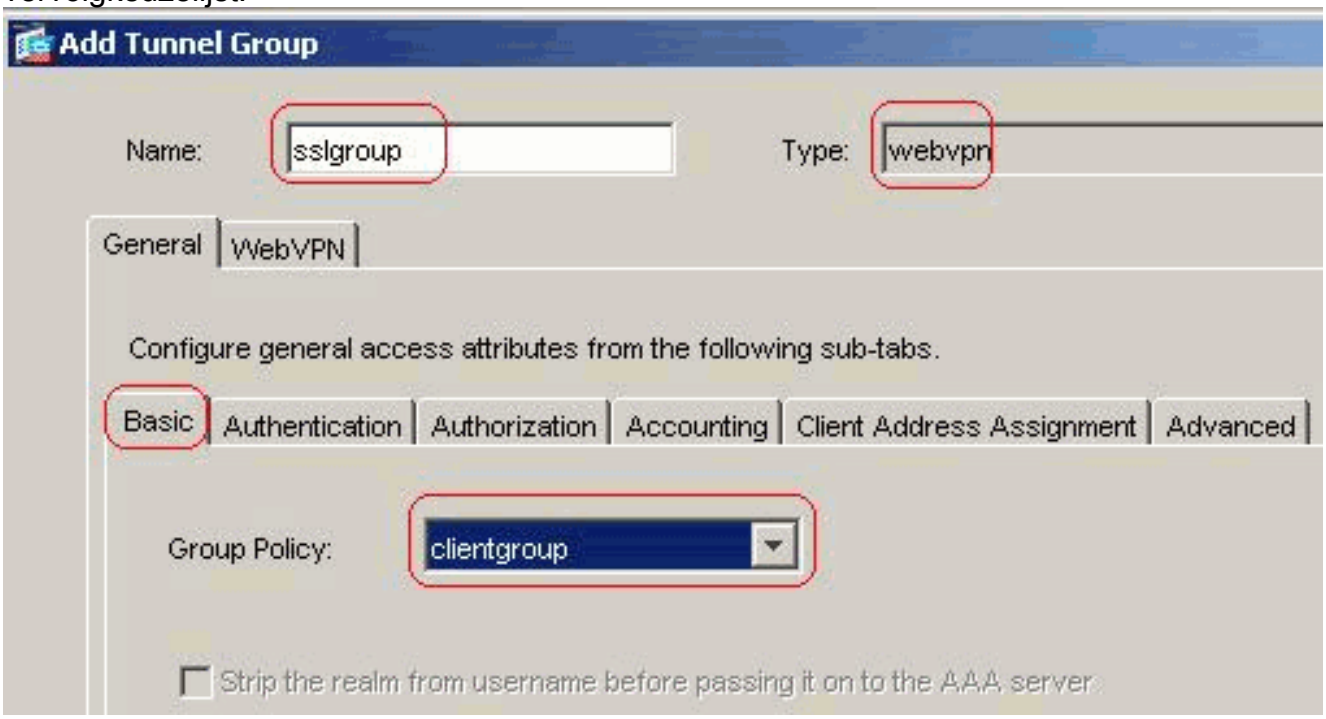
Compatibele CLI-configuratie:

6. Kies **Configuratie > Eigenschappen > AAA Instellingen > AAA-servers > Bewerken** om de standaardinstelling van de servergroep **LOCAL** te wijzigen en kies het aanvinkvakje **Local User Lockout** inschakelen met maximale probewaarde **16**.

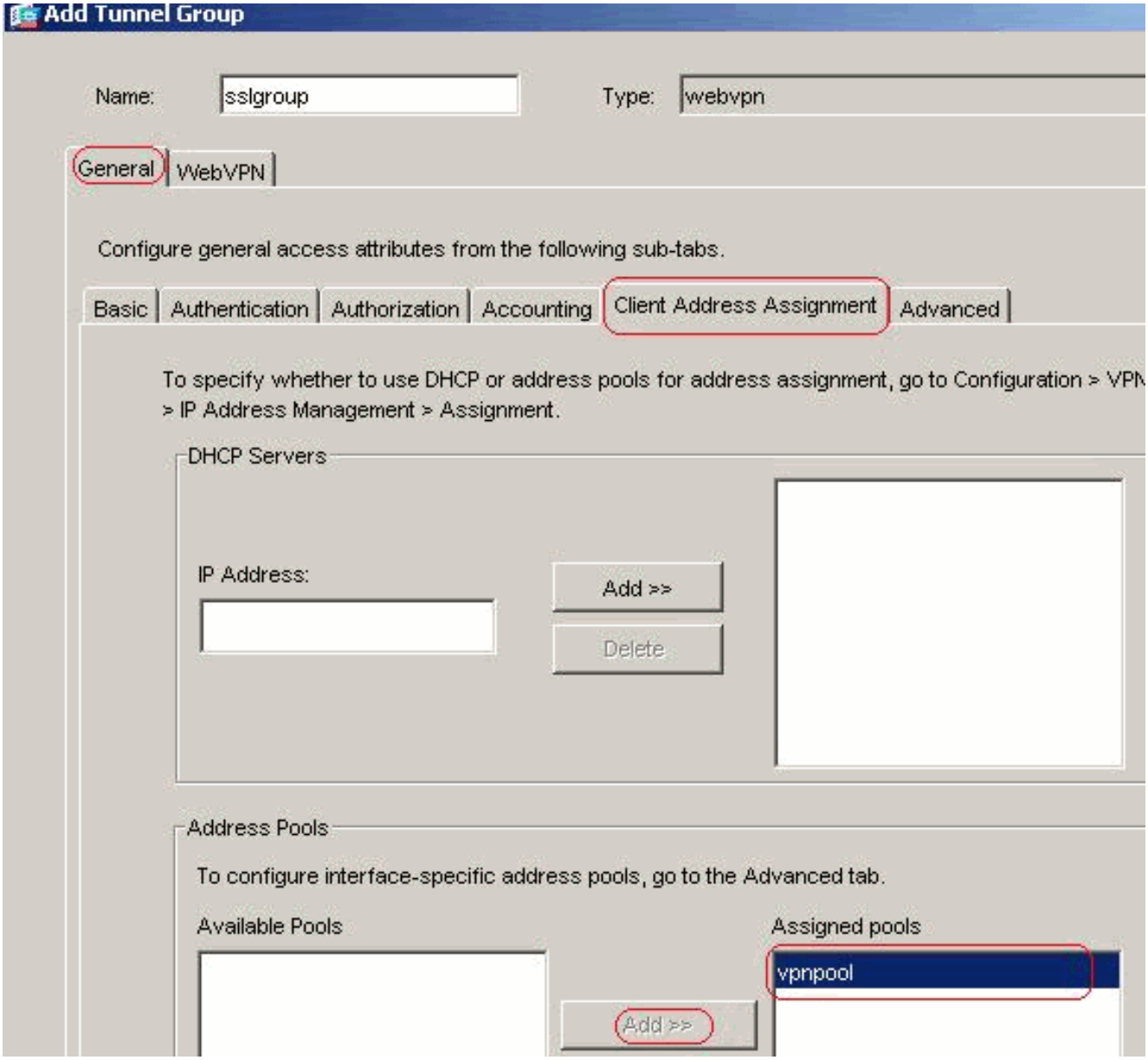


Compatibele CLI-configuratie:

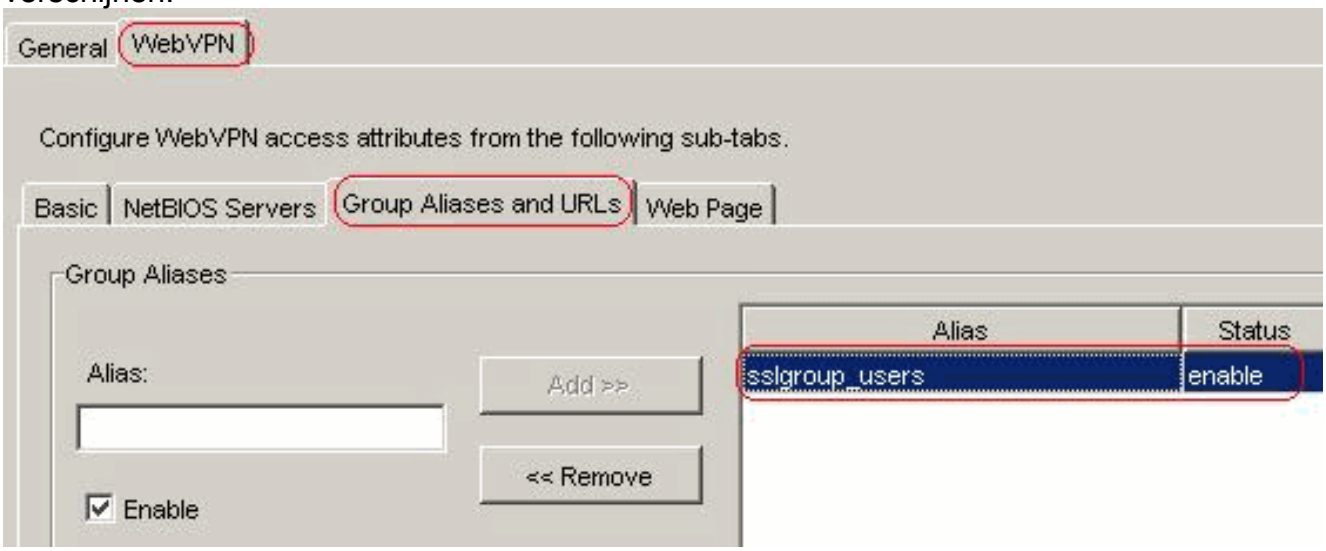
7. **Tunnelgroep configurerenKies Configuration > VPN > General > Tunnel Group > Add (WebVPN-toegang)** om een nieuwe **groep** voor tunnelgroepen te maken.In het tabblad **Algemeen > Basis** kiest u het groepsbeleid als **clientgroep** uit de vervolgkeuzelijst.



In **het** tabblad **Toewijzing van** clientadres, klikt u onder Adres Pools op **Add >>** om het beschikbare **VPN-adrespool** toe te
wijzen.

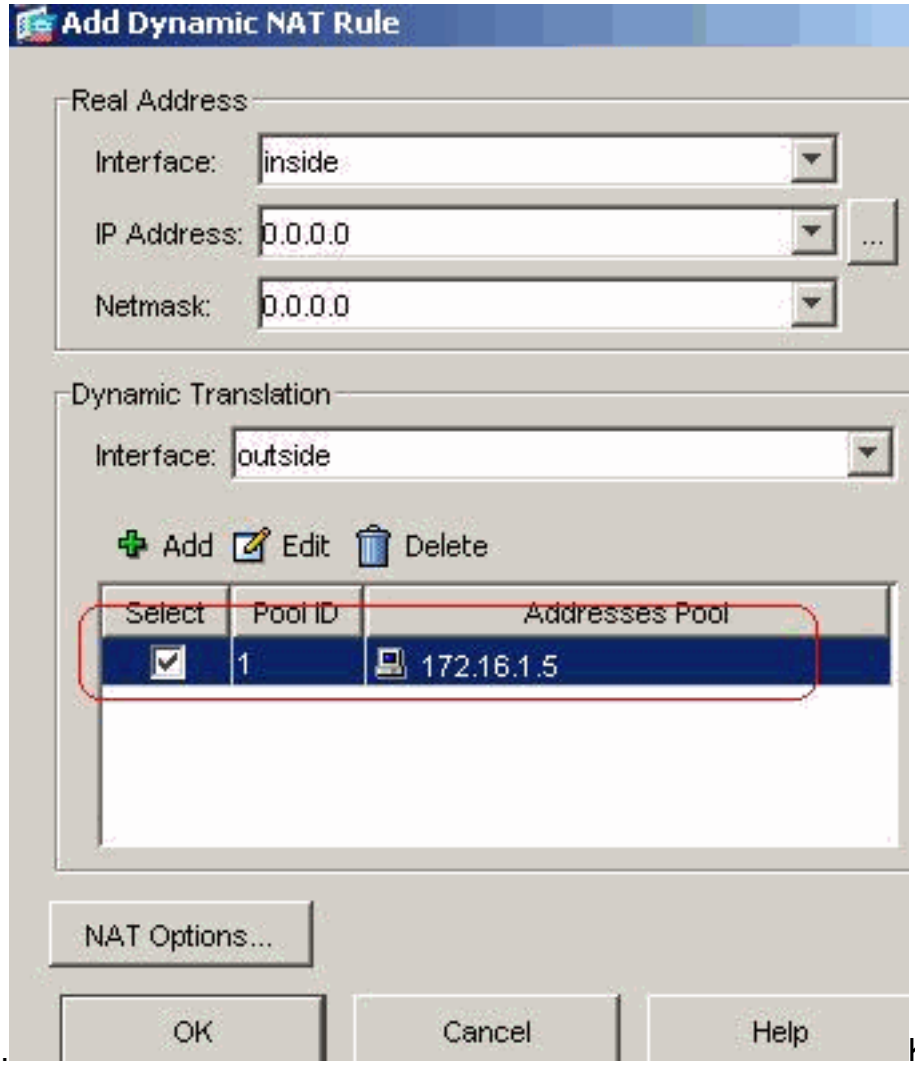


In het tabblad **WebVPN > Group Aliases en URL**'s typt u de naam van het alias in het dialoogvenster parameter en klikt u op **Add >>** om dit in de lijst met groepsnamen in de logpagina te laten
verschijnen.



Klik op **OK** en vervolgens **op Toepassen.Compatibele CLI-configuratie:**

8. **NAT configurerenKies Configuration > NAT > Add > Add > Dynamic NAT Rule** voor het

verkeer dat van het binnennetwerk komt die met extern IP adres 172.16.1.5 kan worden vertaald. 

Klik op **OK** en klik op **Toepassen** in de hoofdpagina.**Compatibele CLI-configuratie:**

9. Configureer de nat-vrijstelling voor het retourverkeer van binnen het netwerk naar de VPN-client.

```
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
```

ASA 7.2(2) Configuratie met 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
```

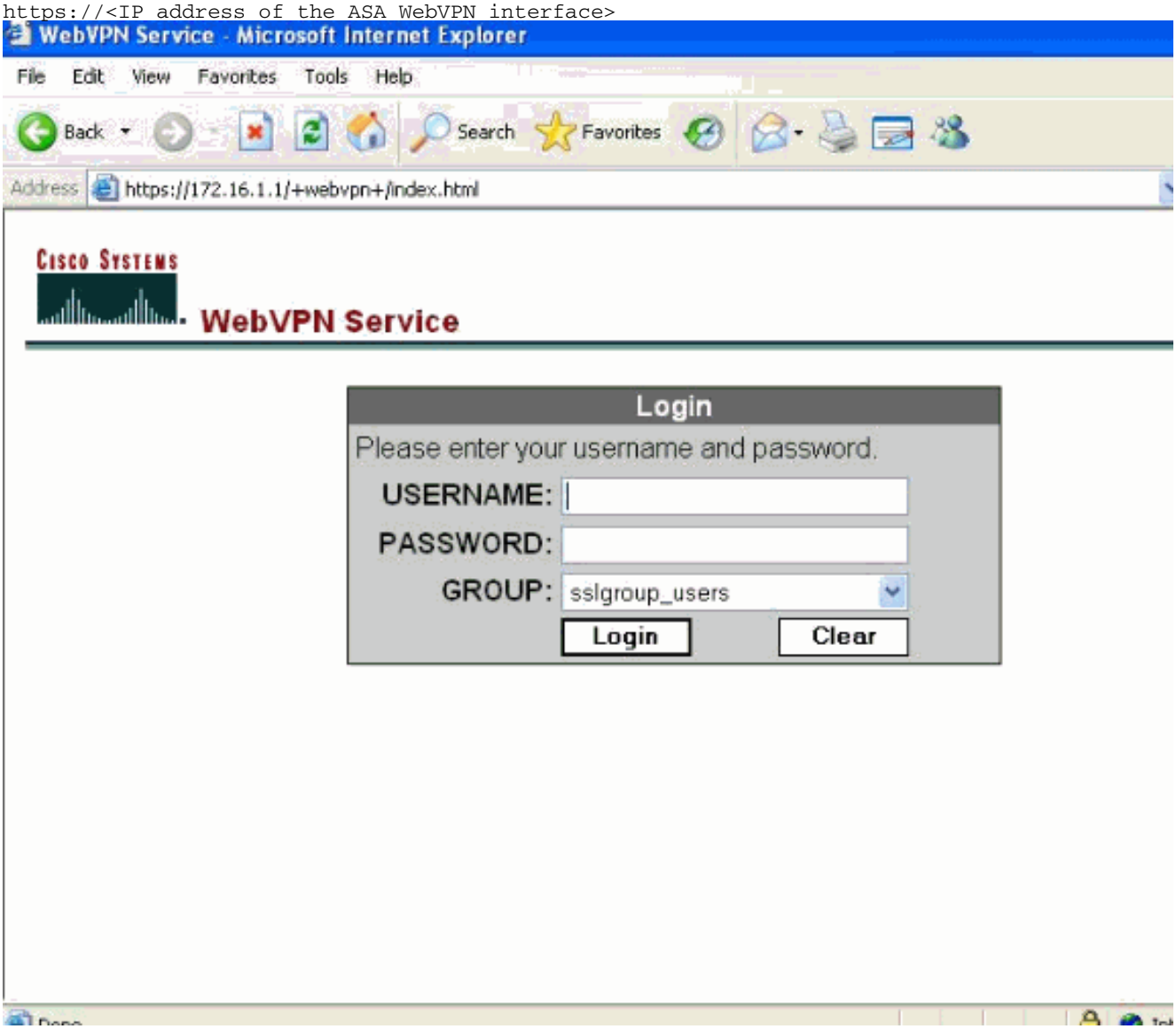
```
!--- Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelspecified
 split-tunnel-network-list value split-tunnel

!--- 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#
```

Instellen van de SSL VPN-verbinding met SVC

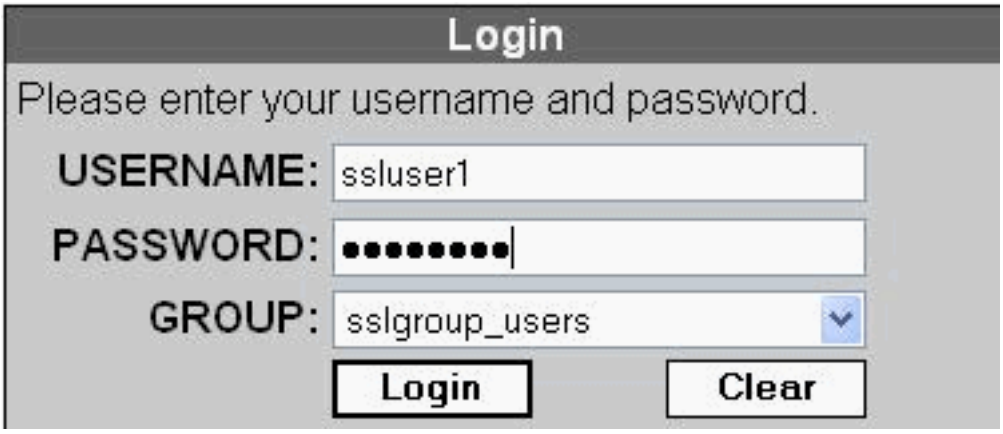
Voltooi deze stappen om een SSL VPN-verbinding met ASA op te zetten.

1. Typ het URL- of IP-adres van de WebVPN-interface van de ASA in uw webbrowser in het formaat zoals weergegeven.
   `https://url`
   OF
   `https://<IP address of the ASA WebVPN interface>`



2. Voer uw gebruikersnaam en wachtwoord in en kies vervolgens uw respectievelijke groep in de vervolgkeuzelijst zoals

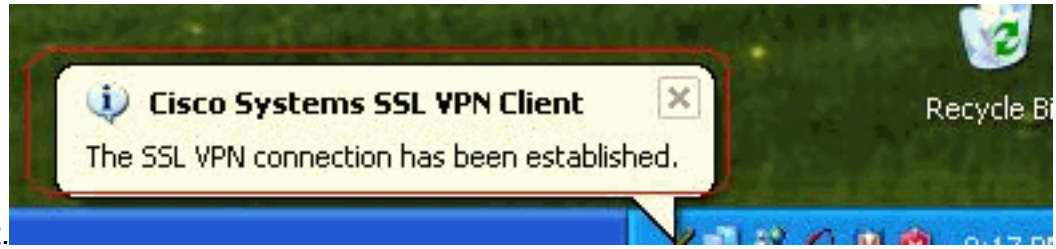
weergegeven.

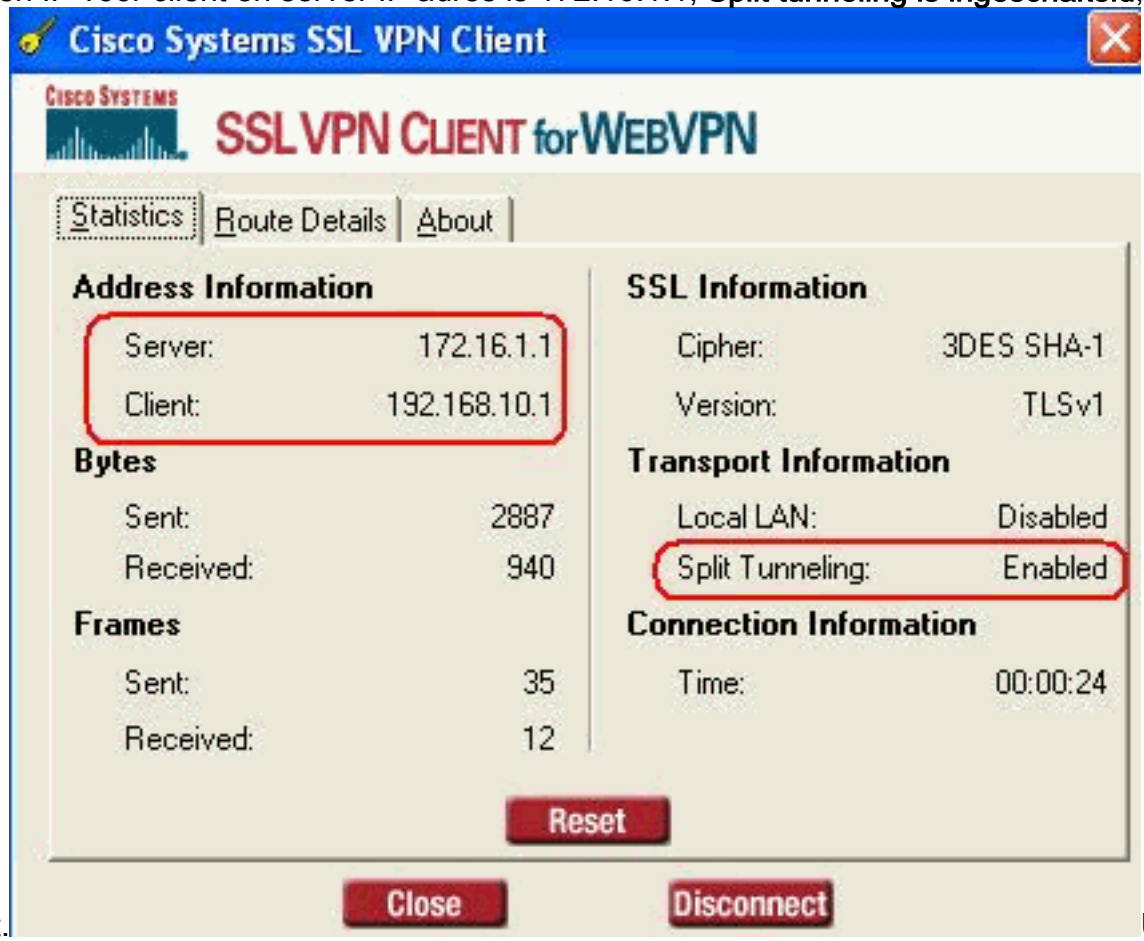


3. ActiveX-software moet in uw computer geïnstalleerd zijn voordat u de SVC downloaden.

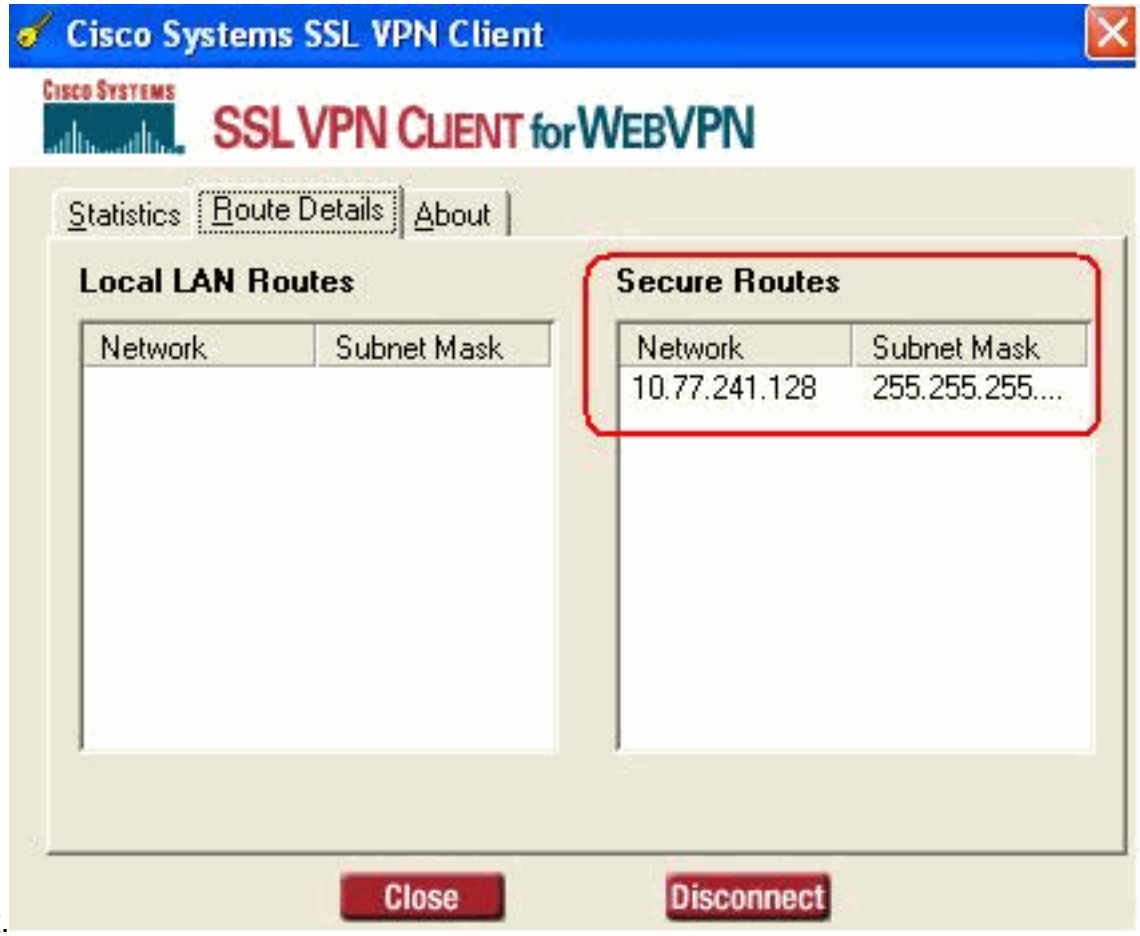
4. Deze vensters verschijnen voordat de SSL VPN-verbinding tot stand is gebracht.

5. U kunt deze vensters verkrijgen zodra de verbinding tot stand is

gebracht. 

6. Klik op de gele toets die in de taakbalk van uw computer verschijnt. Deze vensters worden weergegeven die informatie geven over de SSL-verbinding. Bijvoorbeeld, **192.168.10.1** is de toegewezen IP voor client en server IP adres is 172.16.1.1, **Split tunneling is ingeschakeld**, enzovoort. 

U kunt ook het beveiligde netwerk controleren dat door SSL moet worden versleuteld, de netwerklijst wordt gedownload van de gesplitste tunneltoegangslijst in ASA.In dit voorbeeld, waarborgt de SSL VPN client toegang tot 10.77.241.128/24 terwijl al het andere verkeer niet versleuteld en niet over de tunnel verzonden



wordt.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toon WebVPN svc**-Toont de SVC beelden die in het ASA flash geheugen zijn opgeslagen.

```
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
```

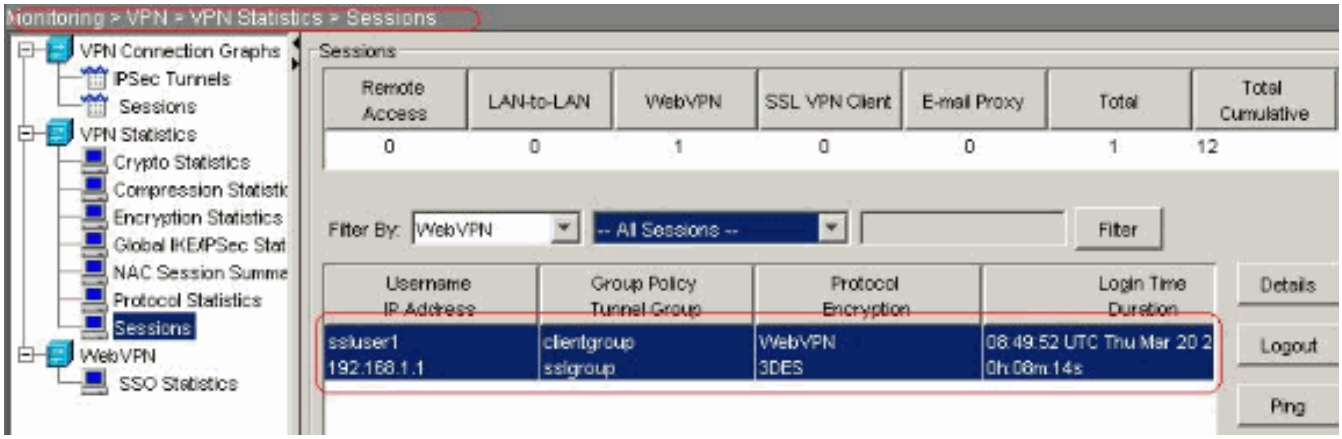
- **toon vpn-sessiondb svc**-Toont de informatie over de huidige SSL verbindingen.

```
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  :
```

- **Laat website-groep-alias**-displays de geconfigureerde alias voor verschillende groepen zien.

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- In ASDM, kies **Bewaking > VPN > Statistieken > Sessies** om over de huidige WebVPN sessies in de ASA te weten te komen.



Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

1. **vpn-sessiondb naam <gebruikersnaam>**- Opdracht om de SSL VPN-sessie voor de specifieke gebruikersnaam op te starten.

```
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
```

Evenzo kunt u de **vpn-sessiondb logoff svc** opdracht gebruiken om alle SVC-sessies te beëindigen.

2. **N.B.:** Als de PC naar de stand-by of de hibernate modus gaat, kan de SSL VPN-verbinding worden afgesloten.

```
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
```

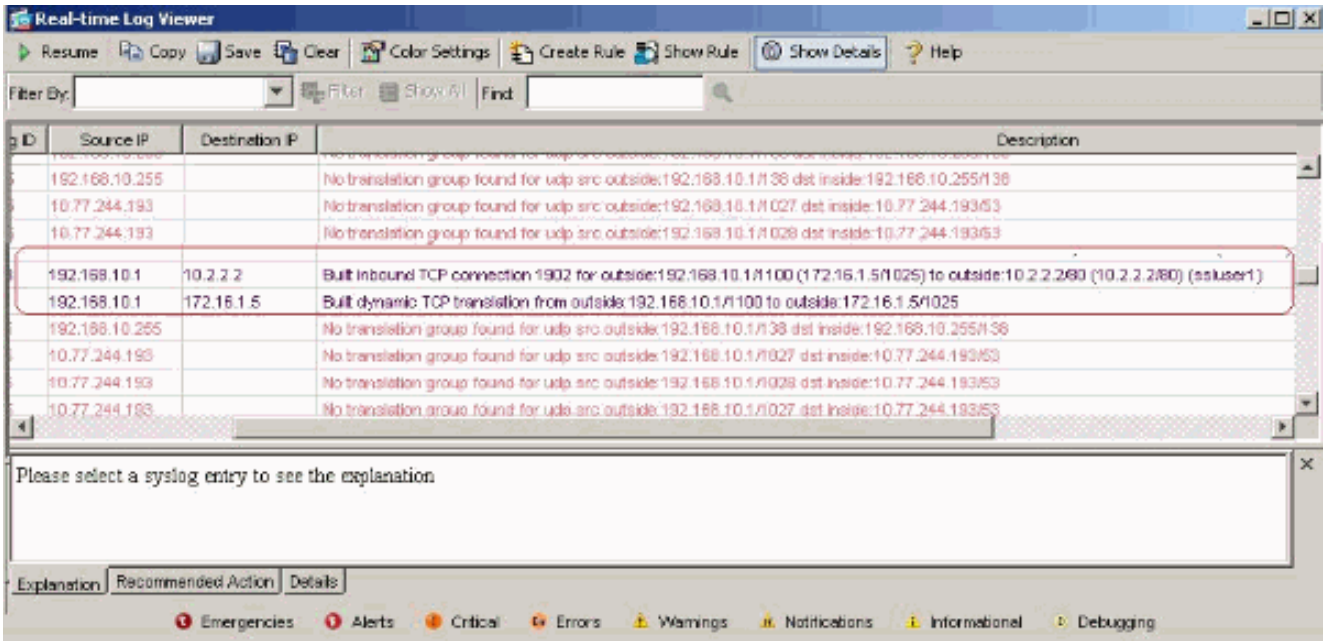
```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

3. **Debug WebVPN svc <1-255>**—Biedt de real-time webgebeurtenissen om de sessie te kunnen opzetten.

```
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. Kies in ASDM **Bewaking > Vastlegging > Realtime logvenster > Weergave** om de gebeurtenissen in realtime te kunnen zien. Dit voorbeeld toont de sessieinformatie tussen SVC 192.168.10.1 en Webserver 10.2.2.2 in het internet via ASA 172.16.1.5.



Gerelateerde informatie

- Cisco 5500 Series adaptieve security applicatie, productondersteuning
- ASA/PIX: Split-tunneling voor VPN-clients toestaan in het ASA Configuration-voorbeeld
- De router staat VPN-clients toe om IPsec en internet te verbinden met behulp van het configuratievoorbeeld voor splitter-tunneling
- PIX/ASA 7.x en VPN-client voor publiek internet VPN op een tick Configuration Voorbeeld
- SSL VPN-client (SVC) op ASA met ASDM Configuratievoorbeeld
- Technische ondersteuning en documentatie – Cisco Systems