

ASA 8.x: Split-tunneling voor AnyConnect VPN-client toestaan in het ASA Configuration-voorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[ASA-configuratie met ASDM 6.0\(2\)](#)

[ASA CLI-configuratie](#)

[Instellen van de SSL VPN-verbinding met SVC](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document bevat stap voor stap instructies hoe u Cisco AnyConnect VPN-clienttoegang tot het internet kunt toestaan terwijl ze in een Cisco adaptieve security applicatie (ASA) 8.0.2 zijn geïntegreerd. Deze configuratie maakt de client beveiligde toegang tot bedrijfsmiddelen via SSL mogelijk terwijl u onbeveiligde toegang tot het internet krijgt door middel van gesplitste tunneling.

[Voorwaarden](#)

[Vereisten](#)

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

- ASA security applicatie moet versie 8.x uitvoeren
- Cisco AnyConnect VPN-client 2.x**Opmerking:** Download het AnyConnect VPN-clientpakket (anyconnect-win*.pkg) van de Cisco [Software Download](#) (alleen [geregistreeerde](#) klanten). Kopieer de AnyConnect VPN-client naar het FastHub van de ASA, dat naar de externe gebruikerscomputers moet worden gedownload om de SSL VPN-verbinding met de ASA op te zetten. Raadpleeg het [gedeelte AnyConnect-client](#) van de ASA-configuratiegids voor meer informatie.

Gebruikte componenten

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

- Cisco 5500 Series ASA-software met versie 8.0(2)
- Cisco AnyConnect SSL VPN-clientversie voor Windows 2.0.343
- PC met Microsoft Vista, Windows XP SP2 of Windows 2000 Professional SP4 met Microsoft Installer versie 3.1
- Cisco Adaptieve Security Devices Manager (ASDM) versie 6.0(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 Cisco AnyConnect VPN-client biedt beveiligde SSL-verbindingen naar het beveiligingsapparaat voor externe gebruikers. Zonder een eerder geïnstalleerde client gaan externe gebruikers het IP-adres in hun browser in van een interface die is geconfigureerd om SSL VPN-verbindingen te accepteren. Tenzij het beveiligingsapparaat is ingesteld om http://-verzoeken om te zetten naar https://, moeten gebruikers de URL in het formulier https://<adres> invoeren.

Nadat u de URL hebt ingevoerd, sluit de browser zich aan op die interface en geeft deze het inlogschermbanner weer. Als de gebruiker voldoet aan de inlognaam en de verificatie en het security apparaat de gebruiker identificeert als de client, wordt de client gedownload die overeenkomt met het besturingssysteem van de externe computer. Na het downloaden, installeert en vormt de client zichzelf, stelt een beveiligde SSL-verbinding in en wordt of blijft of wordt zelf geïnstalleerd (afhankelijk van de configuratie van het beveiligingsapparaat) wanneer de verbinding wordt beëindigd.

In het geval van een eerder geïnstalleerde client, wanneer de gebruiker echt is, onderzoekt het beveiligingsapparaat de herziening van de client en upgrades van de client indien nodig.

Wanneer de client onderhandelt over een SSL VPN-verbinding met het security apparaat, sluit de client verbindingen met behulp van Transport Layer Security (TLS) en naar keuze Datagram Transport Layer Security (DTLS). DTLS vermijdt latentie- en bandbreedteproblemen verbonden aan sommige SSL verbindingen, en verbetert de prestaties van real-time toepassingen die gevoelig zijn voor pakketvertragingen.

De AnyConnect-client kan van het beveiligingsapparaat worden gedownload of door de systeembeheerder handmatig op de externe pc worden geïnstalleerd. Raadpleeg de [Cisco AnyConnect VPN-clientbeheerdershandleiding](#) voor meer informatie over het handmatig installeren van de client.

Het beveiligingsapparaat downloads de client op basis van het groepsbeleid of de gebruikersnaameigenschappen van de gebruiker die de verbinding vormt. U kunt het

beveiligingsapparaat configureren om de client automatisch te downloaden of u kunt de client configureren om de gebruiker te vragen of u de client wilt downloaden. In het laatste geval, als de gebruiker niet reageert, kunt u het security apparaat configureren om de client na een tijdelijke versie te downloaden of de inlogpagina weer te geven.

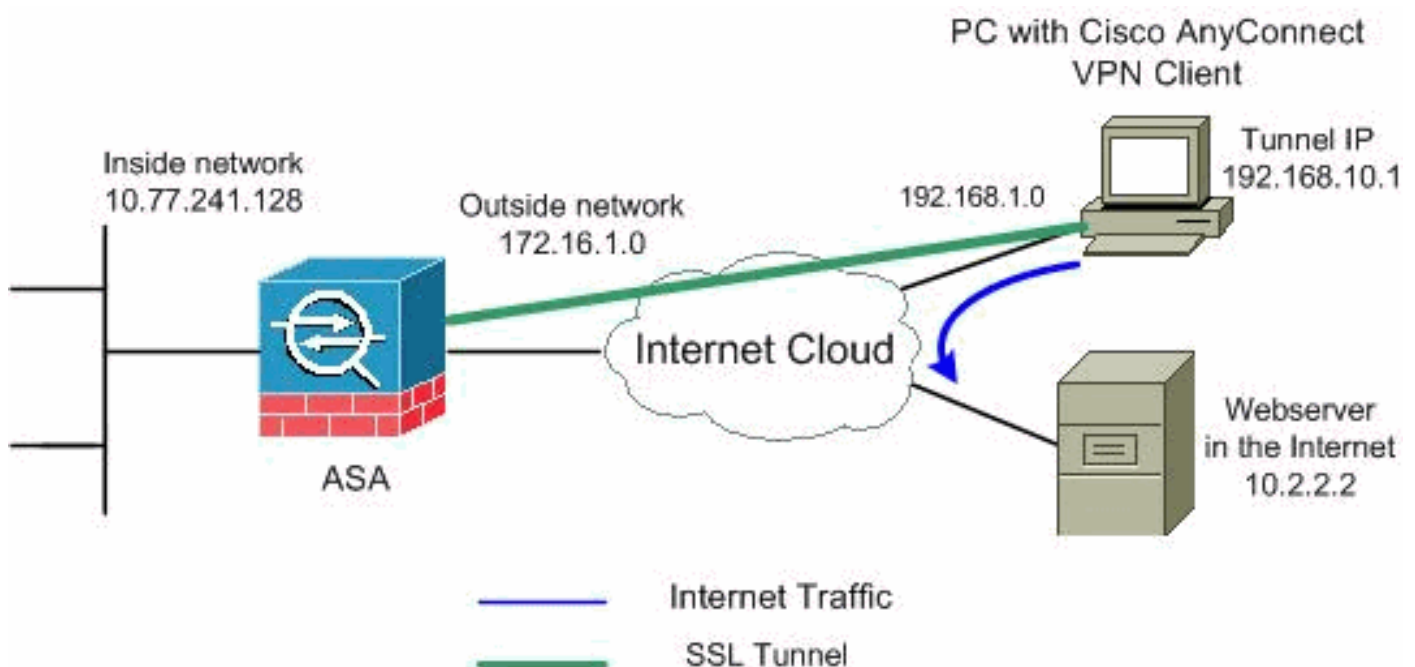
Configureren

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.

Netwerkdigram

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-configuratie met ASDM 6.0(2)

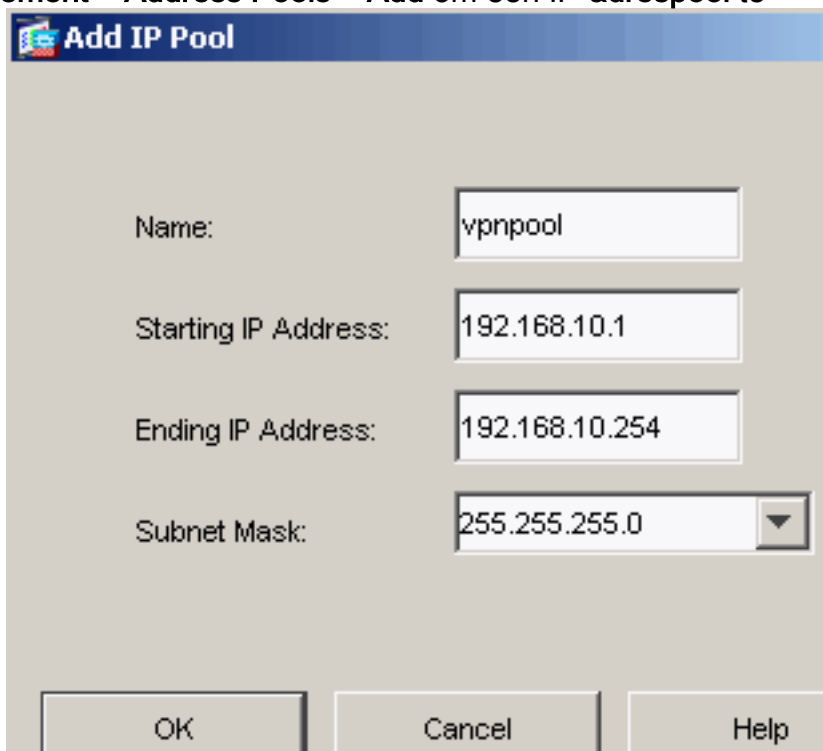
Dit document gaat ervan uit dat de basisconfiguratie, zoals de interfaceconfiguratie, al is gemaakt en correct werkt.

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.

Voltooi deze stappen om SSL VPN op ASA met gesplitste tunneling te configureren:

1. Kies **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add** om een IP-adrespool te



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 at the bottom: OK, Cancel, Help

maken.

2. Klik op **Apply** (Toepassen). **Compatibele CLI-configuratie:**
3. Webex inschakelen. Kies **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN-verbindingsprofielen** en klik onder **Access-interfaces** op de vinkjes **Toegang toestaan** en **DTLS** inschakelen voor de externe interface. Controleer ook de **toegang tot Cisco AnyConnect VPN-client** of **oudere SSL VPN-client** in de interface die in de onderstaande tabel is geselecteerd om SSL VPN op de externe interface mogelijk te maken.

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

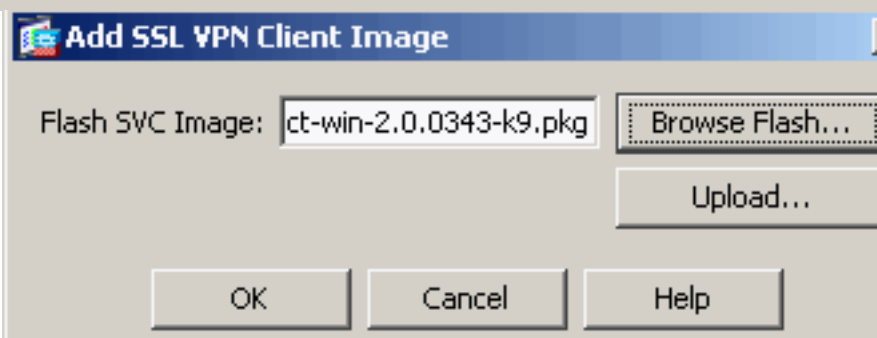
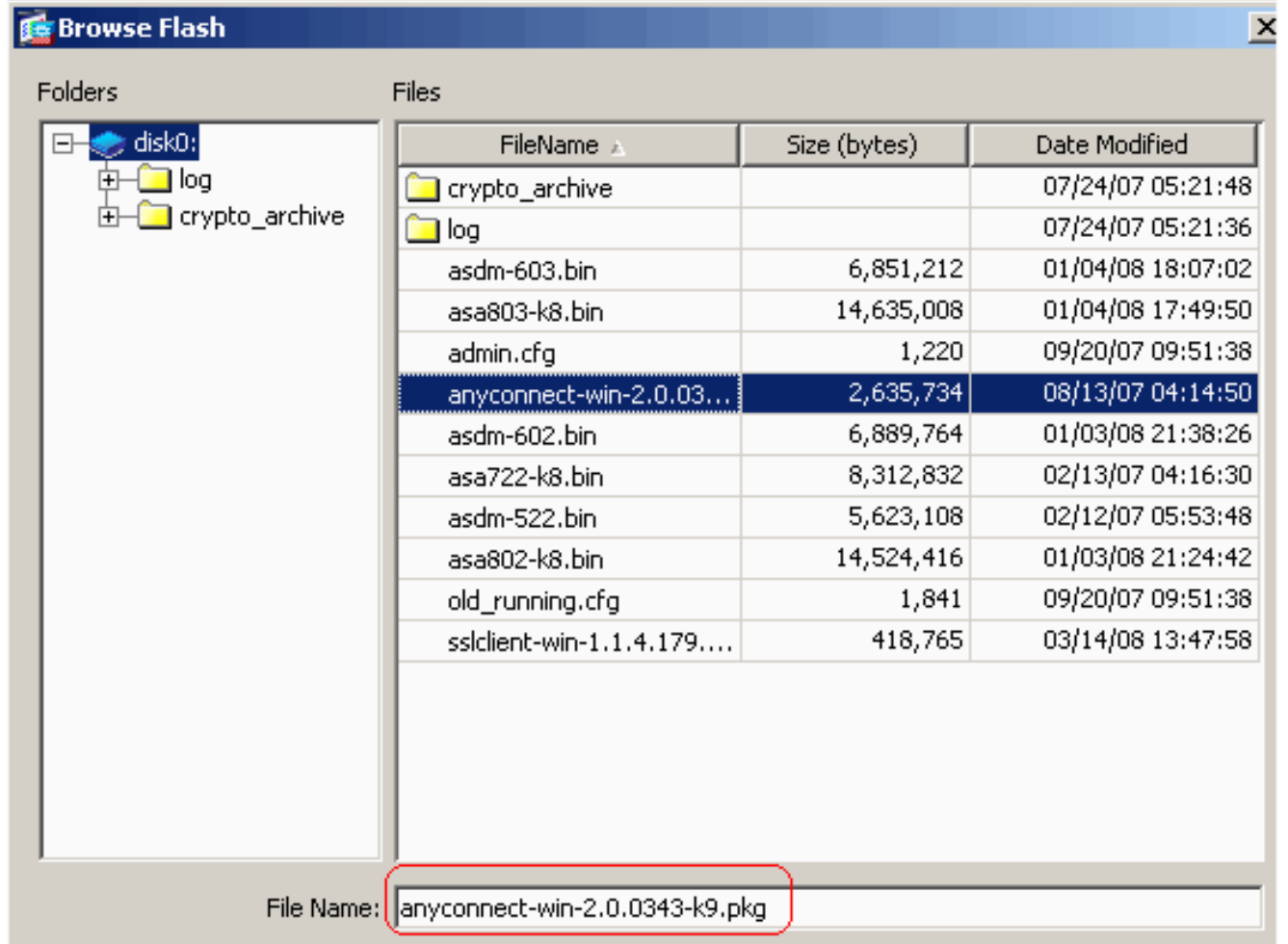
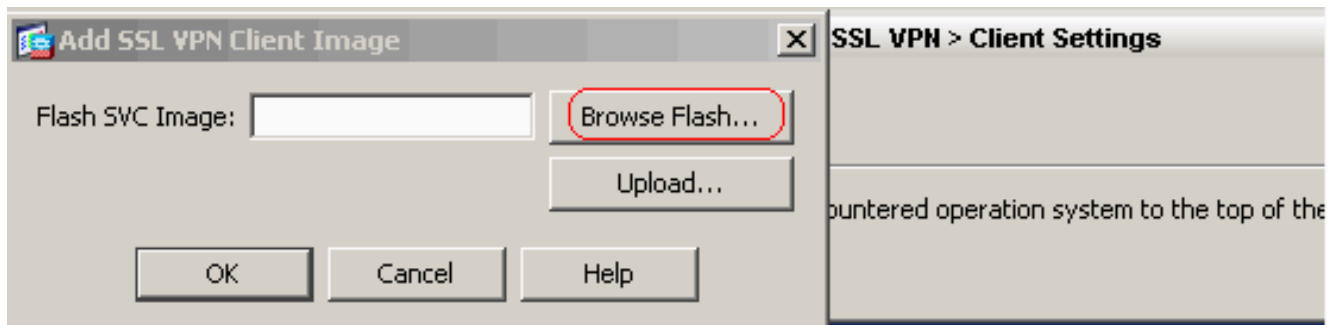
Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

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:

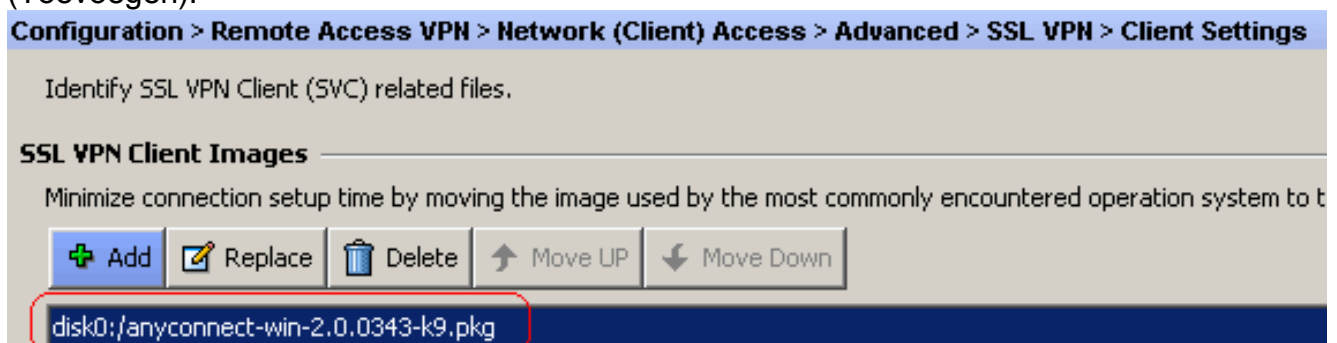
Click here to [Assign Certificate to Interface](#).

Klik op **Apply** (Toepassen). Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Clientinstellingen > Add** om het Cisco AnyConnect VPN-clientbeeld uit het flash-geheugen van ASA toe te voegen zoals wordt weergegeven.



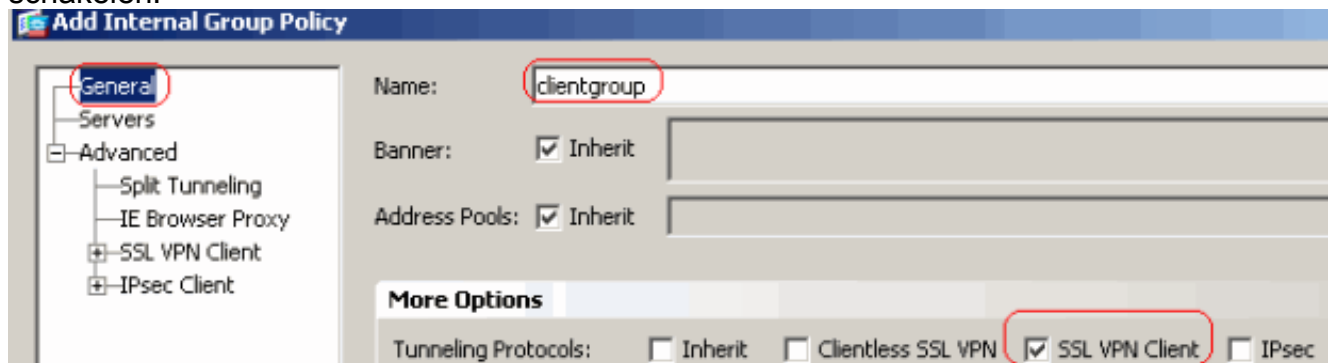
Klik op OK.
(Toevoegen).

Klik op Add

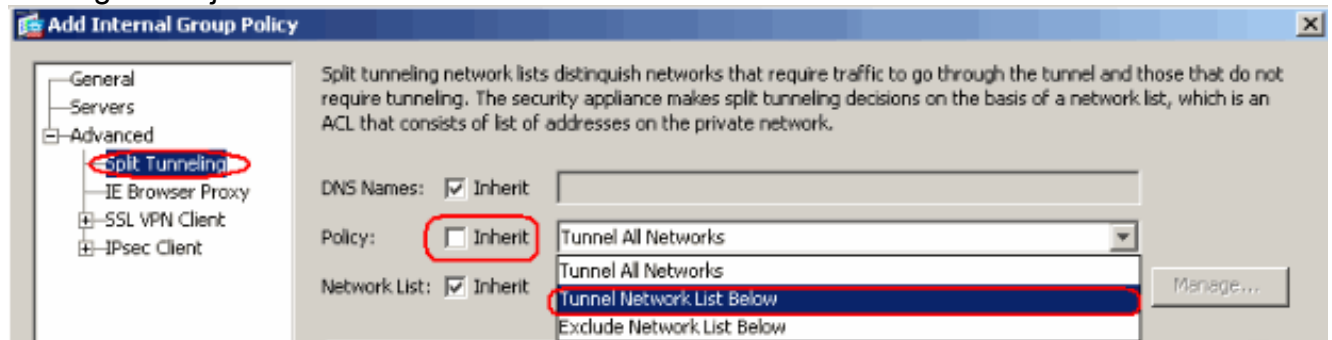


Compatibele CLI-configuratie:

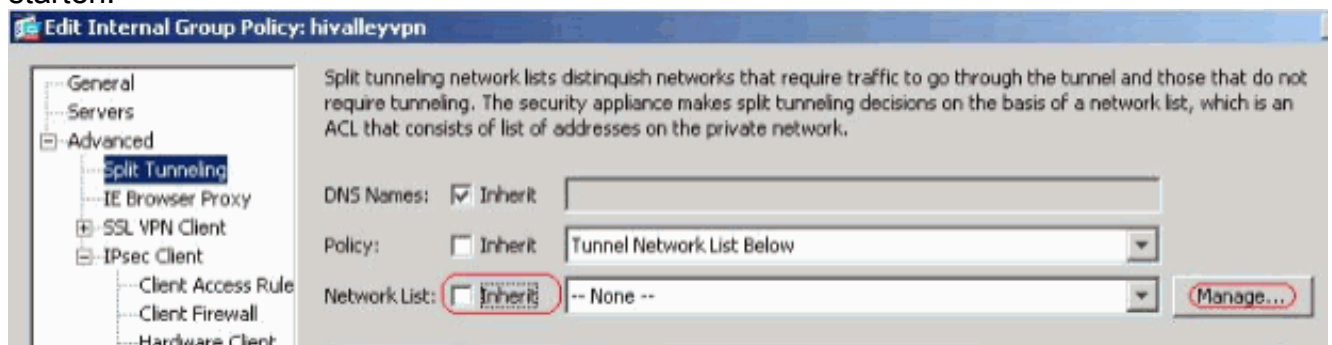
4. Groepsbeleid configureren Kies **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** om een interne **clientgroep** voor groepsbeleid te maken. Selecteer onder het tabblad **Algemeen** het dialogvenster **SSL VPN-client** om Webex als tunneling-protocol in te schakelen.



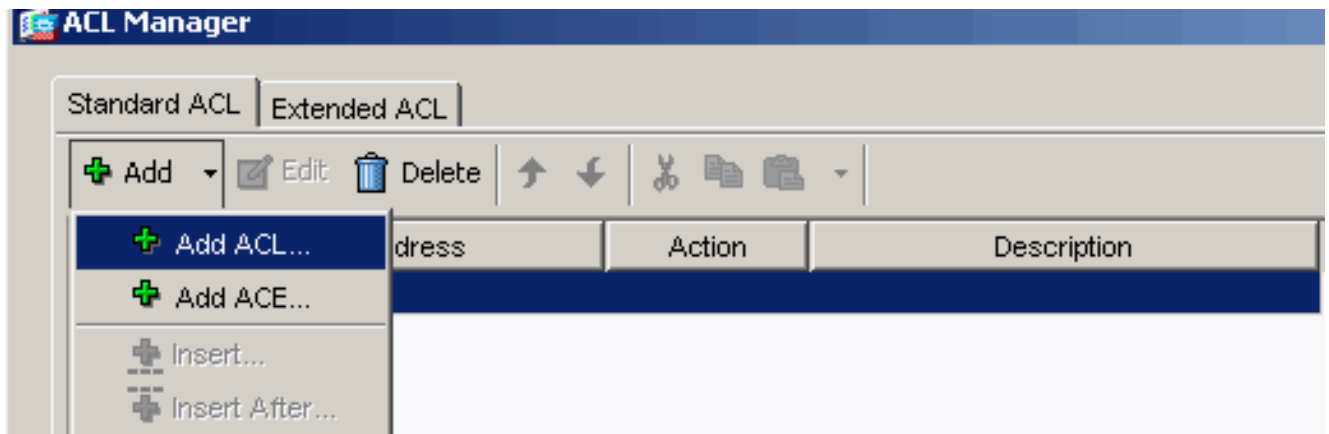
In het tabblad **Geavanceerd > Tunneling splitsen**, schakelt u het vakje **Inherit** uit voor Split Tunnel Policy en kiest u de onderstaande lijst voor **tunnelnetwerk** uit de vervolgkeuzelijst.



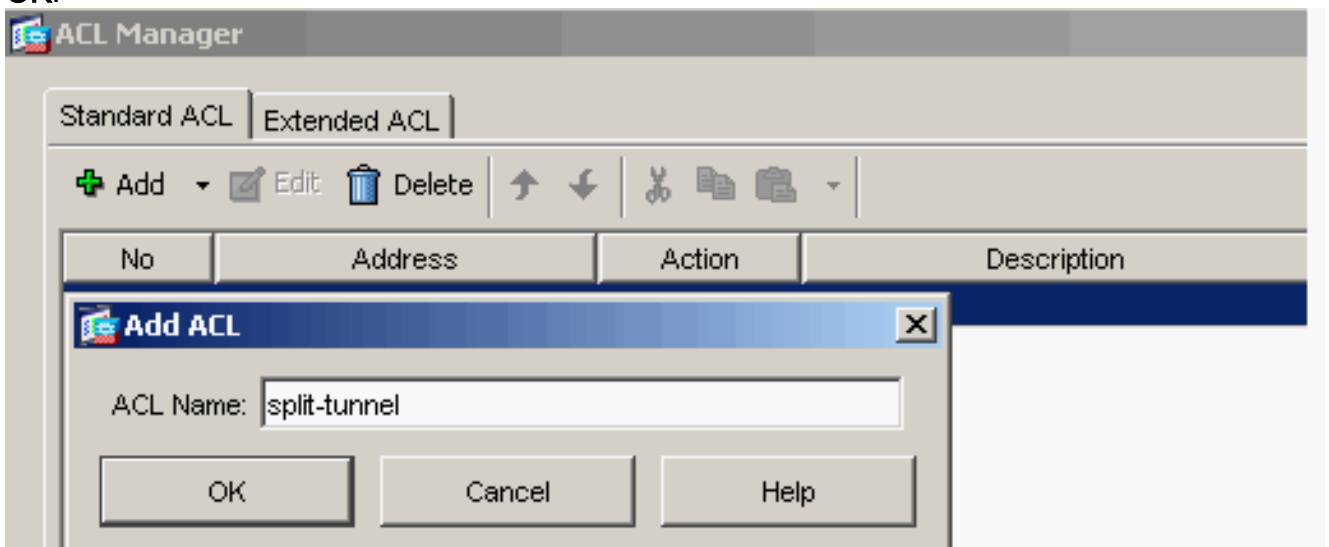
Schakel het vakje **Inherit** uit voor de **netwerklijst Split Tunnel** en klik vervolgens op **Manager beheren** om de ACL Manager te starten.



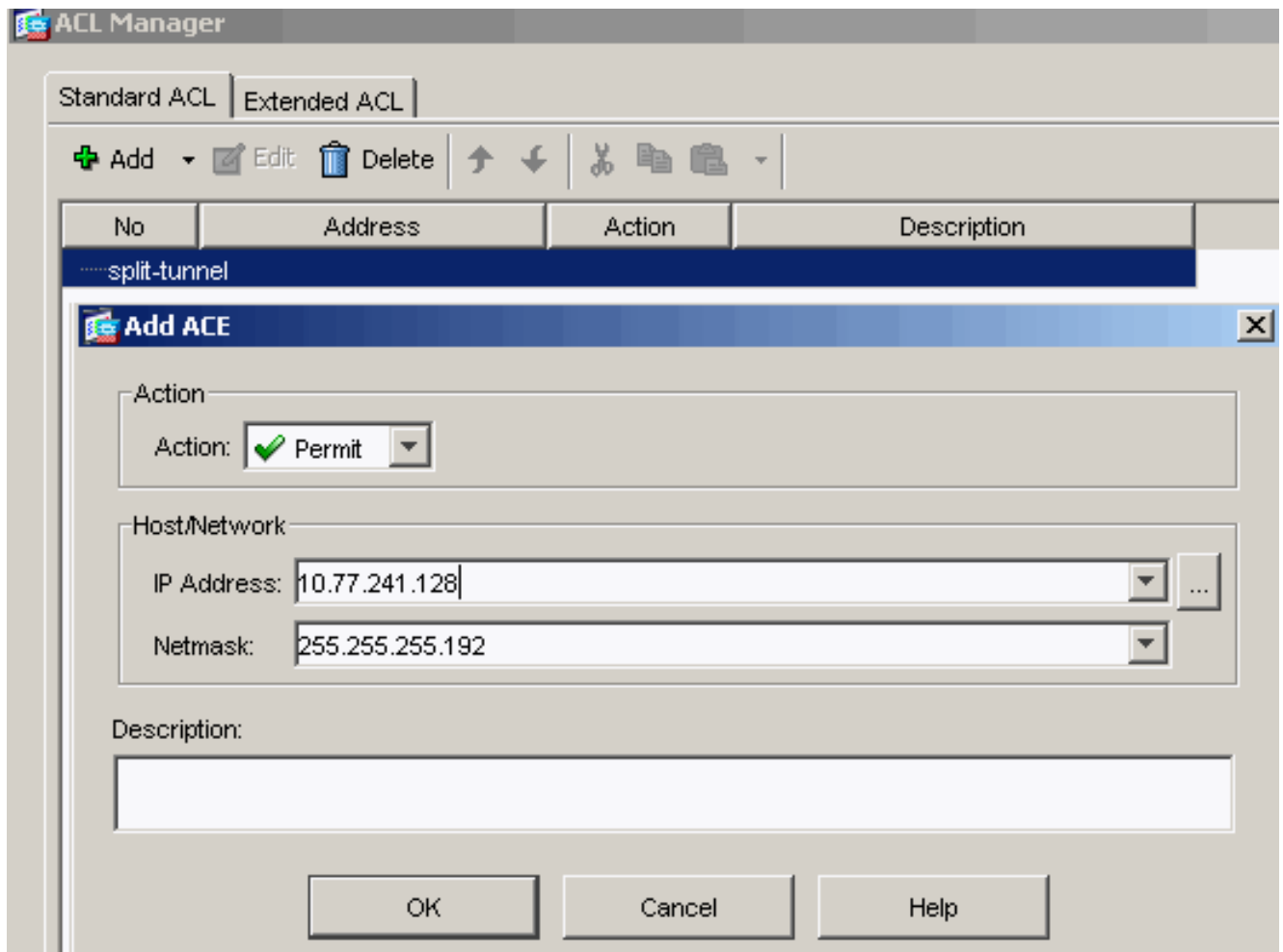
Kies in de ACL Manager **Add > Add ACL...** om een nieuwe toegangslijst te maken.



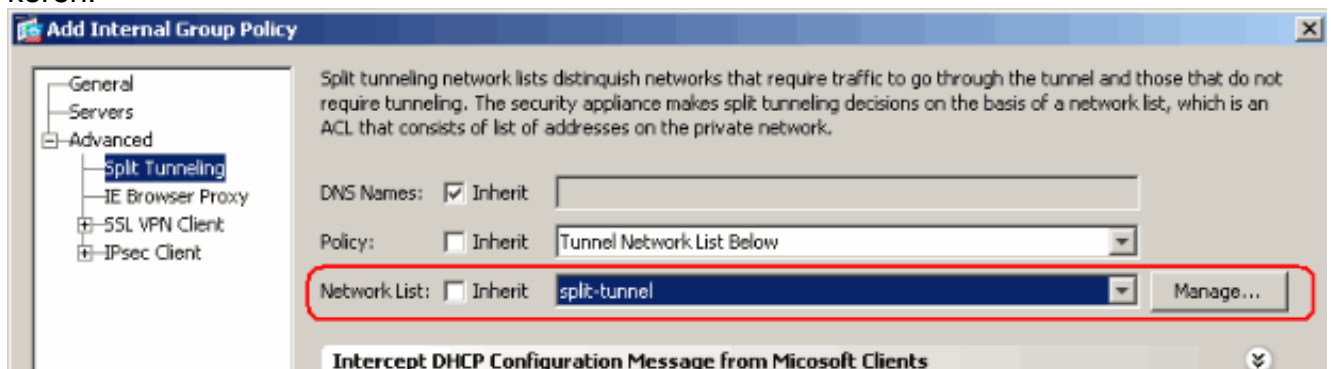
Typ een naam voor ACL en klik op OK.



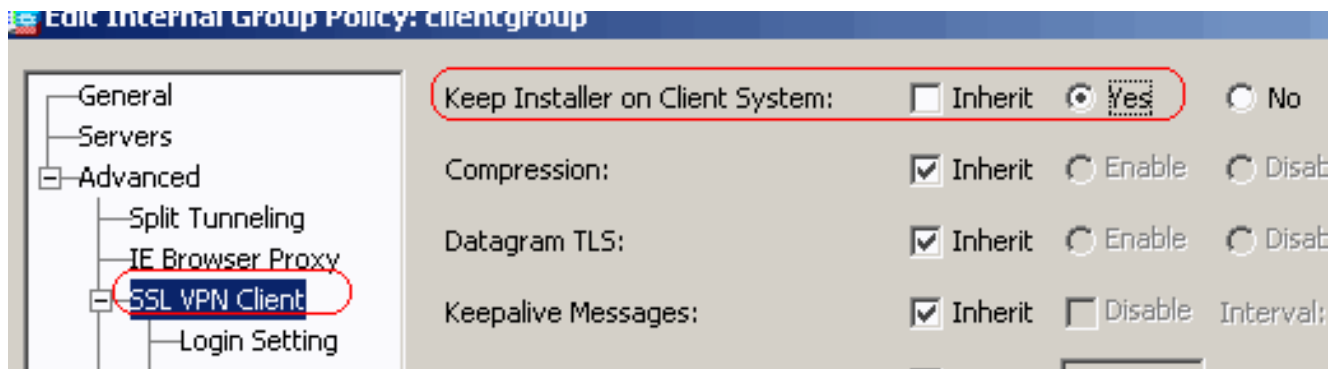
Zodra de ACL-naam is gemaakt, kiest u **Add > Add ACE** om een Access Control Entry (ACE) toe te voegen. Definieer de ACE die overeenkomt met het LAN achter de ASA. In dit geval is het netwerk 10.77.241.128/26 en selecteert u **Toestemming** als de Actie. Klik op **OK** om de ACL-Manager te verlaten.



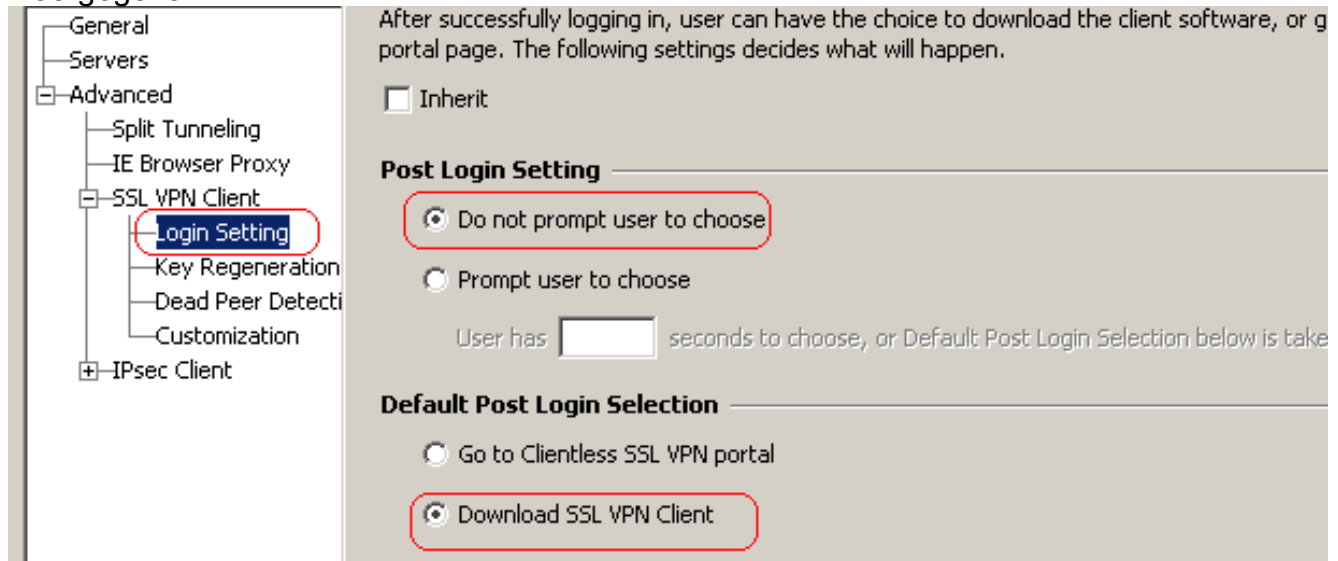
Zorg ervoor dat ACL die u zojuist hebt gemaakt, is geselecteerd voor de lijst van gesplitste tunnels. Klik op **OK** om naar de configuratie van het groepsbeleid terug te keren.



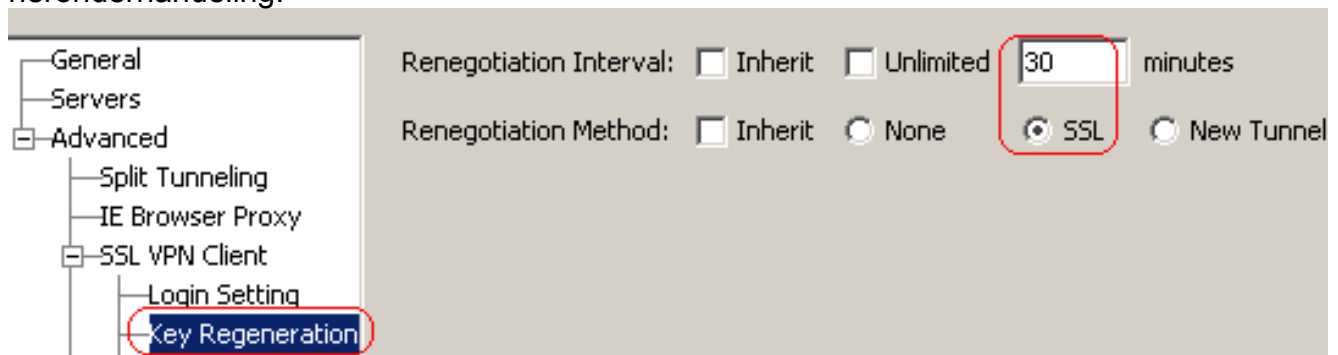
Klik op de hoofdpagina op **Toepassen** en stuur de opdrachten (indien nodig) naar de ASA door. Configureer de **SSL VPN**-instellingen onder de modus groepsbeleid. Schakel het vakje **Inherit uit** voor de optie Installeren bij clientsysteem en klik vervolgens op het radioknop **Ja**. Met deze actie 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.



Klik op **Aanmelden** om de inloginstelling voor **Post** in te stellen en de selectie voor **standaardmelding** zoals wordt weergegeven.






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 door limieten in te stellen aan de tijdsduur die een sleutel 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.



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

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.

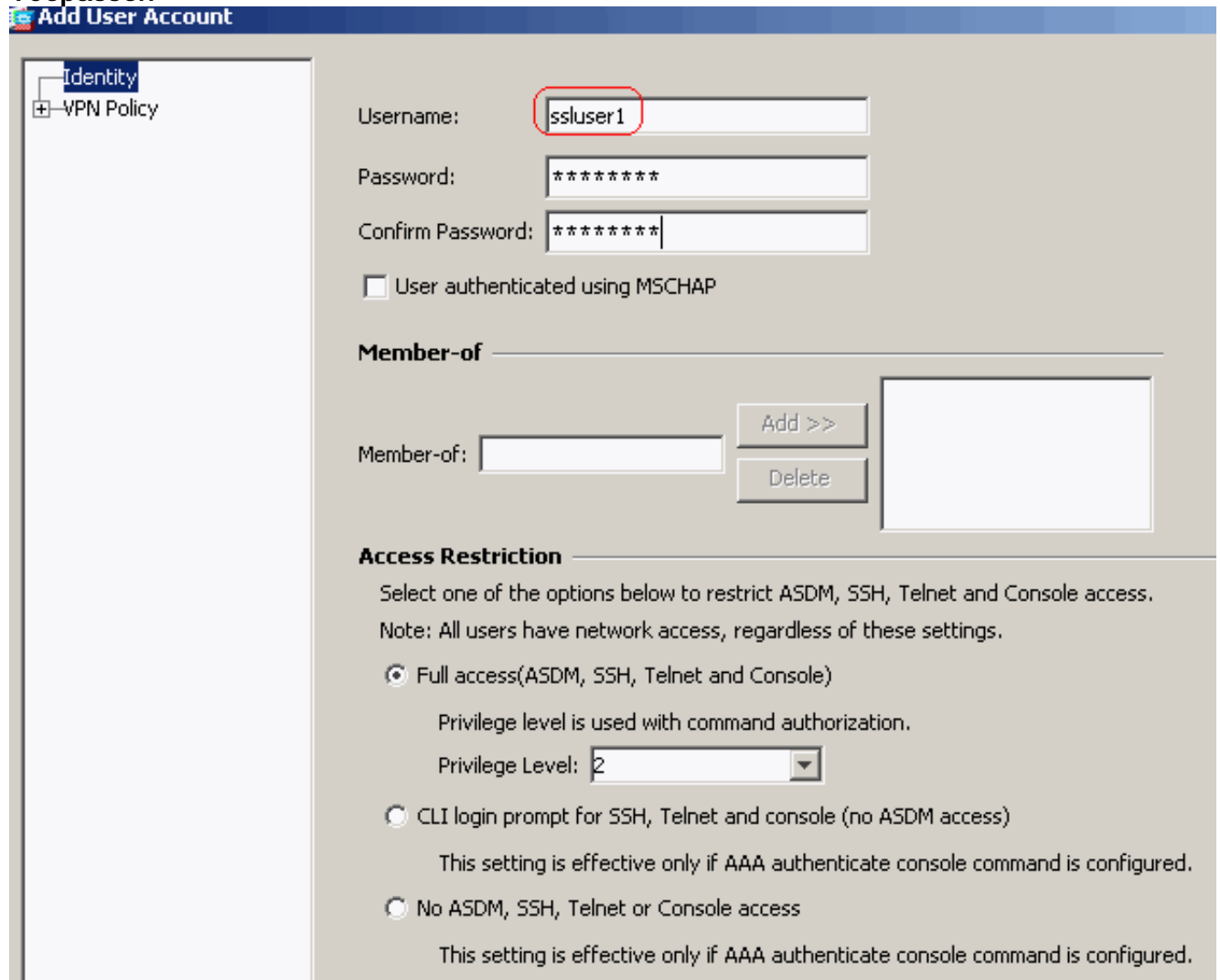
 Add  Edit  Delete

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

Compatibele CLI-configuratie:

5. Kies **Configuration > Remote Access VPN > AAA-instelling > Local Gebruikers > Add** om een nieuwe gebruiker-account **gebruiker1** te maken. Klik op **OK** en

Toepassen.



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.

Compatibele CLI-configuratie:

6. Kies **Configuration > Remote Access VPN > AAA-servergroepen > AAA-servers > Bewerken** om de standaardservergroep **LOCAL** aan te passen door het aanvinkvakje **Local User Lockout** inschakelen te **controleren** met de maximale probewaarde **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. Klik op **OK** en vervolgens op **Toepassen**. **Compatibele CLI-configuratie:**

8. Tunnelgroep configureren Kies **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection profielen > Add** om een nieuwe groep tunnelgroepen te maken. In het tabblad **Basic** kunt u de lijst met configuraties uitvoeren zoals wordt weergegeven: Geef de tunnelgroep een naam als **groep**. Kies onder Clientadrestoewijzing het **vpn** van de adrespool in de vervolgkeuzelijst. Selecteer onder Standaardgroepsbeleid de **clientgroep** voor groepsbeleid uit de vervolgkeuzelijst.

Add SSL VPN Connection Profile

Basic (selected) | Advanced

Name:

Aliases:

Authentication

Method: AAA Certificate Both

AAA Server Group: Manage

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools: Select

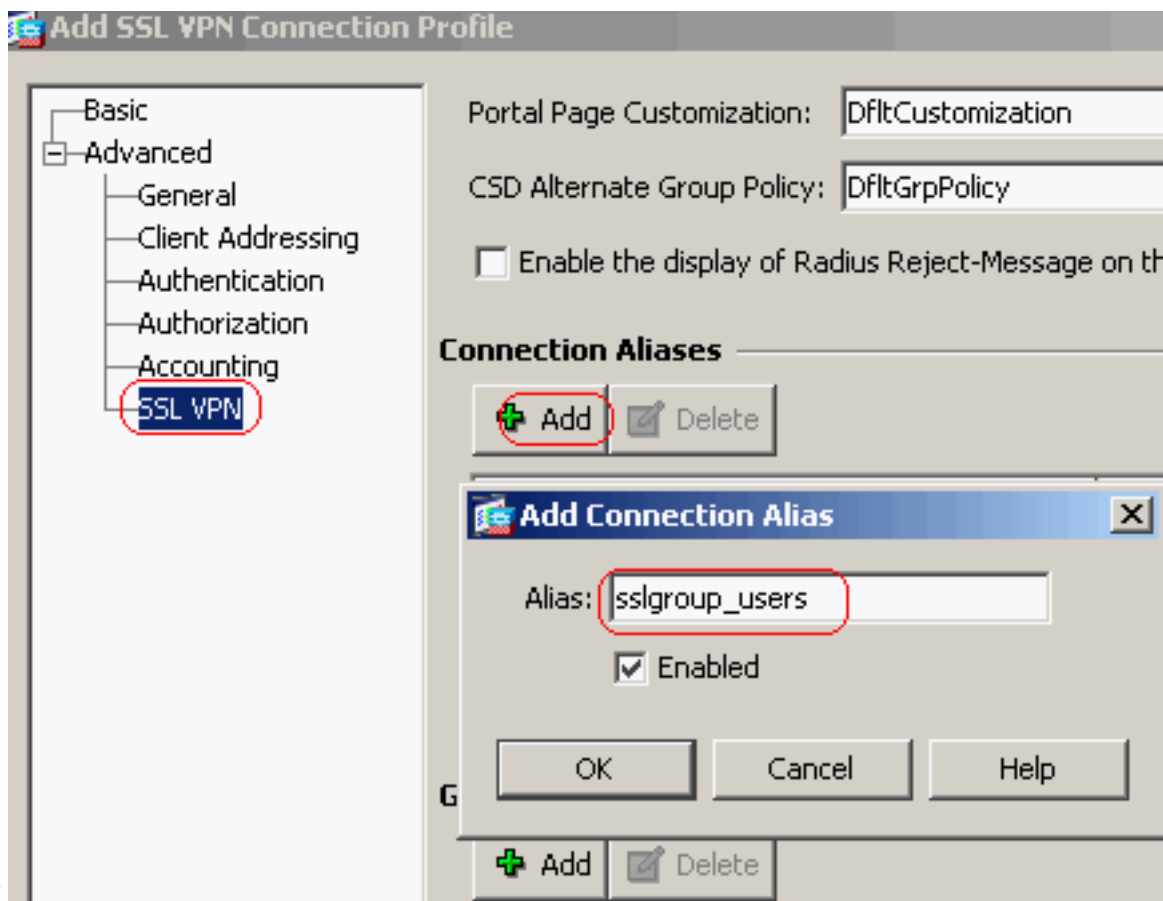
Default Group Policy

Group Policy: Manage

SSL VPN Client Protocol: Enabled

OK Cancel Help

Specificeer onder het tabblad **SSL VPN > Connection Aliases** de naam van de groep als **sslgroup_user** en klik op

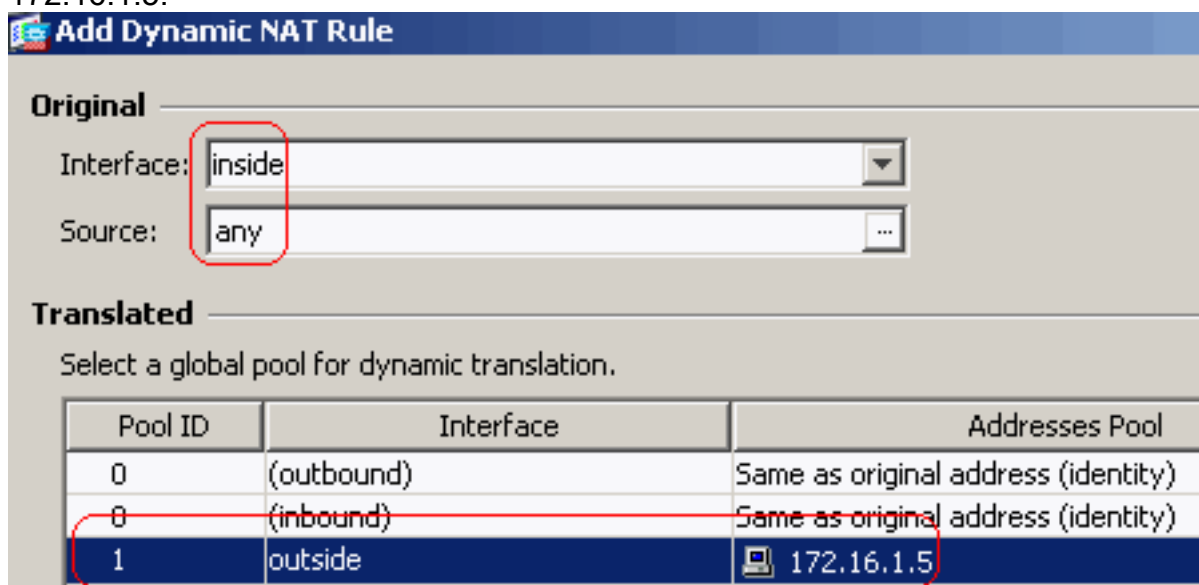


OK.

Klik op

OK en vervolgens op Toepassen. Compatibele CLI-configuratie:

9. Configuratie NAT. Kies Configuratie > Firewall > NAT-regels > Dynamische NAT-regel toevoegen zodat het verkeer dat afkomstig is van het interne netwerk kan worden vertaald met extern IP-adres 172.16.1.5.



Klik op

OK. Klik op

OK.

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

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

10. 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 CLI-configuratie](#)

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)#

```

Instellen van de SSL VPN-verbinding met SVC

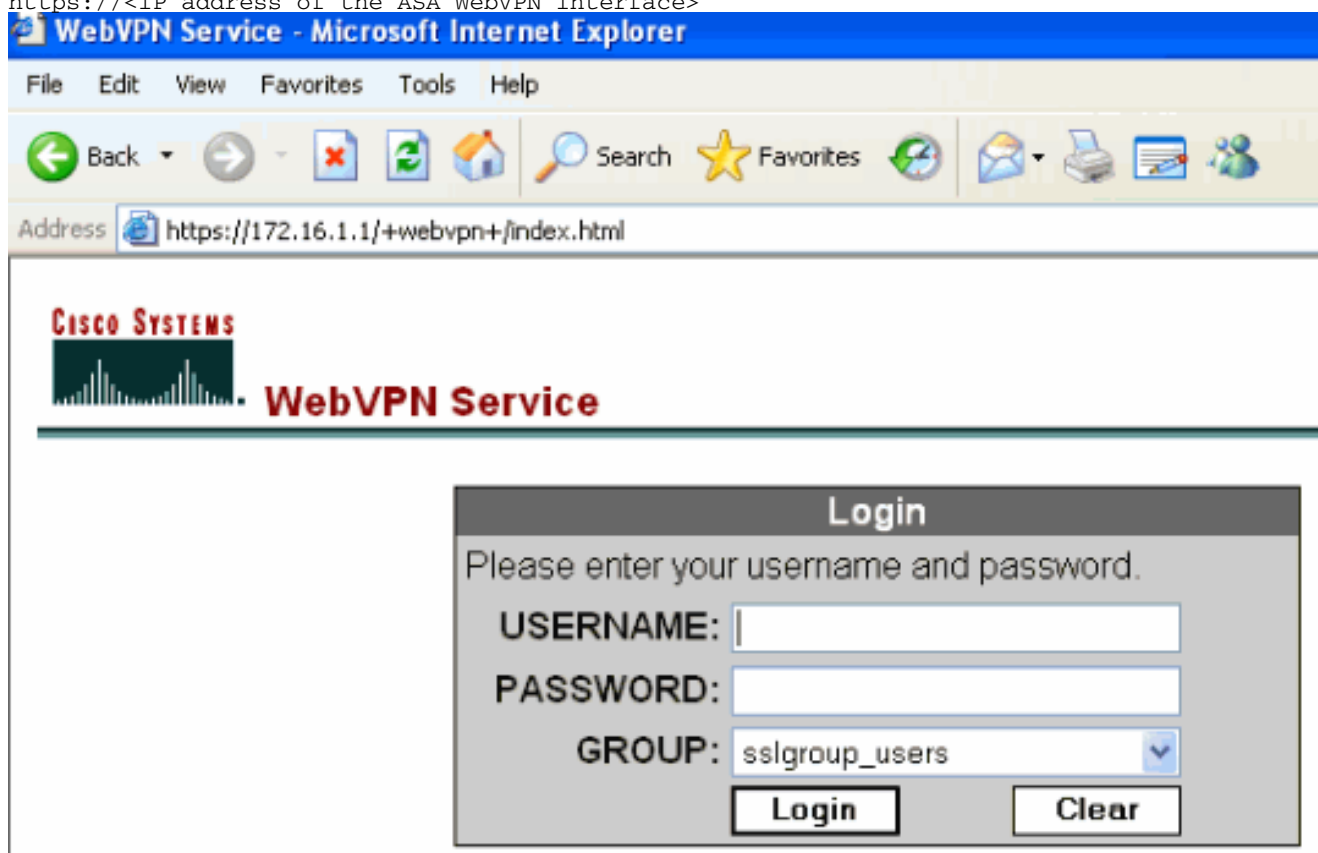
Voltooi deze stappen om een SSL VPN-verbinding met ASA op te zetten:

1. Voer het URL- of IP-adres in van de ASA WebVPN-interface in uw webbrowser in de notatie zoals getoond.

https://url

OF

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



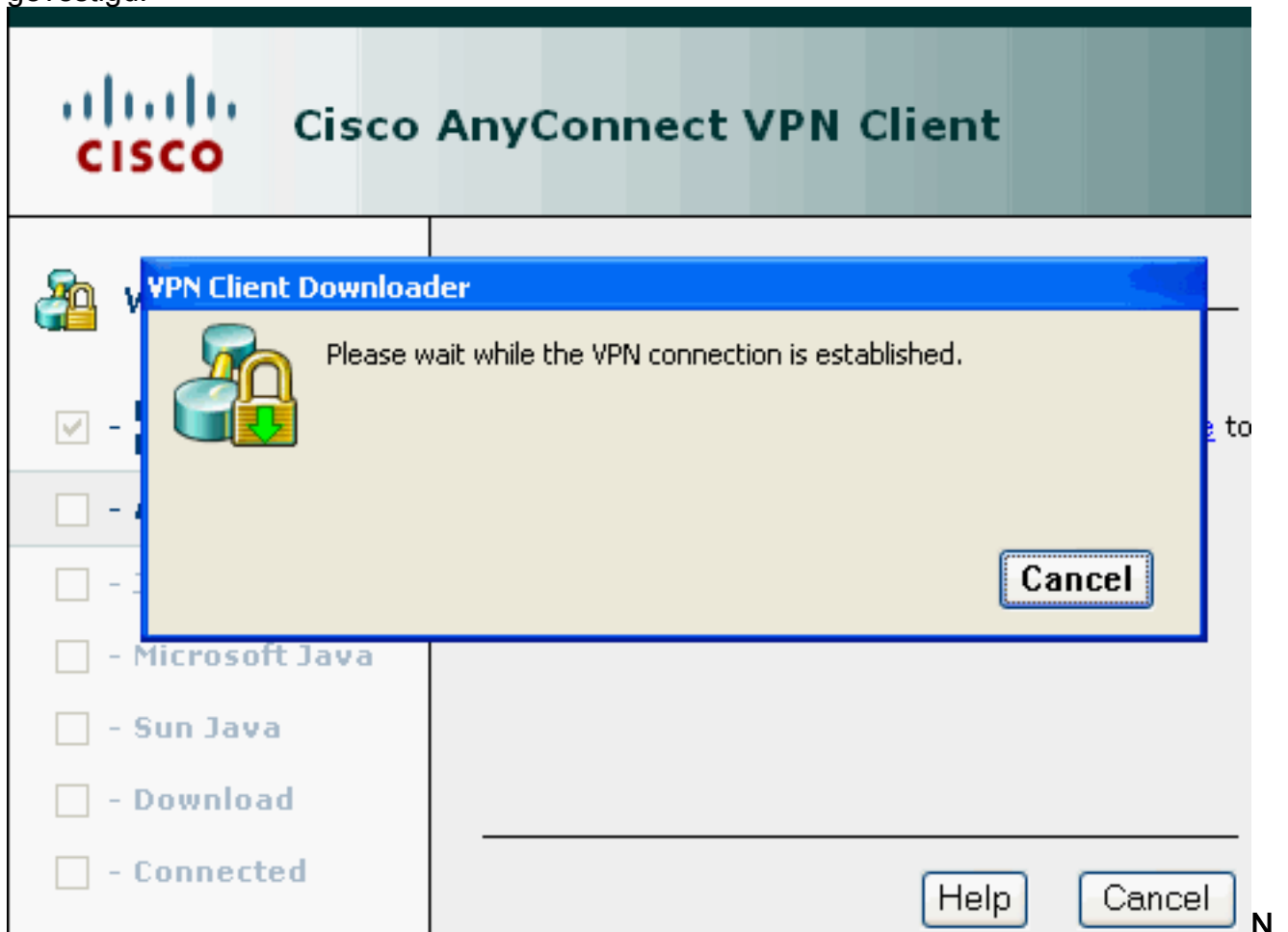
2. Voer uw gebruikersnaam en wachtwoord in. Kies ook uw respectievelijke groep in de vervolgkeuzelijst zoals

weergegeven.

venster verschijnt voordat de SSL VPN-verbinding is

Dit

gevestigd.



.B.: ActiveX-software moet op uw computer geïnstalleerd zijn voordat u de SVC downloaden.U ontvangt dit venster zodra de verbinding is tot stand gebracht.



Cisco AnyConnect VPN Client



WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Microsoft Java
- Sun Java
- Download
- Connected

Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:



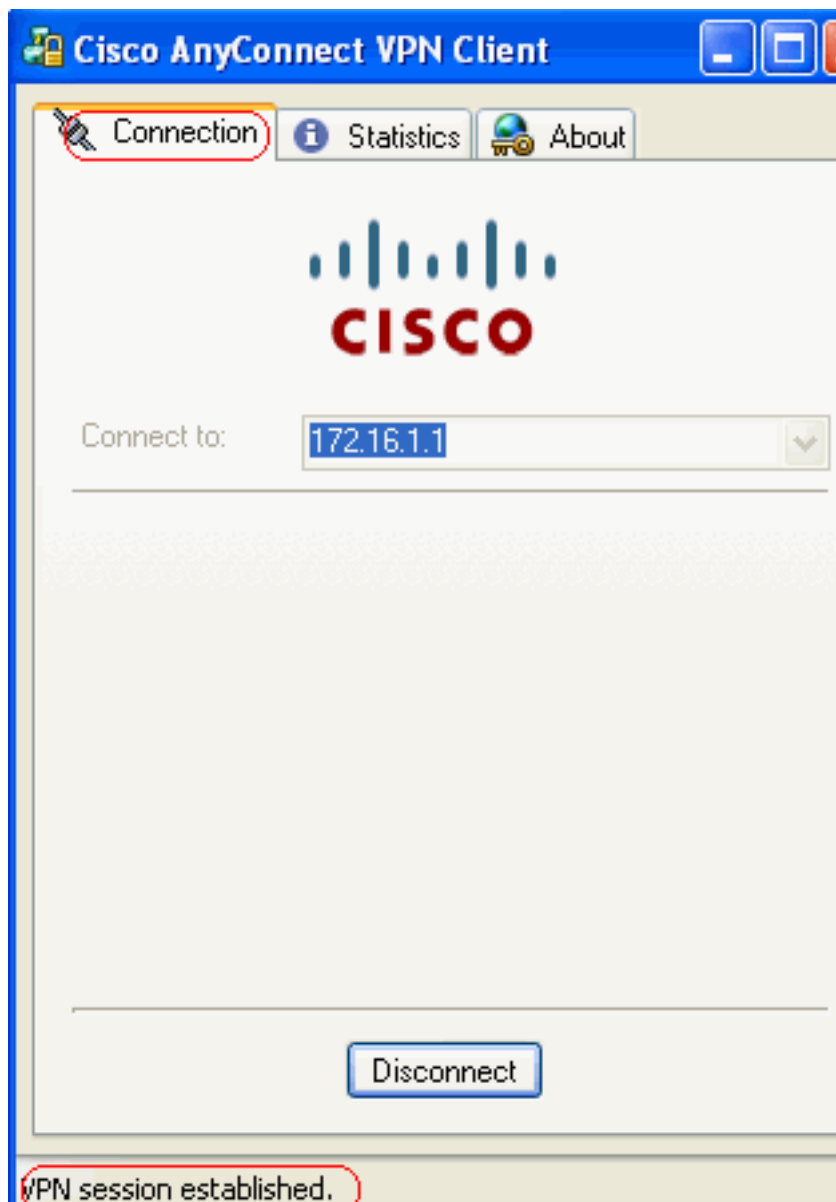
Help

Cancel

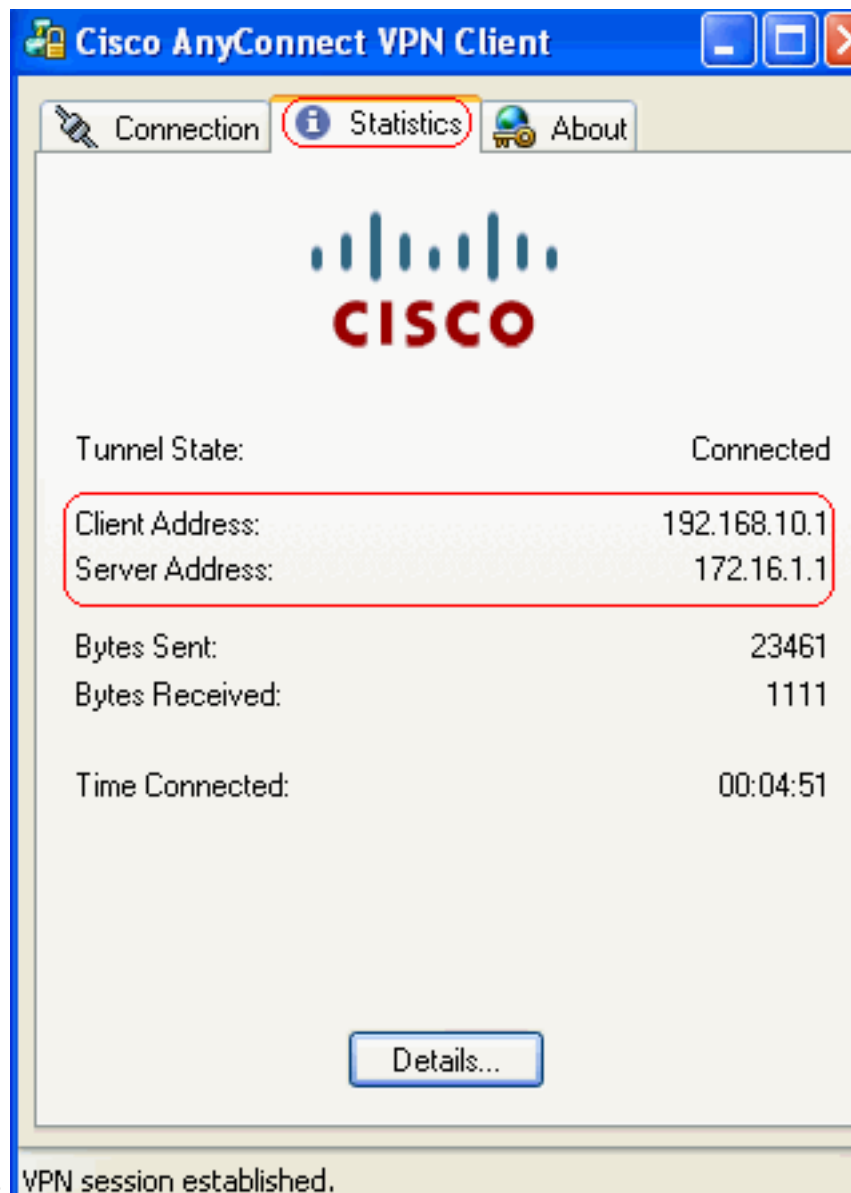
system... anyconnect - Paint

Cisco AnyConnect Connected

3. Klik op de vergrendeling die in de taakbalk van uw computer



verschijnt. **VPN session established.** Dit venster verschijnt en geeft informatie over de SSL-verbinding. Bijvoorbeeld, **192.168.10.1** is de toegewezen IP



door de ASA, enz.

VPN session established.

Dit venster

toont de informatie over de clientversie van Cisco AnyConnect



Verifiëren

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

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) 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:/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
```

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

```
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

```

- **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 de huidige WebVPN sessies in de ASA te kennen.

Sessions

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

Filter By: **SSL VPN Client** -- All Sessions -- Filter

Username IP Address	Group Policy Connection	Protocol Encryption	Login Time Duration	Byt Byt
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

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 af te sluiten.

```

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)

```

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

```

```
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 web svc <1-255>—Hier vindt u de real-time webgebeurtenissen om de sessie te kunnen maken.

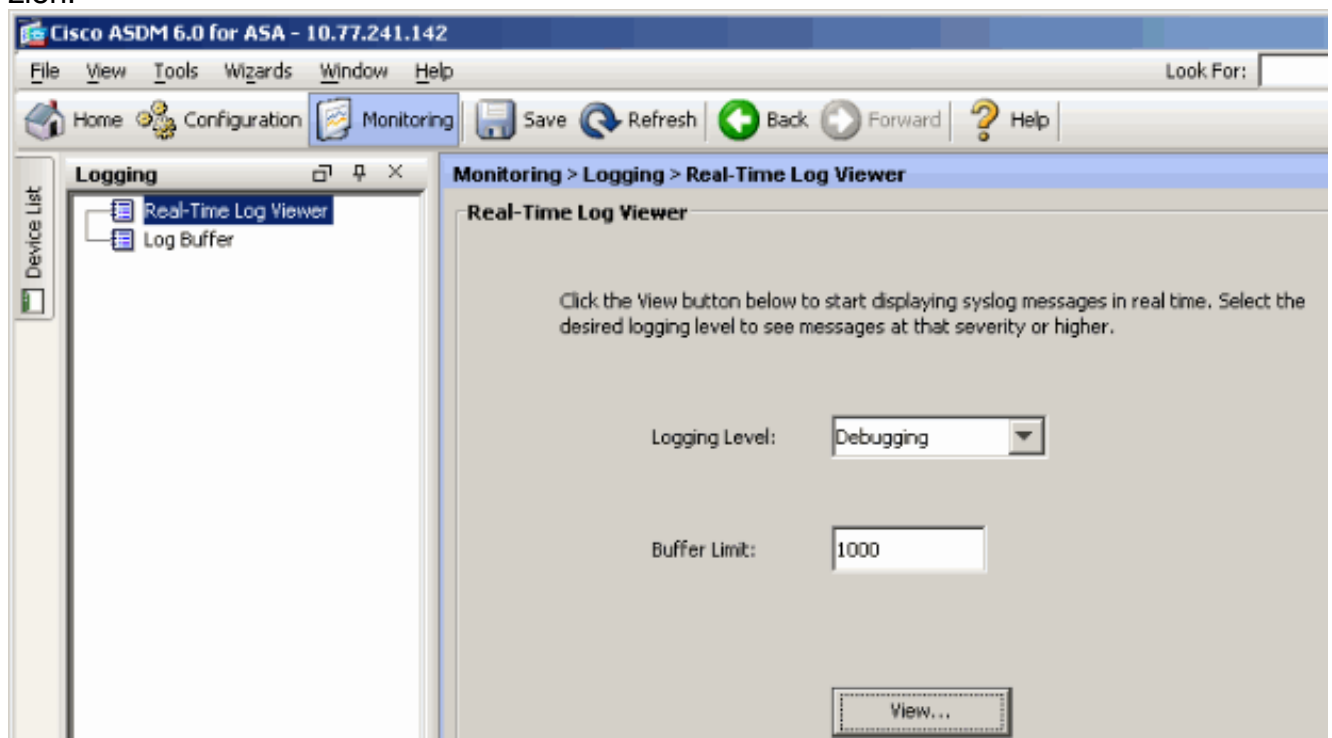
```
Ciscoasa#debug webvpn svc 7
```

```
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: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AFCEB9501758FF3B7B5545973C06F6393C92E59693'
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AFCEB9501758FF3B7B5545973C06F6393C92E59693'
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. Kies in ASDM **Bewaking > Vastlegging > Realtime logvenster > Weergave** om de gebeurtenissen in realtime te kunnen zien.



Dit voorbeeld toont aan dat de SSL sessie met het hoofd eindapparaat is gevestigd.

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.

Gerelateerde informatie

- [Cisco 5500 Series ondersteuningspagina voor adaptieve security applicatie](#)
- [Releaseopmerkingen van AnyConnect VPN-client, release 2.0](#)
- [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](#)