ASA 7.2(2): SSL VPN-client (SVC) voor publiek internet VPN op een tick Configuration Voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een adaptieve security applicatie (ASA) 7.2.2 kunt instellen om SSL VPN op een stick uit te voeren. Deze instelling is van toepassing op een specifiek geval waarin de ASA geen gesplitste tunneling toestaat en gebruikers rechtstreeks verbinding maken met de ASA voordat ze naar internet mogen.

Opmerking: In ASA versie 7.2.2 staat het *intra-interface* ***sleutelwoord van het de*** configuratiewijze van de **zelfde-veiligheid-verkeer** al verkeer toe om het zelfde interface in te gaan en te verlaten (niet slechts IPsec verkeer).

Voorwaarden

Vereisten

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

- De hub ASA security applicatie moet versie 7.2.2 uitvoeren
- Cisco SSL VPN-client (SVC) 1.x**Opmerking:** Download het SSL VPN-clientpakket (sslclient-win*.pkg) van Cisco Software Download (alleen geregistreerde klanten). Kopieert de SVC

naar het flash-geheugen op de ASA. De SVC moet naar de externe gebruikerscomputers worden gedownload om de SSL VPN-verbinding met de ASA op te zetten. Raadpleeg het gedeelte SVC-software installeren van de *Cisco Security Appliance Opdracht Line Guide, versie 7.2* voor meer informatie.

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
- PC met Windows 2000 Professional of Windows XP
- 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 geeft 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 op te zetten, gaat de externe gebruiker het IP-adres in van een WebVPN-interface van het security apparaat in de browser, en de browser sluit op die interface en geeft het inlogscherm van WebeVPN weer. Als de gebruiker voldoet aan de inlognaam en de verificatie en het beveiligingsapparaat de gebruiker identificeert zoals deze de SVC nodig heeft, wordt de SVC naar de externe computer gedownloads. Als het beveiligingsapparaat de gebruiker identificeert met de optie om de SVC te gebruiken, downloads de SVC-installatie naar de externe computer terwijl er een link op het gebruikersscherm verschijnt om de SVC-installatie te overslaan.

Na het downloaden, installeert en vormt de SVC zichzelf, en vervolgens blijft de SVC (afhankelijk van de configuratie) zelf op de afstandscomputer installeren en verwijderen wanneer de verbinding wordt beëindigd.

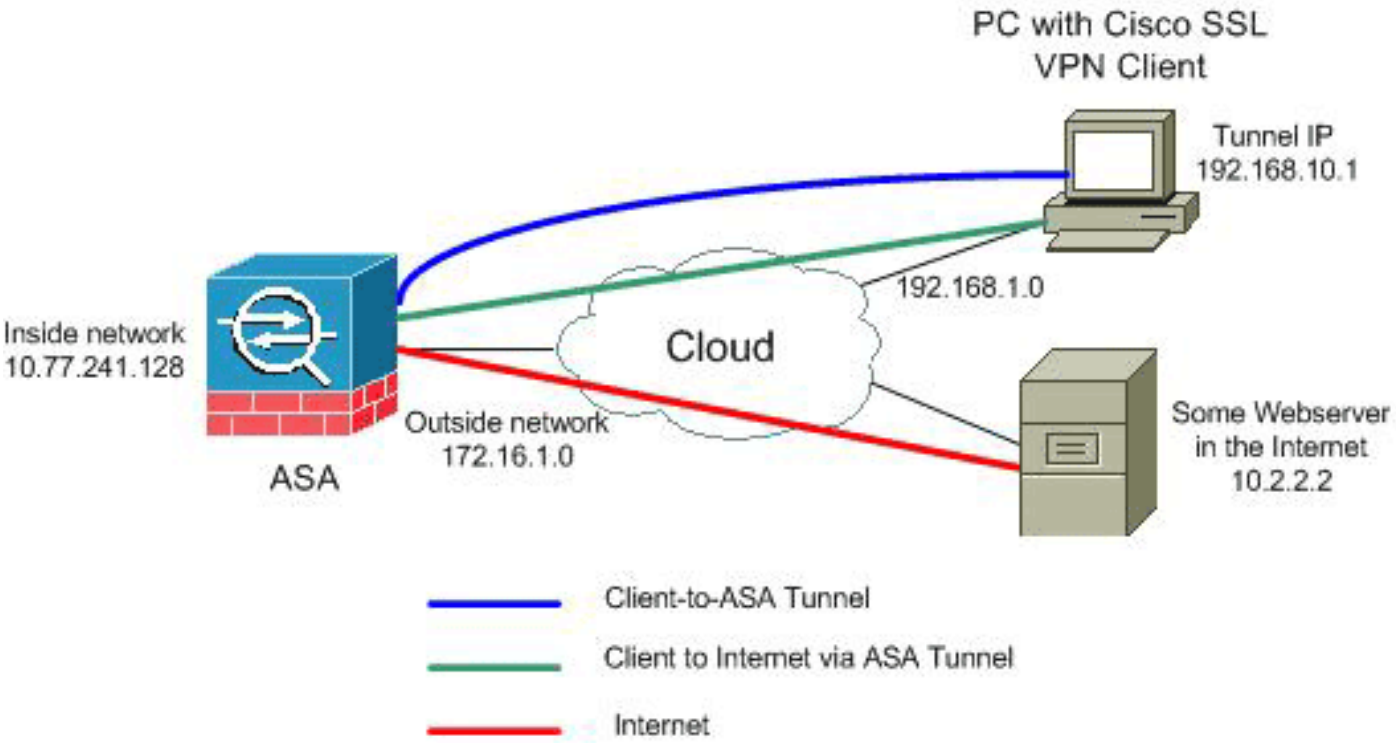
Configureren

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

Opmerking: Gebruik het Opname Gereedschap (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. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

ASA 7.2(2) Configuraties met ASDM 5.2(2)

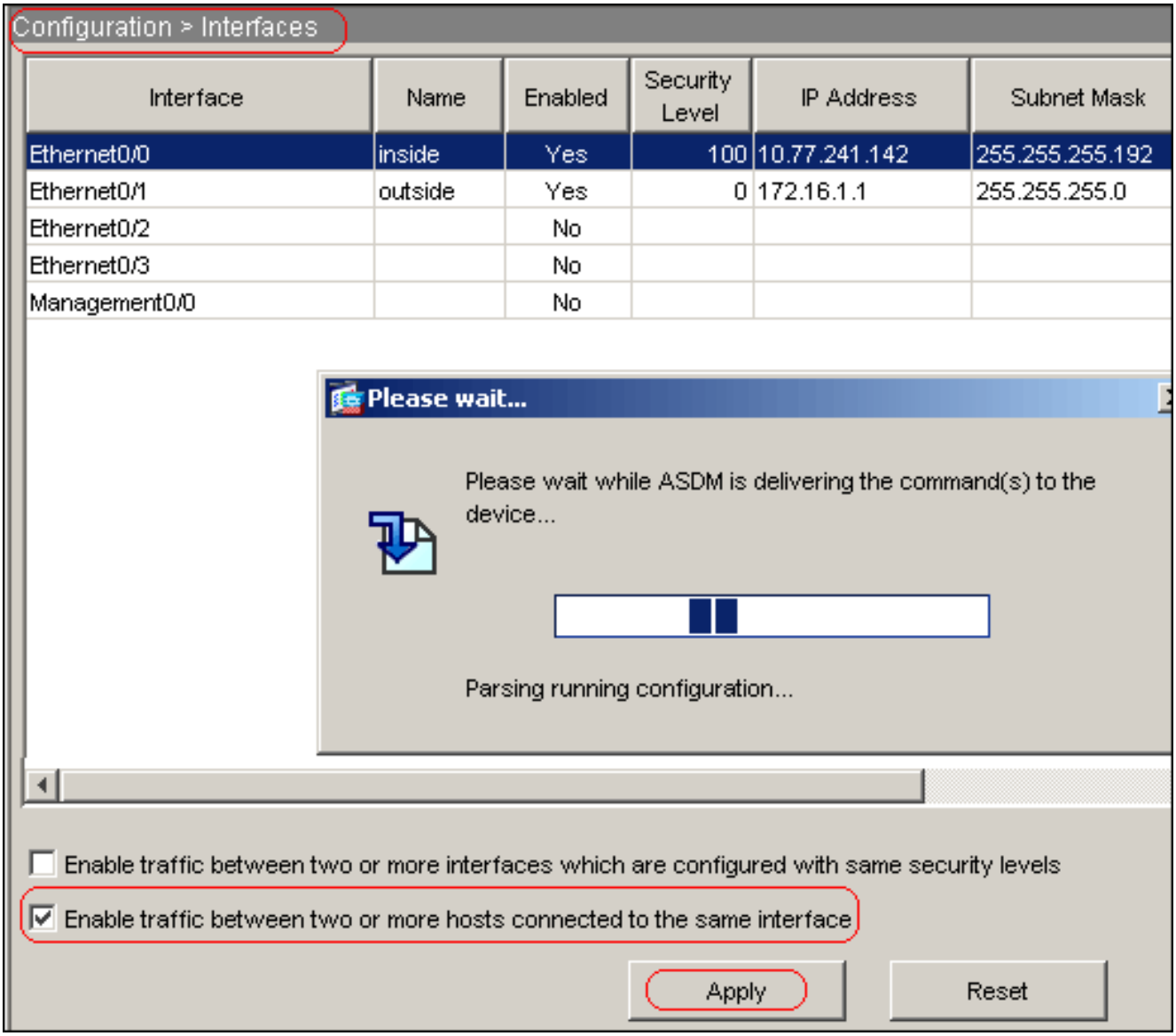
Dit document gaat uit van de basisconfiguraties, zoals de interfaceconfiguratie, die al gemaakt zijn en correct werken.

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.

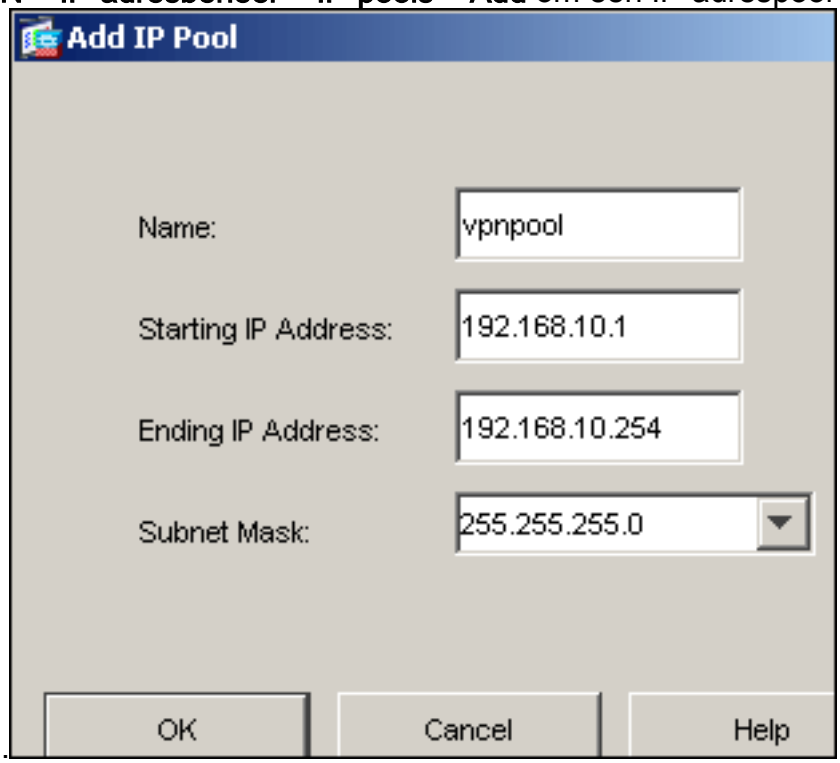
Voltooi deze stappen om SSL VPN op een stok in ASA te configureren:

1. Kies **Configuration > Interfaces** en controleer **het verkeer tussen twee of meer hosts die zijn aangesloten op dezelfde interface-**controle om SSL VPN-verkeer in te schakelen en dezelfde interface te verlaten.
2. Klik op **Toepassen**.



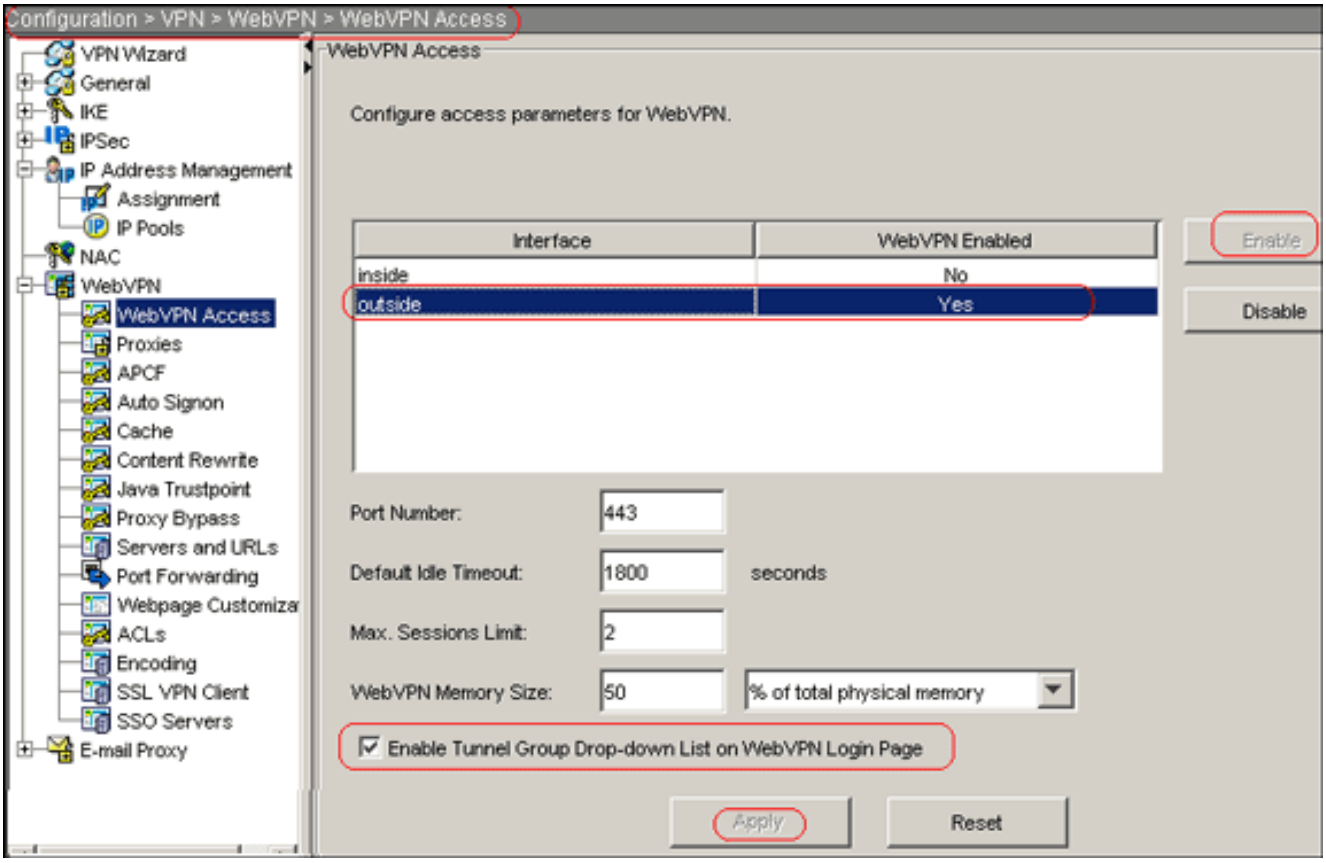
Opmerking: Hier is de equivalente CLI configuratie opdracht:

3. Kies **Configuration > VPN > IP-adresbeheer > IP-pools > Add** om een IP-adrespool met de naam *vpnpool* te maken.

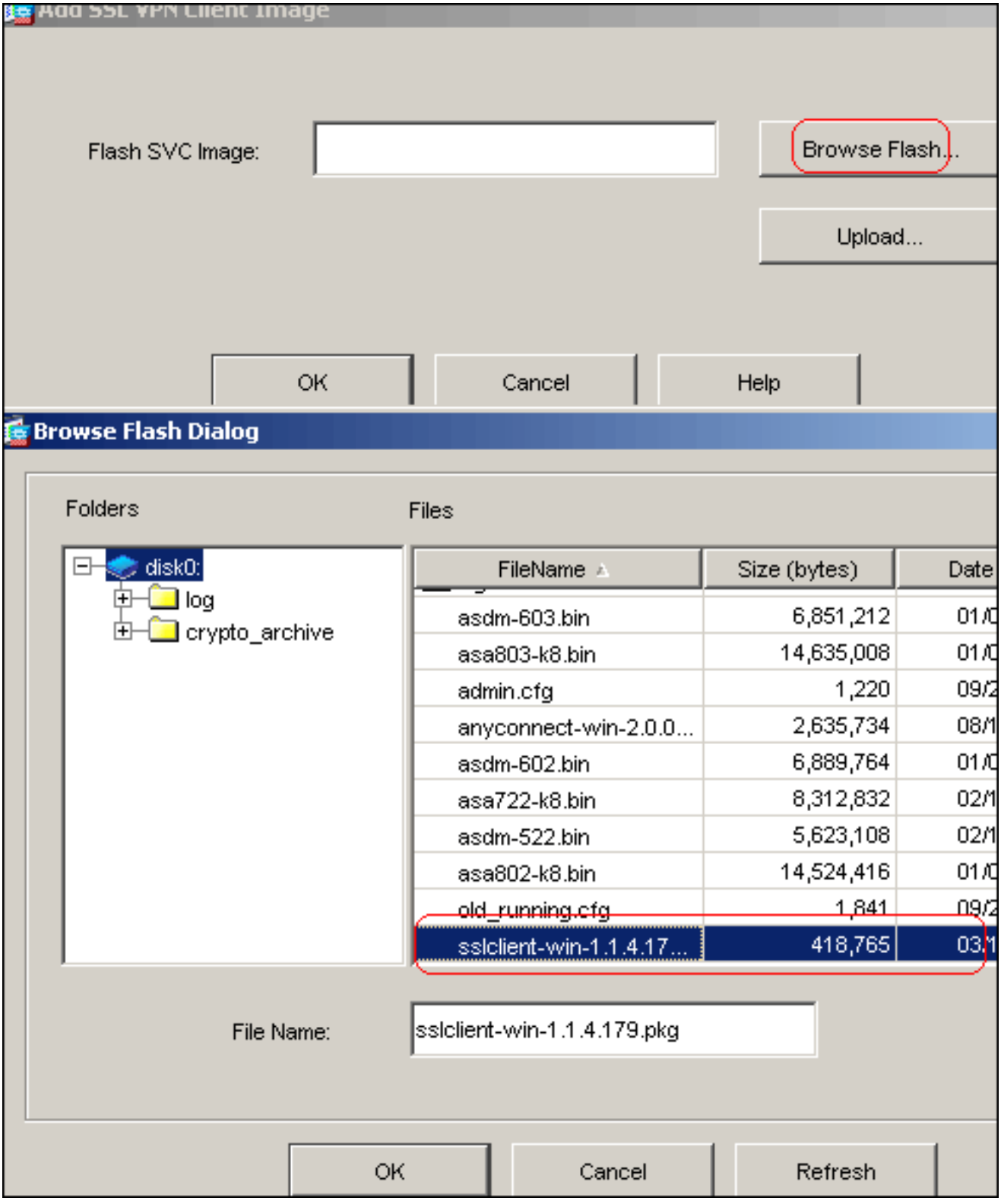


4. Klik op **Toepassen**.**Opmerking:** Hier is de equivalente CLI configuratie opdracht:

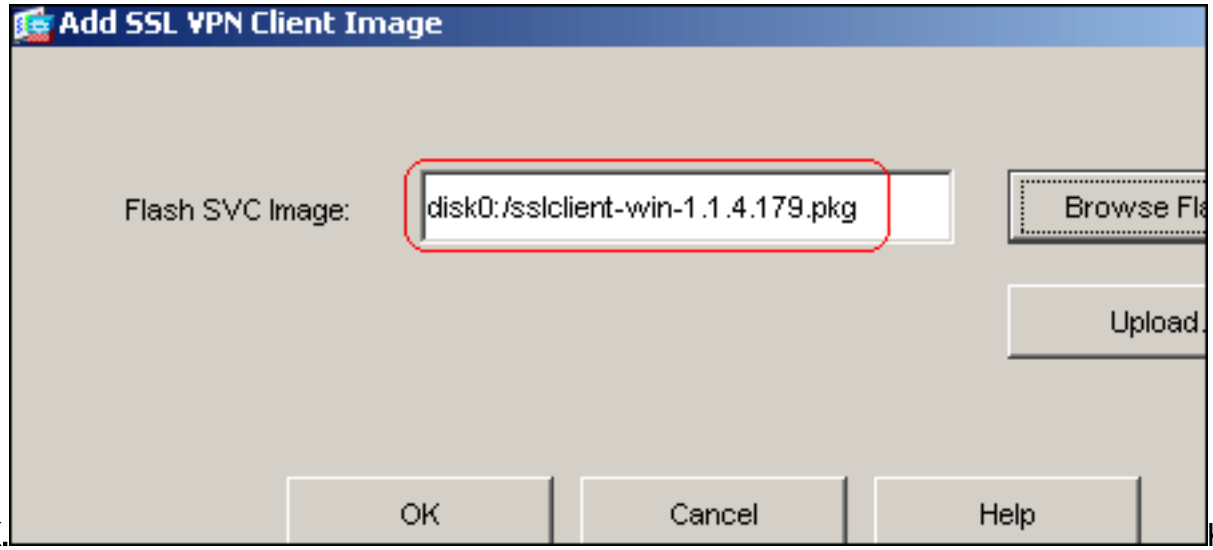
5. WebVPN inschakelen:Kies **Configuratie > VPN > WebVPN > WebVPN Access** en selecteer de externe interface.Klik op **Inschakelen**.Controleer de **vervolgkeuzelijst Trunnengroep inschakelen in het** dialoogvenster **Pagina voor loggen van WebVPN** om gebruikers in staat te stellen hun respectievelijke groepen op de loginpagina te kiezen.



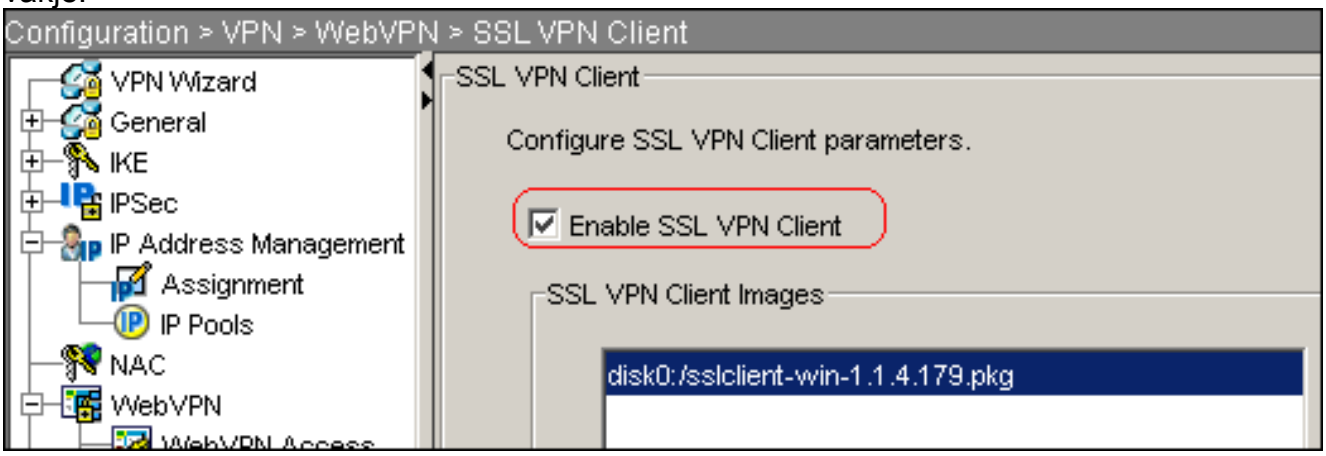
Klik op **Toepassen**.Kies **Configuratie > VPN > WebVPN > SSL VPN-client > Add** om het SSL VPN-clientbeeld uit het flash-geheugen van ASA toe te voegen.


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

Klik op

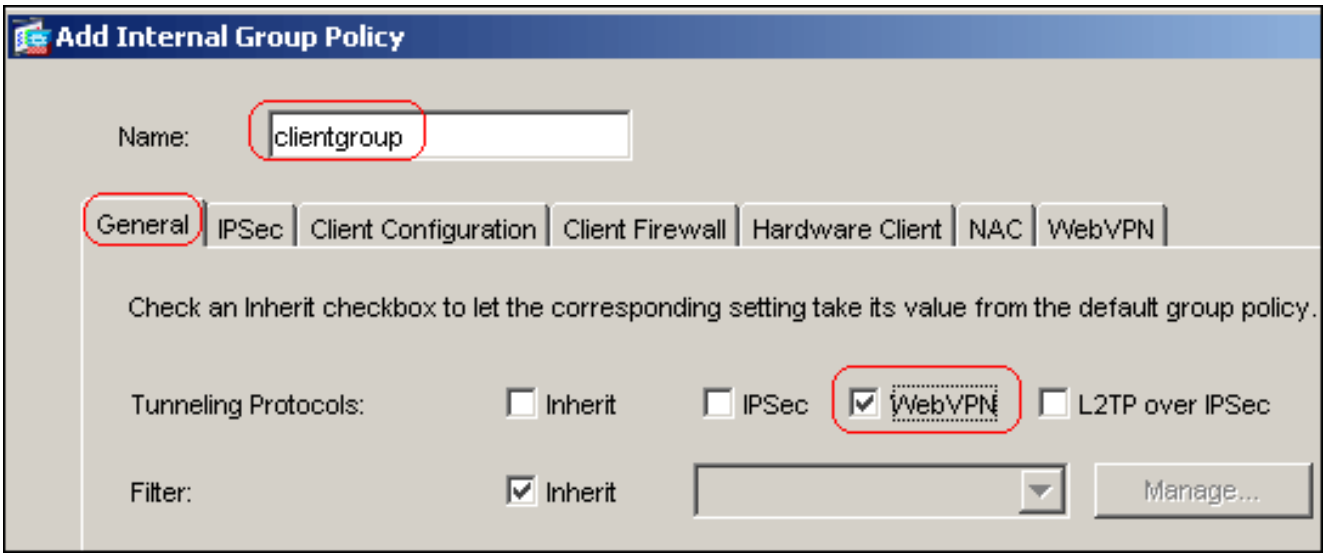


OK.Klik op **OK**.Klik op **SSL VPN-client** vakje.



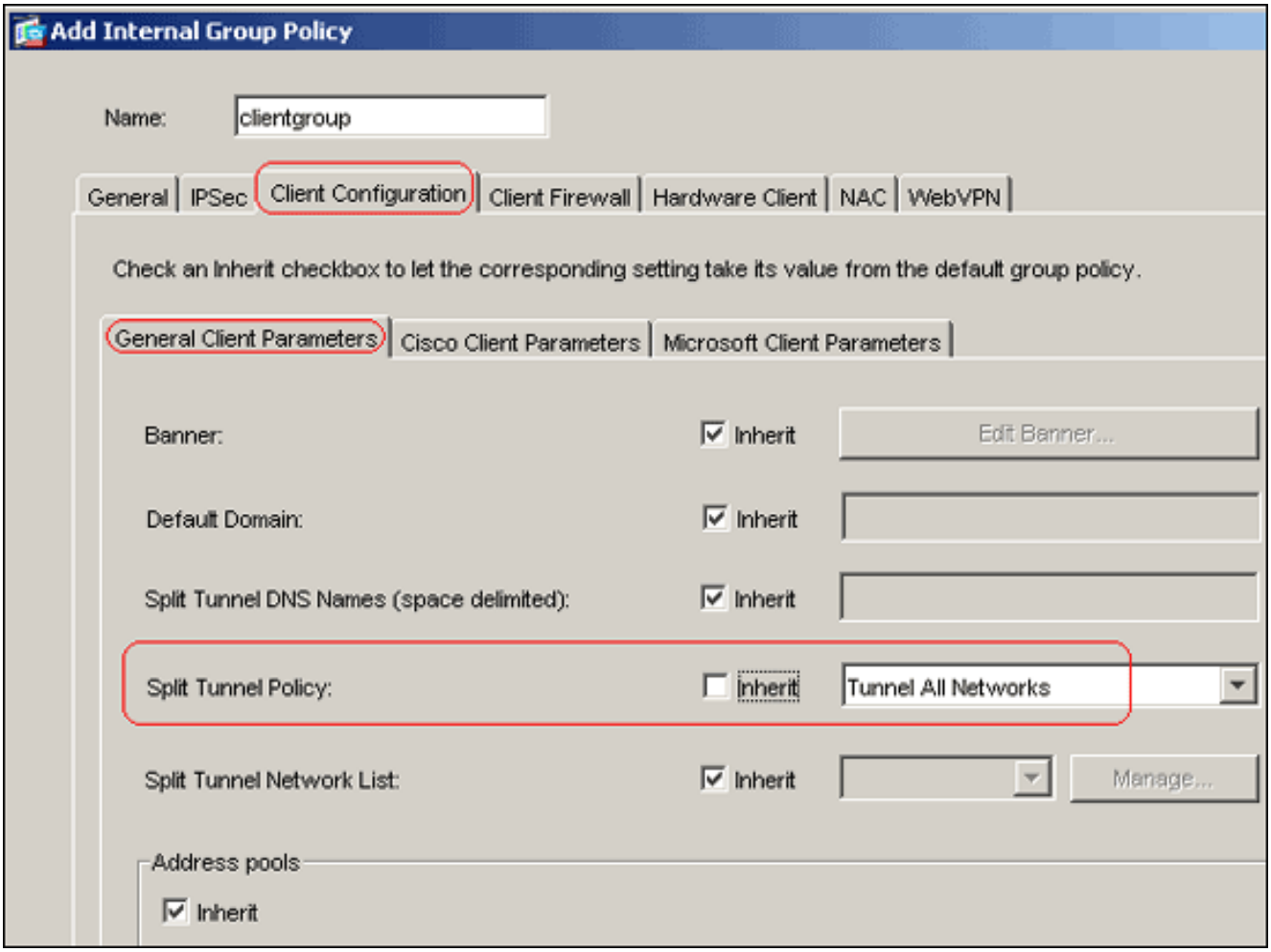
Opmerking: Hier zijn de gelijkwaardige CLI-configuratieopdrachten:

6. Configuratie van het groepsbeleid:Kies **Configuratie > VPN > Algemeen > Groepsbeleid > Toevoegen (Intern Groepsbeleid)** om een intern groepsbeleid te creëren dat *clientgroep* wordt genoemd.Klik op het tabblad **Algemeen** en selecteer het dialoogvenster **WebVPN** om het protocol voor een tunneling in te schakelen.

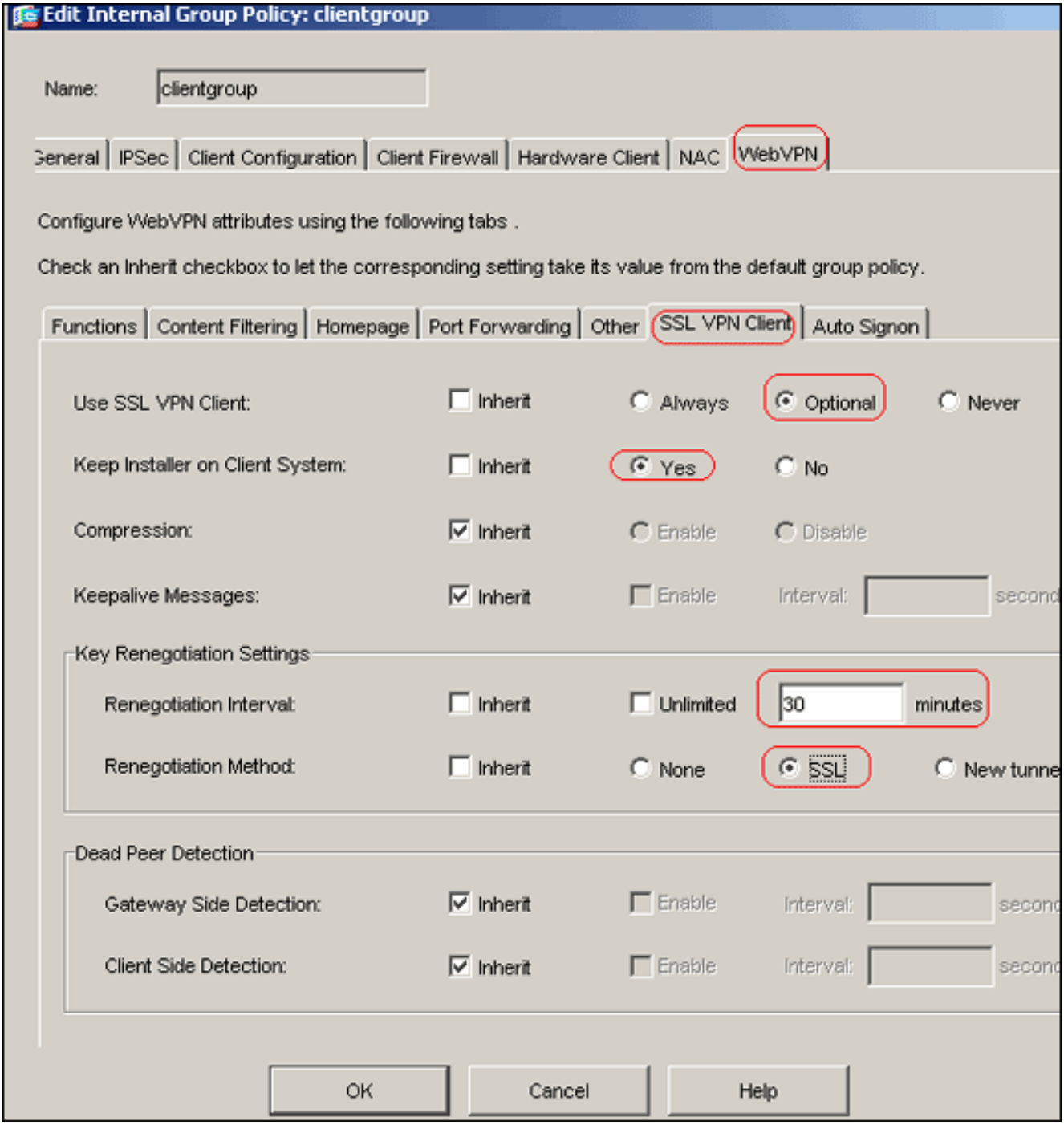


Klik op het tabblad **Clientconfiguratie** en klik vervolgens op het tabblad **Algemene clientparameters**.Kies **Tunnel All Networks** van de vervolgkeuzelijst Split Tunnel Policy om alle pakketten van de afstandsbediening van een beveiligde tunnel te

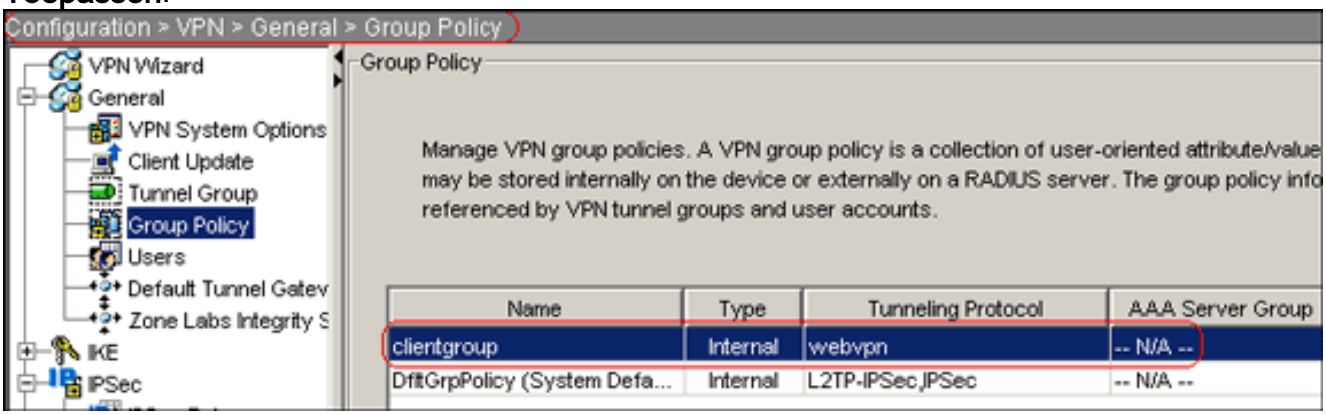
maken.



Klik op het tabblad **WebVPN > client** voor **VPN** en kies deze opties:Schakel het vakje **Inherit uit** voor de optie SSL VPN-client en klik vervolgens op de **optionele** radioknop.Met deze optie kan de externe client kiezen of de SVC al dan niet wordt gedownload. 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 optie blijft de SVC-software op de client actief. 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.**Opmerking:** De beveiliging wordt verbeterd door limieten in te stellen voor de tijdsduur die een toets geldig is.Schakel het vakje **Inherit uit** voor de optie Heronderhandelingsmethode en klik op de radioknop **SSL**.**Opmerking:** Heronderhandeling kan gebruik maken van de huidige SSL-tunnel of van een nieuwe tunnel die speciaal is gemaakt voor heronderhandeling.Uw SSL VPN-clienteigenschappen moeten worden geconfigureerd zoals in deze
afbeelding:



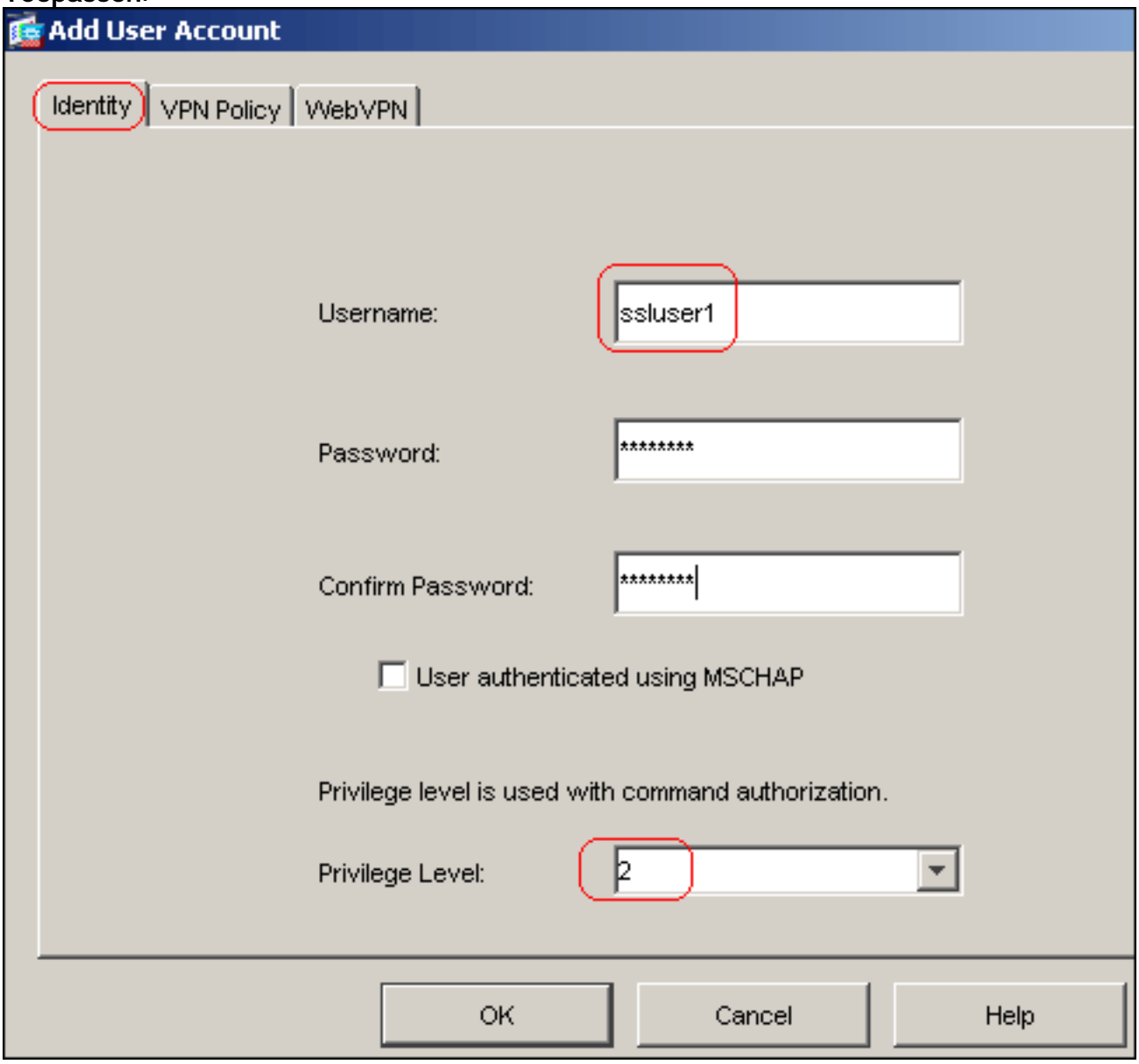
Klik op **OK** en vervolgens op **Toepassen**.



Opmerking: Hier zijn de gelijkwaardige CLI-configuratieopdrachten:

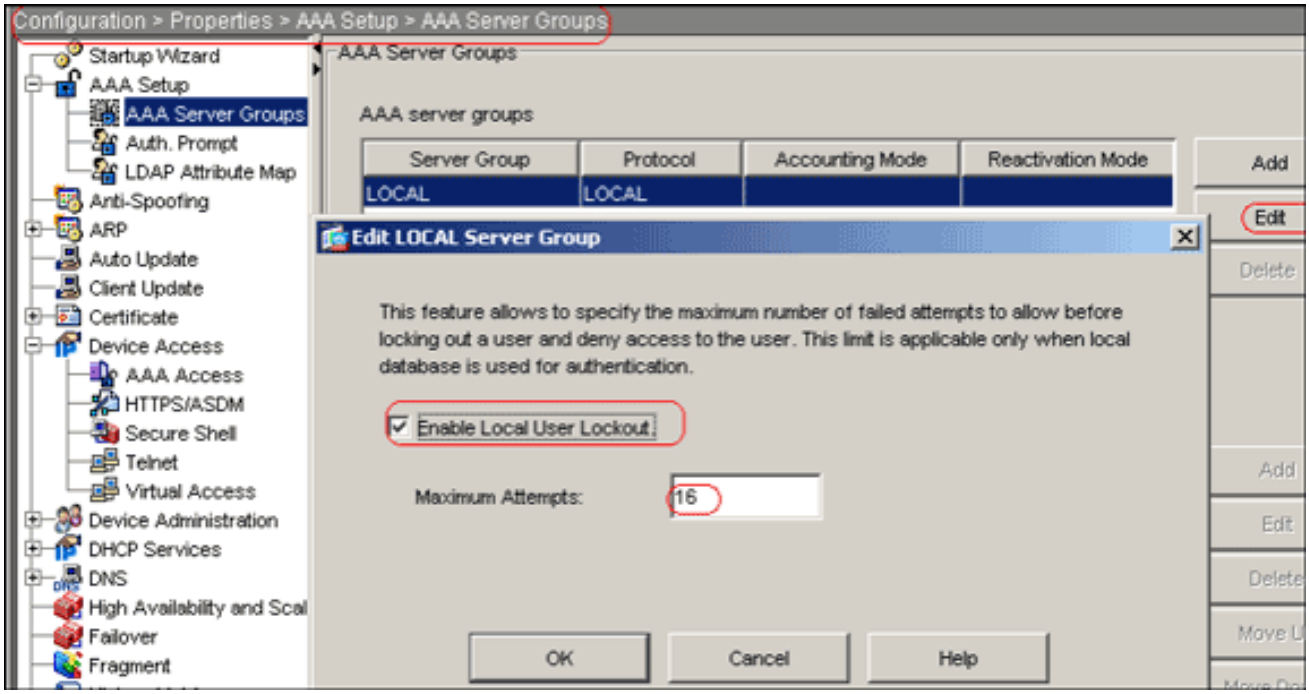
7. Kies **Configuratie > VPN > Algemeen > Gebruikers > Toevoegen** om een nieuwe *gebruikersaccount* te maken*1*.

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



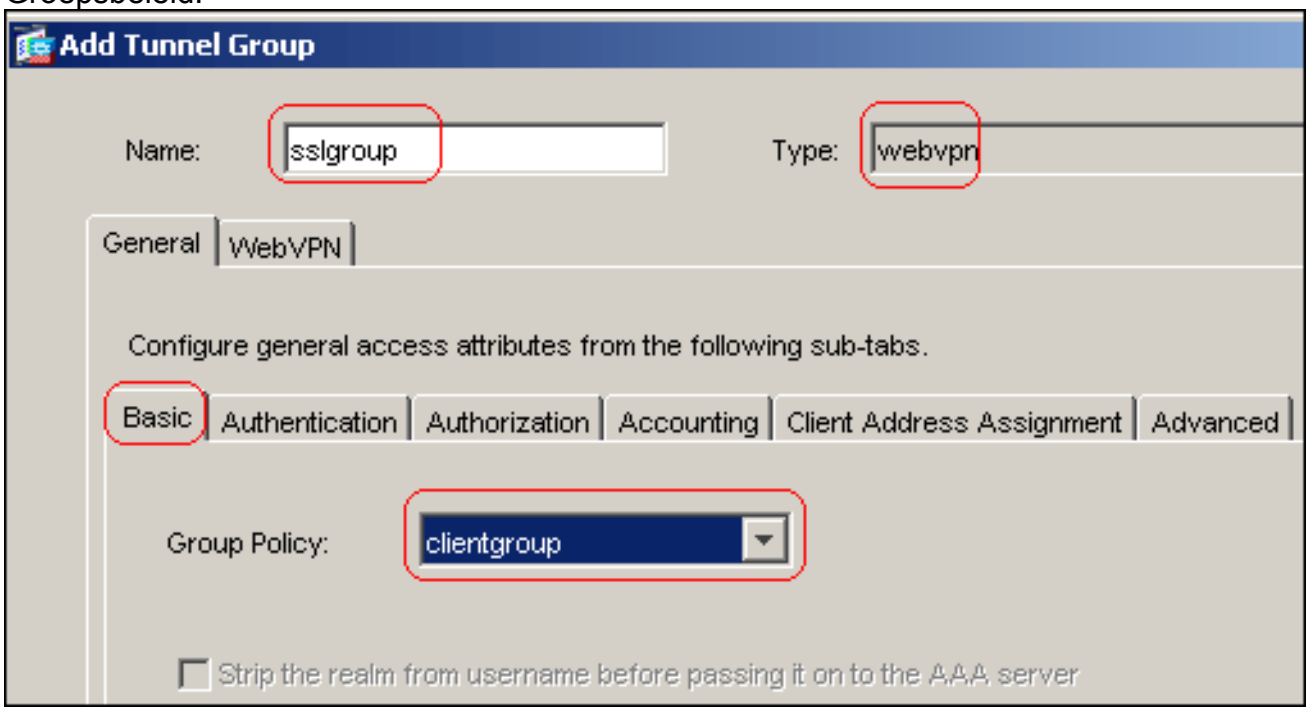
Opmerking: Dit is de gelijkwaardige CLI-opdracht:

9. Kies **Configuratie > Eigenschappen > AAA Instellingen > AAA-servers > Bewerken**.
10. Selecteer het standaardservervak *LOKAAL* en klik op **Bewerken**.
11. Klik in het dialoogvenster LOCAL Server Group bewerken op het dialoogvenster **Local User Lockout** inschakelen en voer 16 in het tekstvak Maximum aantal pogingen in.
12. Klik op **OK**.

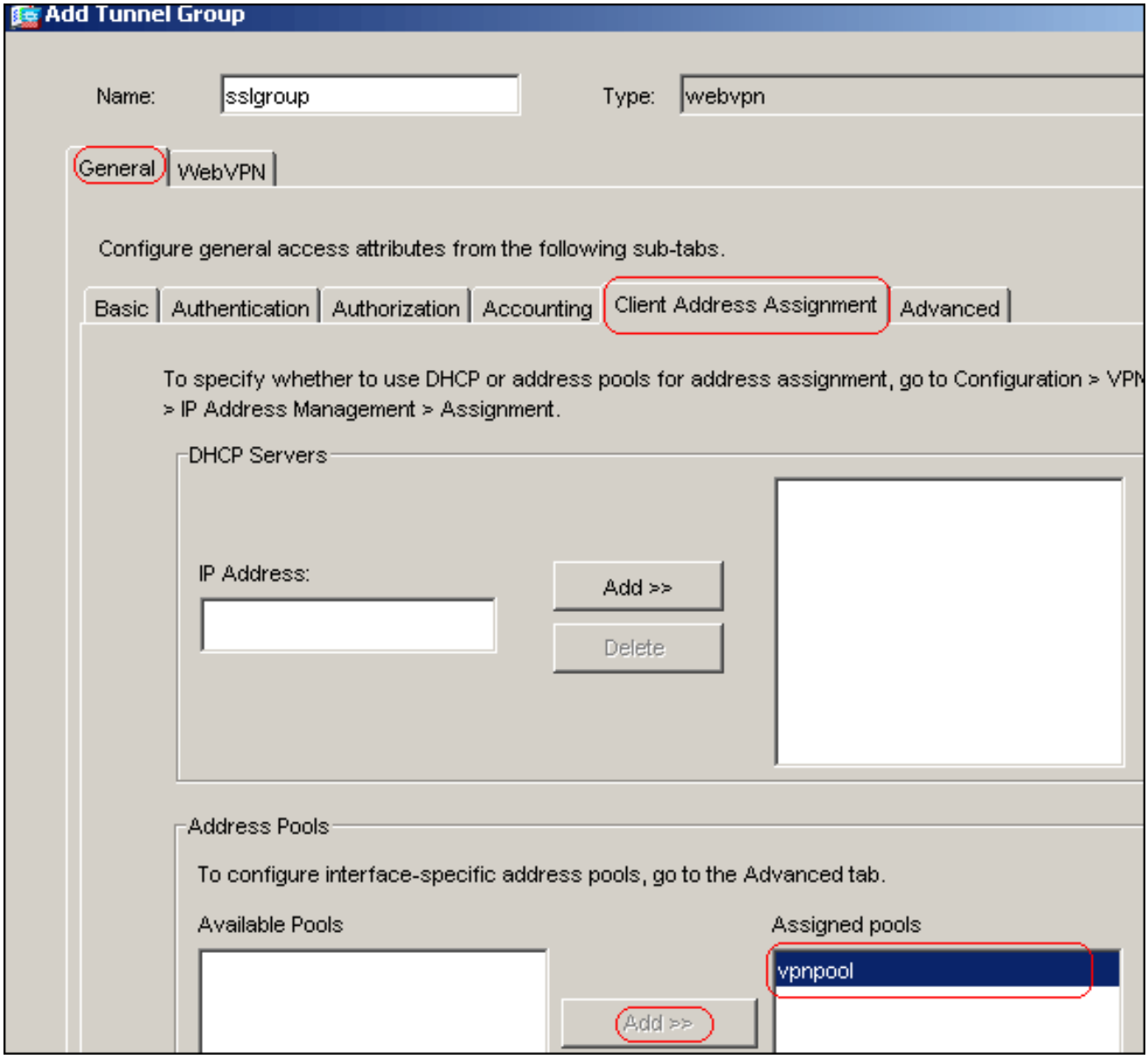


Opmerking: Dit is de gelijkwaardige CLI-opdracht:

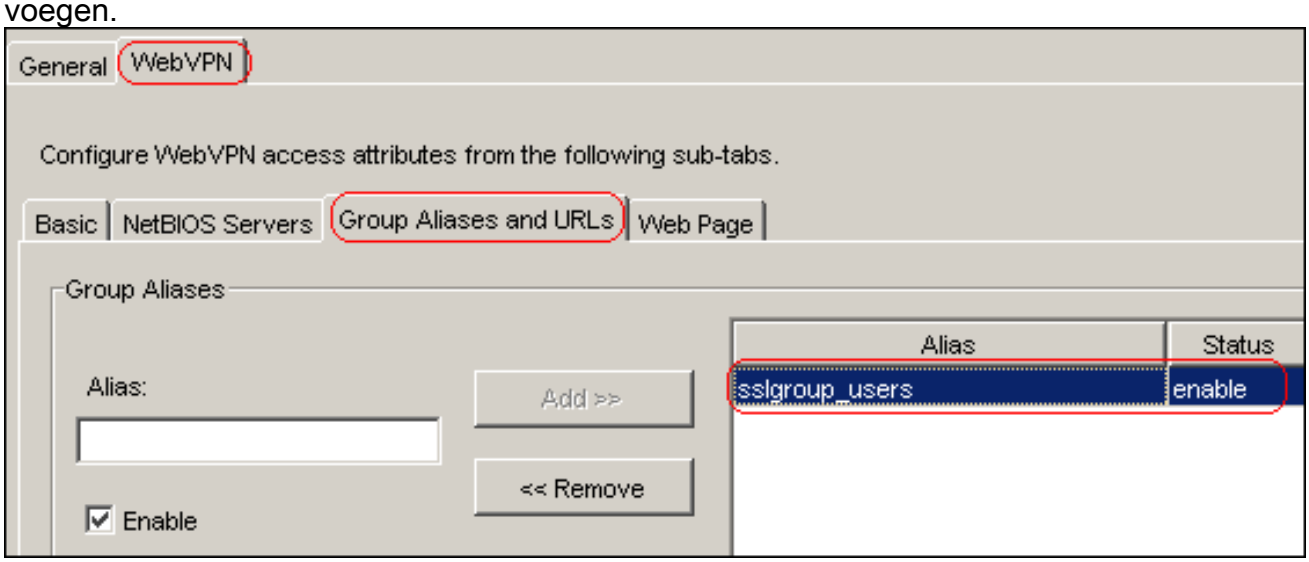
13. Configuratie van de tunnelgroep:Kies **Configuration > VPN > General > Tunnel Group > Add (WebVPN-toegang)** om een nieuwe tunnelgroep met de naam *Sslgroup* te maken.Klik op het tabblad **Algemeen** en klik vervolgens op het tabblad **Basis**.Kies **clientgroep** uit de vervolgkeuzelijst
Groepsbeleid.



Klik op het tabblad **Clientadrestoewijzing** en klik vervolgens op **Toevoegen** om het beschikbare *deelvenster* met adressen toe te
wijzen.



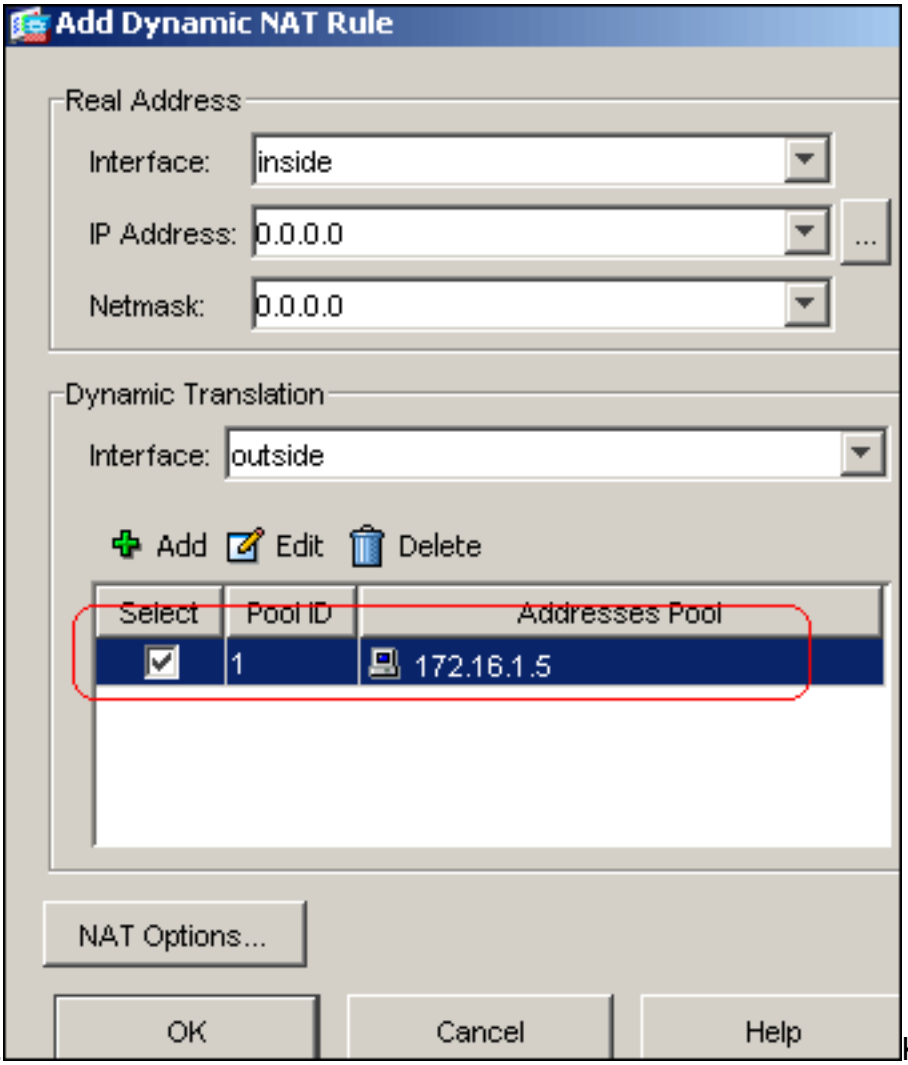
Klik op het tabblad **WebVPN** en klik vervolgens op het tabblad **Group Aliases en URL**.Typ de naam van het alias in het veld parameter en klik op **Toevoegen** om deze aan de lijst met groepsnamen op de pagina Aanmelden toe te
voegen.



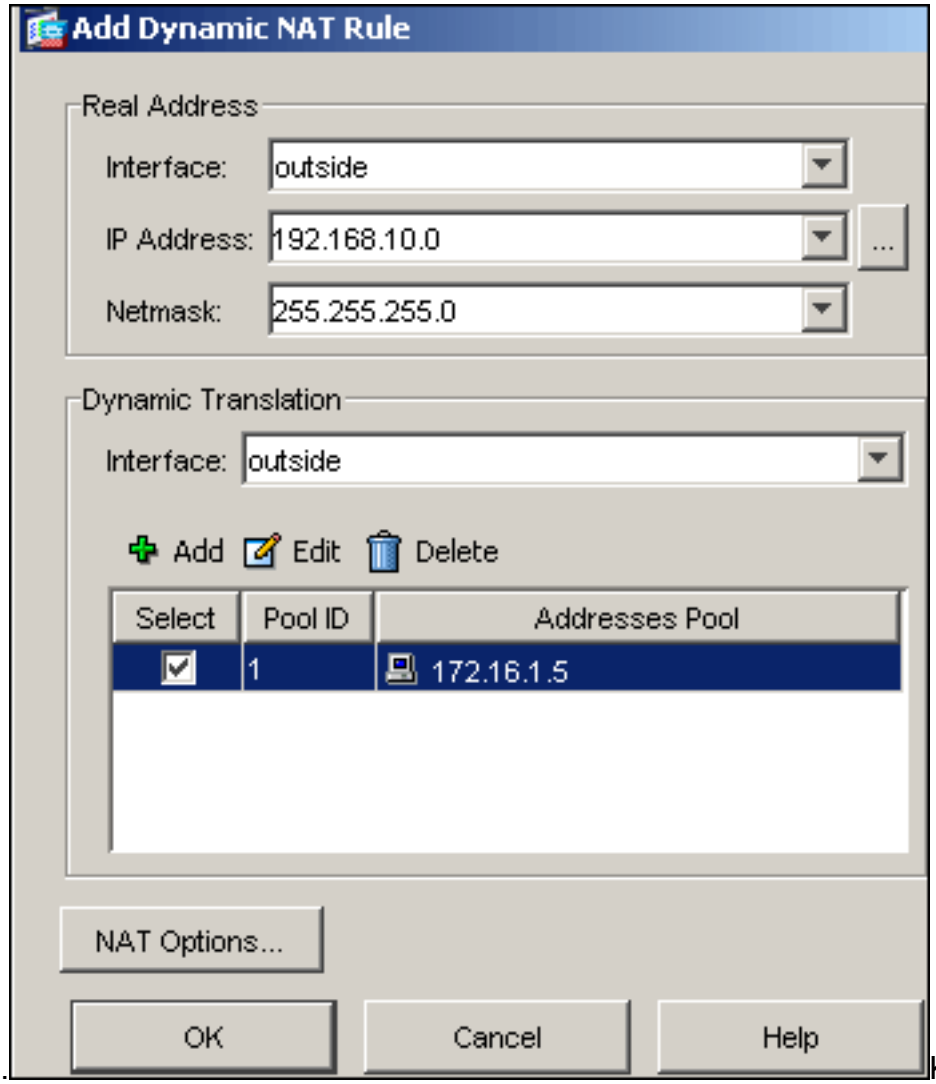
Klik op **OK** en vervolgens op **Toepassen**.**Opmerking:** Hier zijn de gelijkwaardige CLI-configuratieopdrachten:

14. NAT configureren:Kies **Configuration > NAT > Add > Add > Dynamic NAT Rule** om het

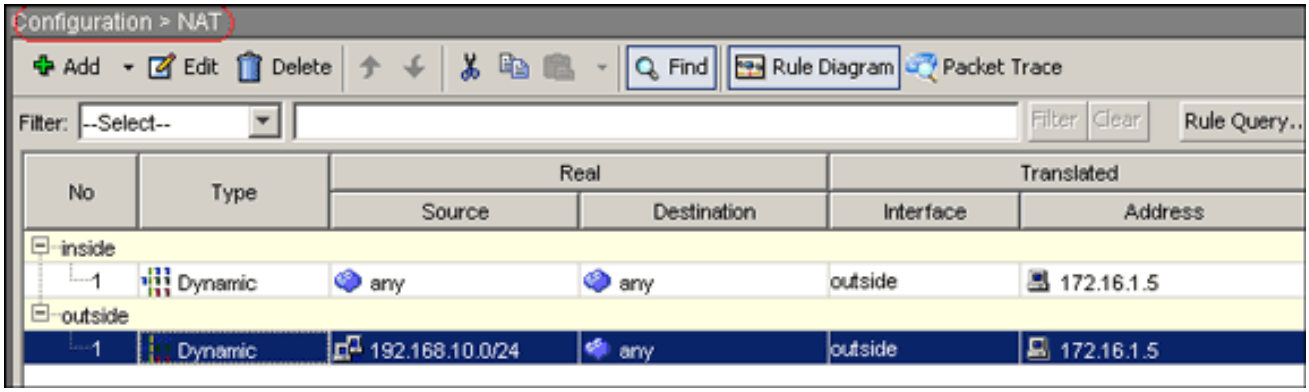
verkeer dat van het binnennetwerk komt toe te laten om met het gebruik van het buitenIP adres 172.16.1.5 te worden



vertaald. Klik op **OK**.Kies **Configuration > NAT > Add > Add > Dynamic NAT Rule** om het verkeer dat van het buitennetwerk 192.168.10.0 komt te vertalen met het gebruik van het buitenIP adres



172.16.1.5. Klik op **OK**.



Klik op **Toepassen**.**Opmerking:** Hier zijn de gelijkwaardige CLI-configuratieopdrachten:

ASA 7.2(2) CLI-configuratie

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
same-security-traffic permit intra-interface

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

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

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

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

access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal
```

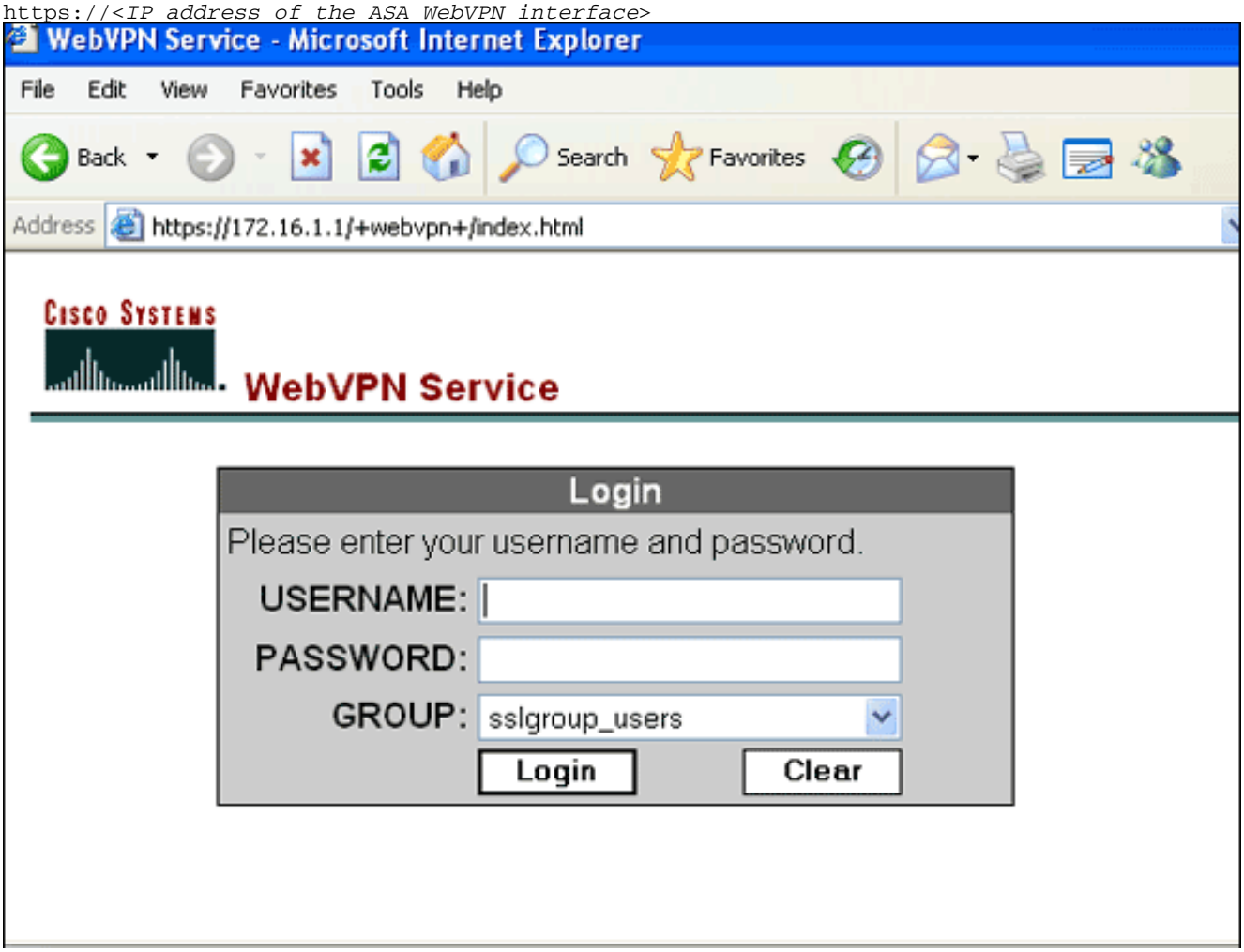
```
!--- Create an internal group policy "clientgroup."
group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

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

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

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

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

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

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

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

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

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

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

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

 group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users. telnet
timeout 5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
webvpn
 enable outside

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

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

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

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

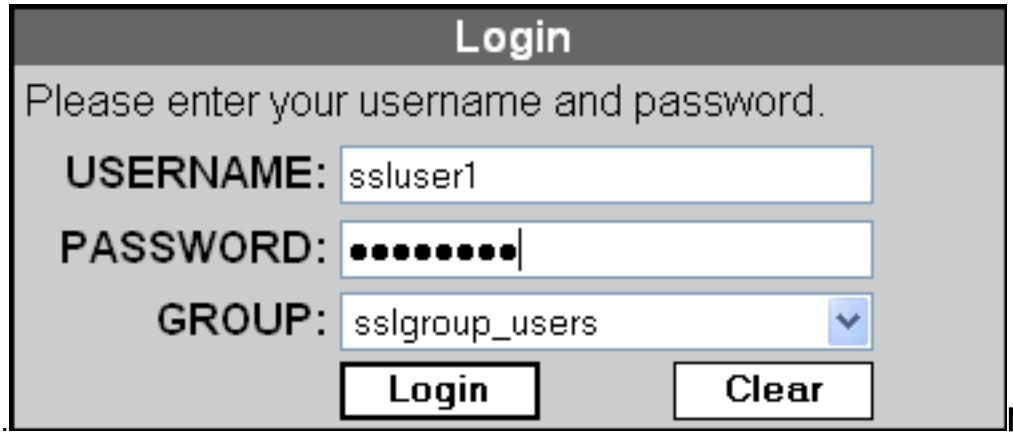
Instellen van de SSL VPN-verbinding met SVC

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

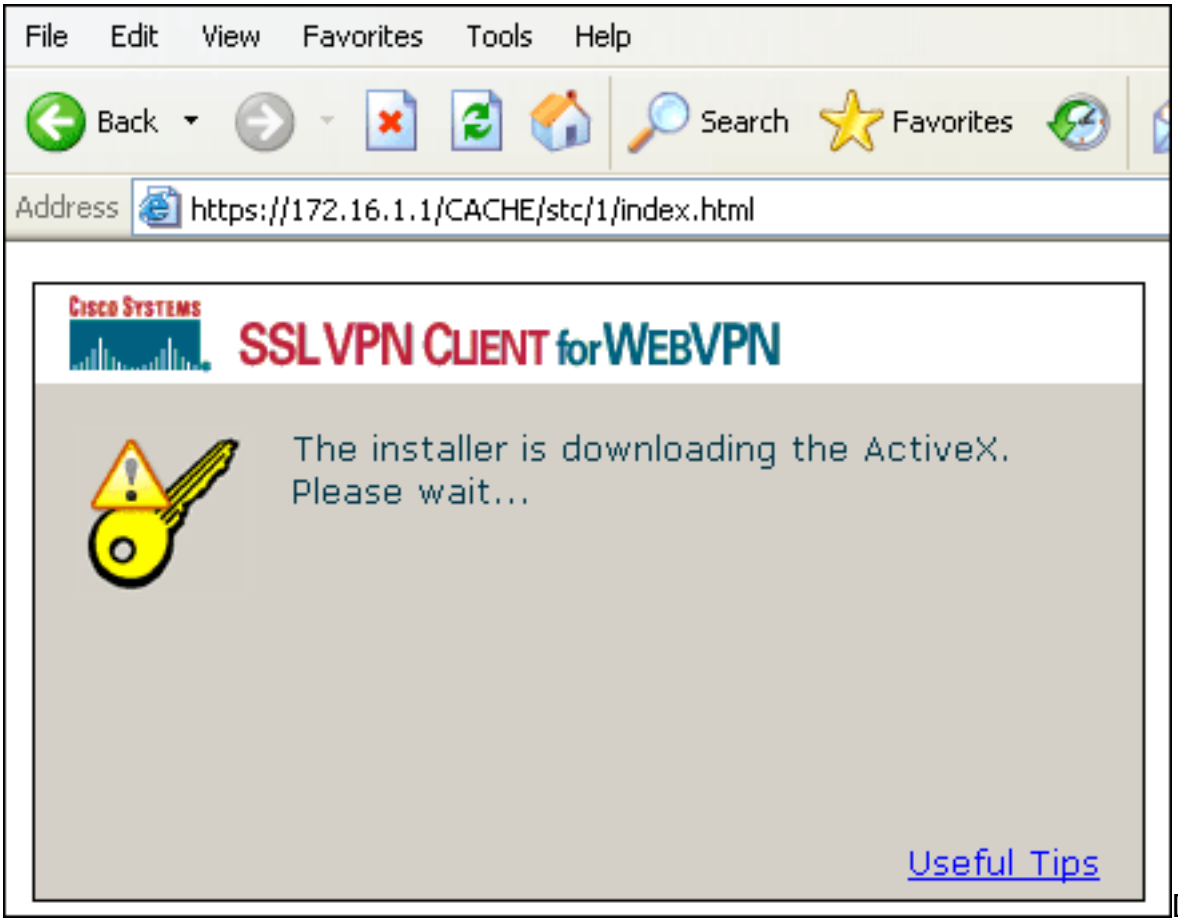
1. Typ in het veld Adres van uw webbrowser het URL- of IP-adres voor de WebVPN-interface van de ASA.Bijvoorbeeld:
   `https://<IP address of the ASA WebVPN interface>`



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



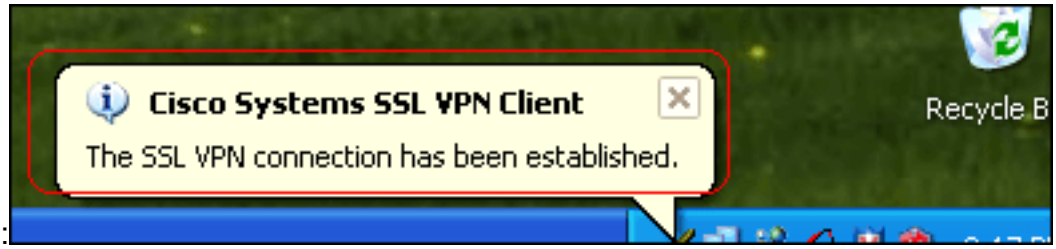
Groep.**N.B.:** ActiveX-software moet in uw computer geïnstalleerd zijn voordat u de SSL VPN-client downloaden.



Dit dialoogvenster verschijnt naarmate de verbinding tot stand is

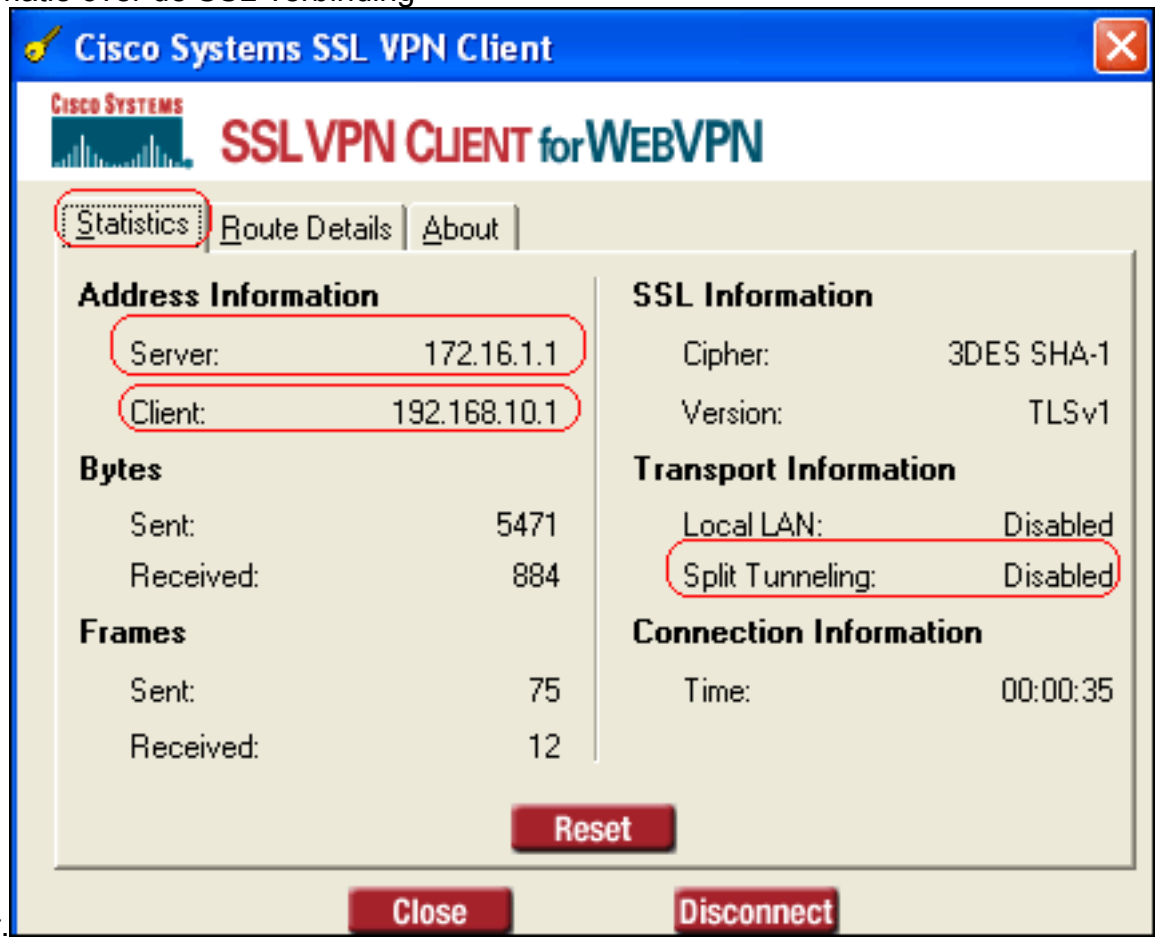
gebracht:Dit bericht verschijnt nadat de verbinding is

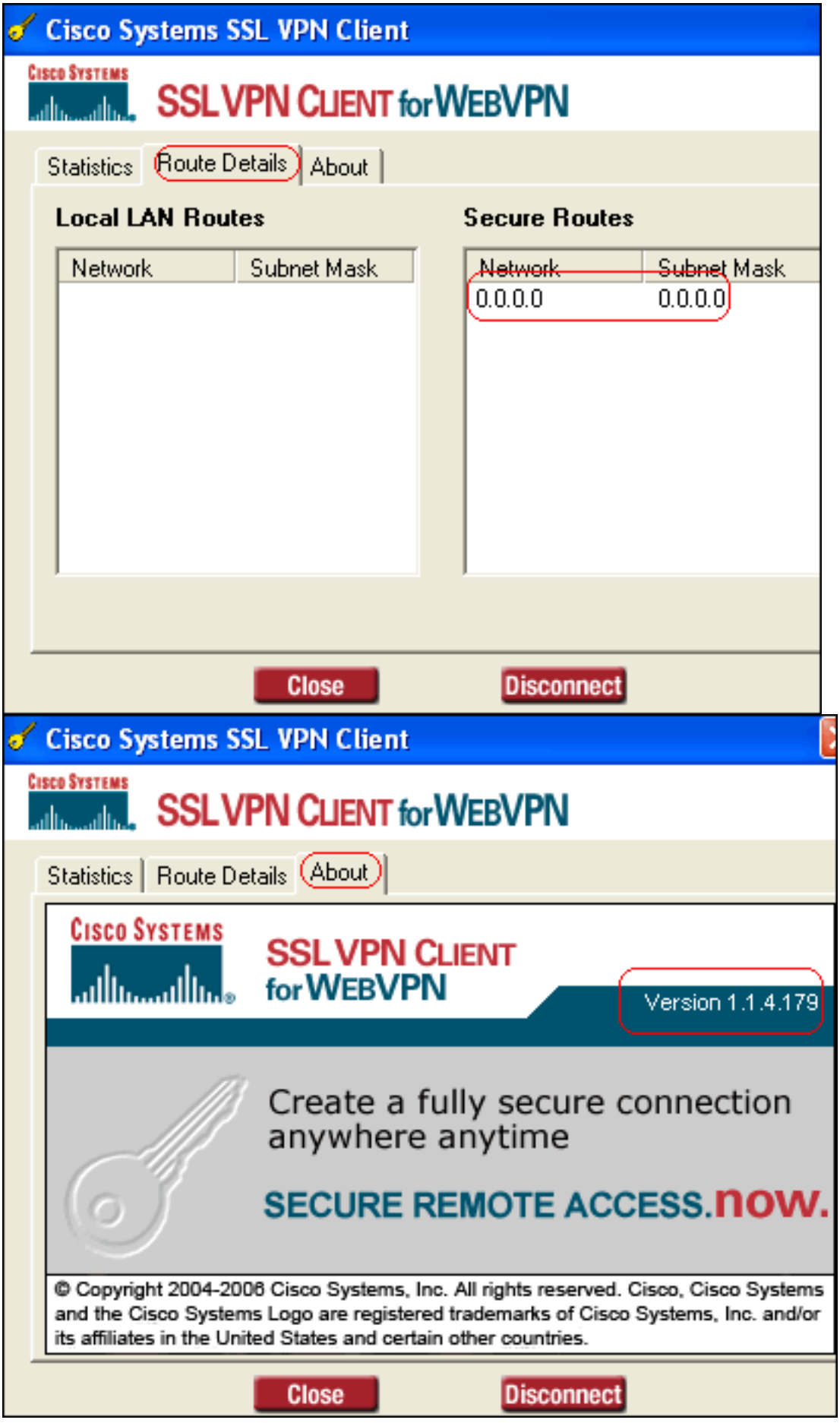
gelegd:



3. Nadat de verbinding is bereikt, dubbelklikt u op het pictogram gele toets dat in de taakbalk van uw computer verschijnt.Het dialoogvenster Cisco Systems SSL VPN-client geeft informatie over de SSL-verbinding

weer.





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
```

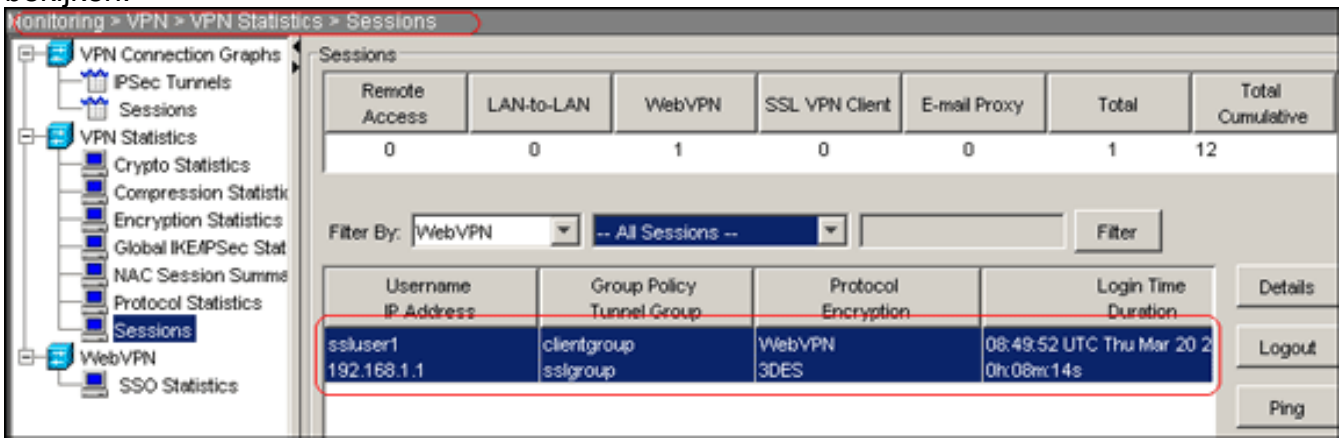
- **toon vpn-sessiondb svc**-Toont de informatie over de huidige SSL verbindingen.

```
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 **Controle > VPN > Statistieken > Sessies** om informatie over de huidige WebVPN sessies in de ASA te bekijken.



Problemen oplossen

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

- Hiermee kunt u **de** SSL VPN-sessie voor de gespecificeerde gebruikersnaam **beëindigen**.

```
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 opdracht **vpn-sessiondb logoff svc** gebruiken om alle SVC-sessies te beëindigen.**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
```

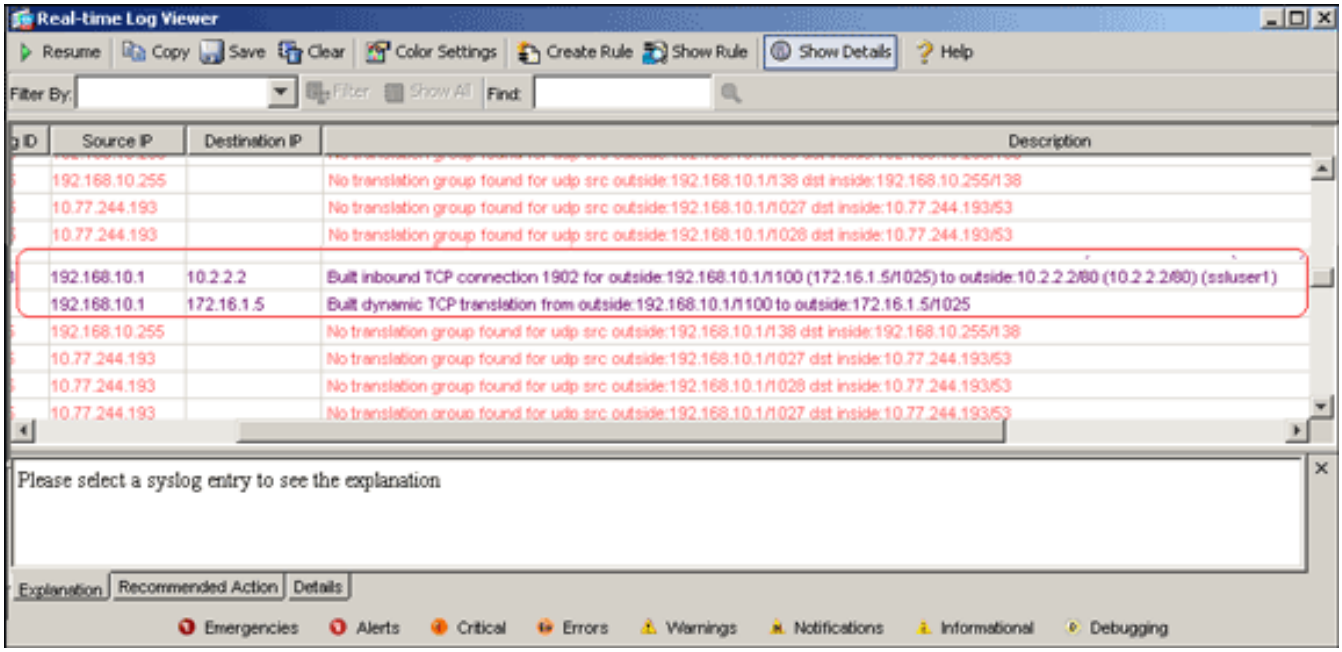
```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

- **Debug WebVPN svc <1-255>**—Biedt de real-time WebVPN-gebeurtenissen om de sessie te maken.

```
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
```

- Kies in ASDM **Bewaking > Vastlegging > Realtime logvenster > Weergave** om de gebeurtenissen in realtime weer te geven. Deze voorbeelden tonen sessieinformatie tussen de 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 ondersteuningspagina voor adaptieve security applicatie
- 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