ASA met WebVPN en Single aanmelding bij gebruik van ASDM en NTLMv1 Configuration Voorbeeld

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Configureren](#)
[Een AAA-server voor Windows-domeinverificatie toevoegen](#)
[Een zelfondertekend certificaat maken](#)
[WebexVPN op de externe interface inschakelen](#)
[Een URL-lijst configureren voor uw interne server(s)](#)
[Een intern groepsbeleid configureren](#)
[Een tunnelgroep configureren](#)
[Automatische handtekeningen voor een server configureren](#)
[Definitieve ASA-configuratie](#)
[Verifiëren](#)
[Een WebVPN-aanmelding testen](#)
[Monitorsessies](#)
[WebVPN-sessie verwijderen](#)
[Problemen oplossen](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de Cisco adaptieve security applicatie (ASA) kunt configureren om automatisch inlogaanmeldingsgegevens van WebVPN aan servers door te geven, evenals secundaire verificatie, waarvoor extra inlogvalidatie nodig is tegen Windows Active Directory met NT LAN Manager versie 1 (NTLMv1). Deze optie staat bekend als single-sign-on (SSO). Het geeft links die voor een specifieke WebVPN-groep zijn ingesteld de mogelijkheid om deze gebruikersauthenticatie-informatie door te geven, waardoor meerdere authenticatie-aanwijzingen worden geëlimineerd. Deze optie kan ook worden gebruikt op het niveau van de wereldwijde configuratie of gebruikersconfiguratie.

Voorwaarden

Vereisten

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

- Verzeker u ervan dat NTLMv1 en Windows toegang voor de beoogde VPN-gebruikers zijn geconfigureerd. Raadpleeg uw Microsoft documentatie voor meer informatie over Windows-toegangsrechten.

Gebruikte componenten

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

- Cisco ASA 7.1(1)
- Cisco Adaptieve Security Devices Manager (ASDM) 5.1(2)
- Microsoft Internet Information Services (IS)

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.

Configureren

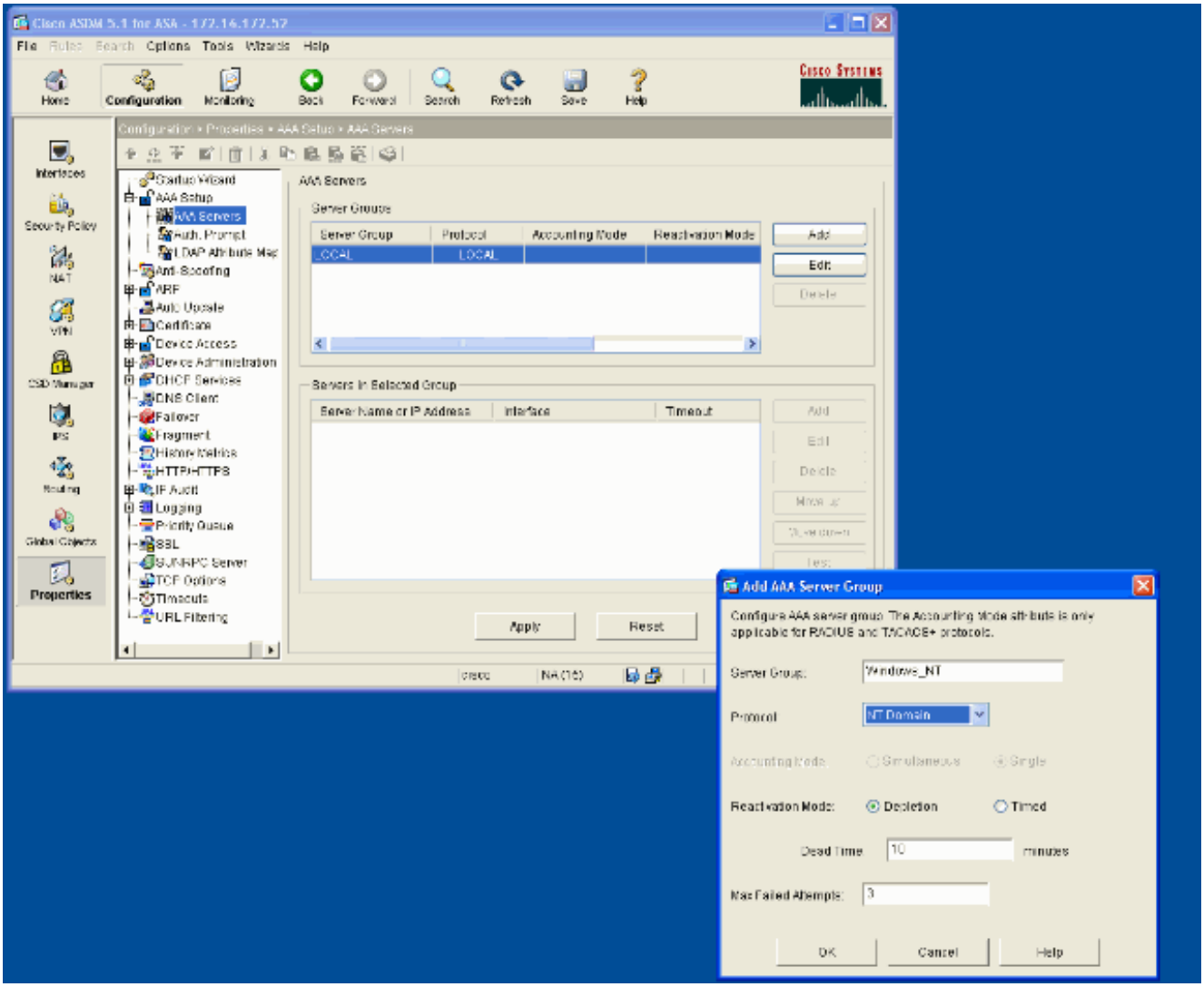
In deze sectie, wordt u voorgesteld met de informatie om de ASA als een WebVPN server met SSO te vormen.

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

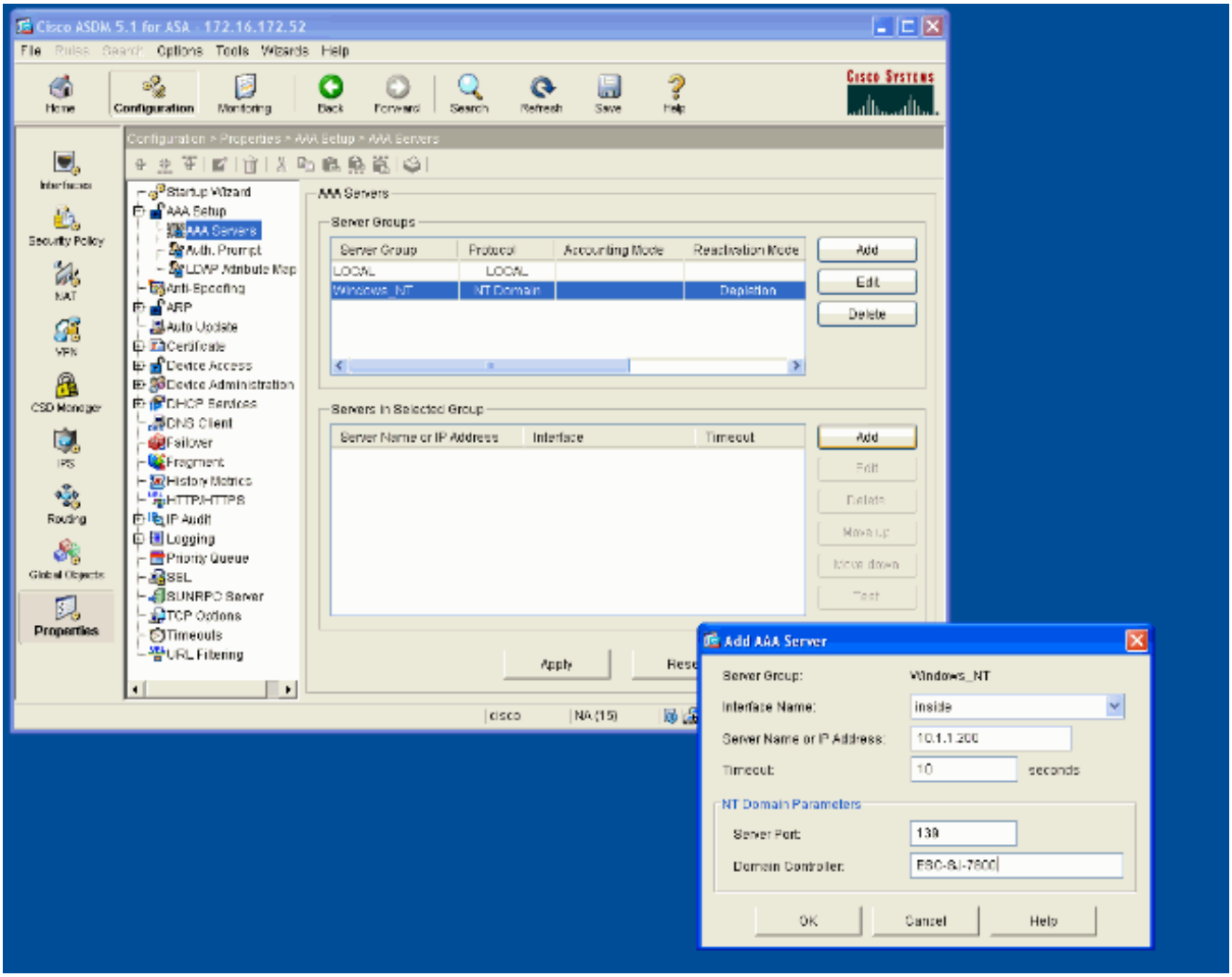
Een AAA-server voor Windows-domeinverificatie toevoegen

Voltooi deze stappen om de ASA te configureren om een domeincontroller te gebruiken voor verificatie.

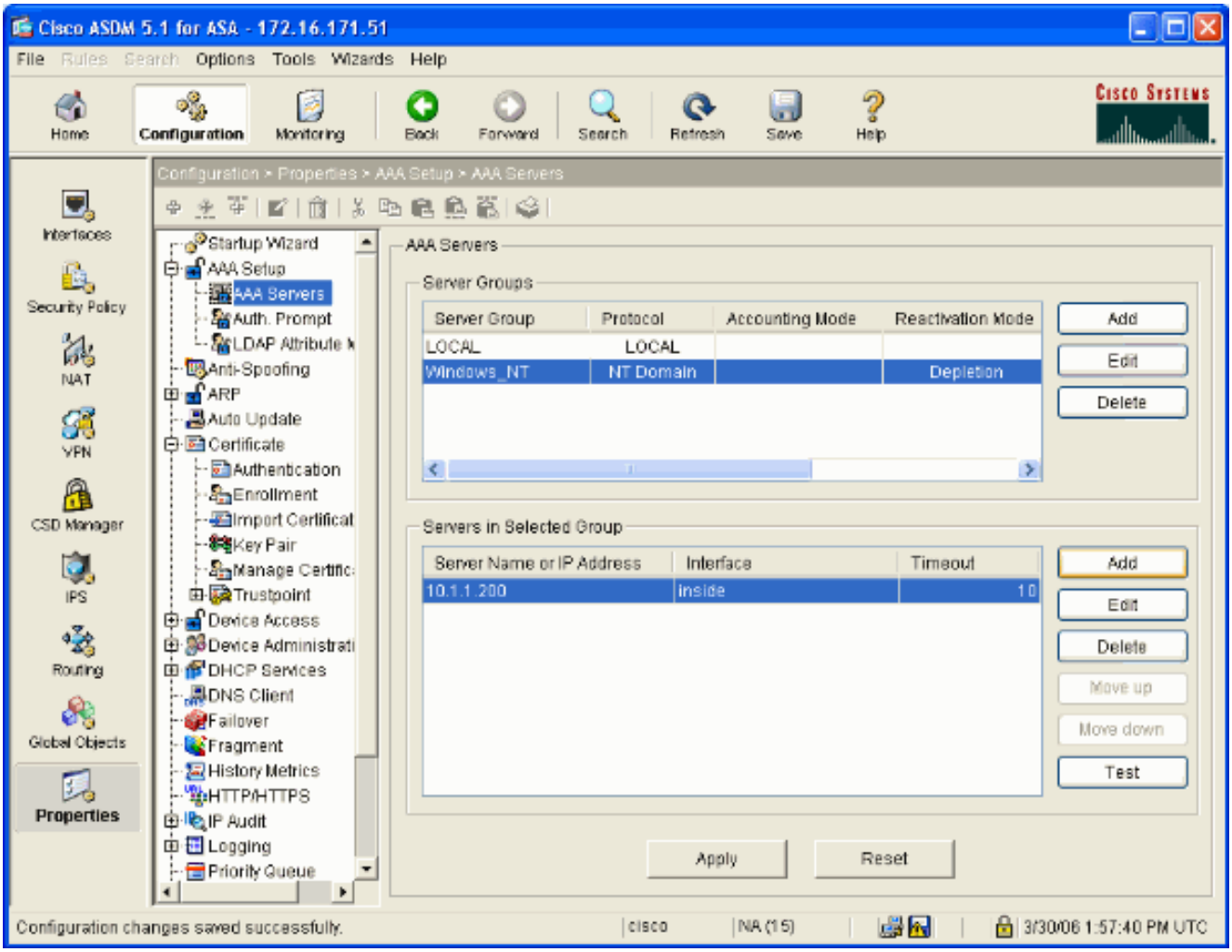
1. Selecteer **Configuration > Properties > AAA Setup > AAA servers** en klik op **Add**. Typ een naam voor de servergroep, zoals Windows_NT, en kies **NT Domain** als protocol.



2. Voeg een Windows server toe.Selecteer de nieuwe groep en klik op **Toevoegen**. Selecteer de interface waar de server zich bevindt en voer de IP-adres en domeincontrolenaam in. Zorg ervoor dat de domeincontrolenaam in alle hoofdletters is ingevoerd. Klik op **OK** wanneer u klaar
bent.



Dit venster toont de voltooide AAA-configuratie:

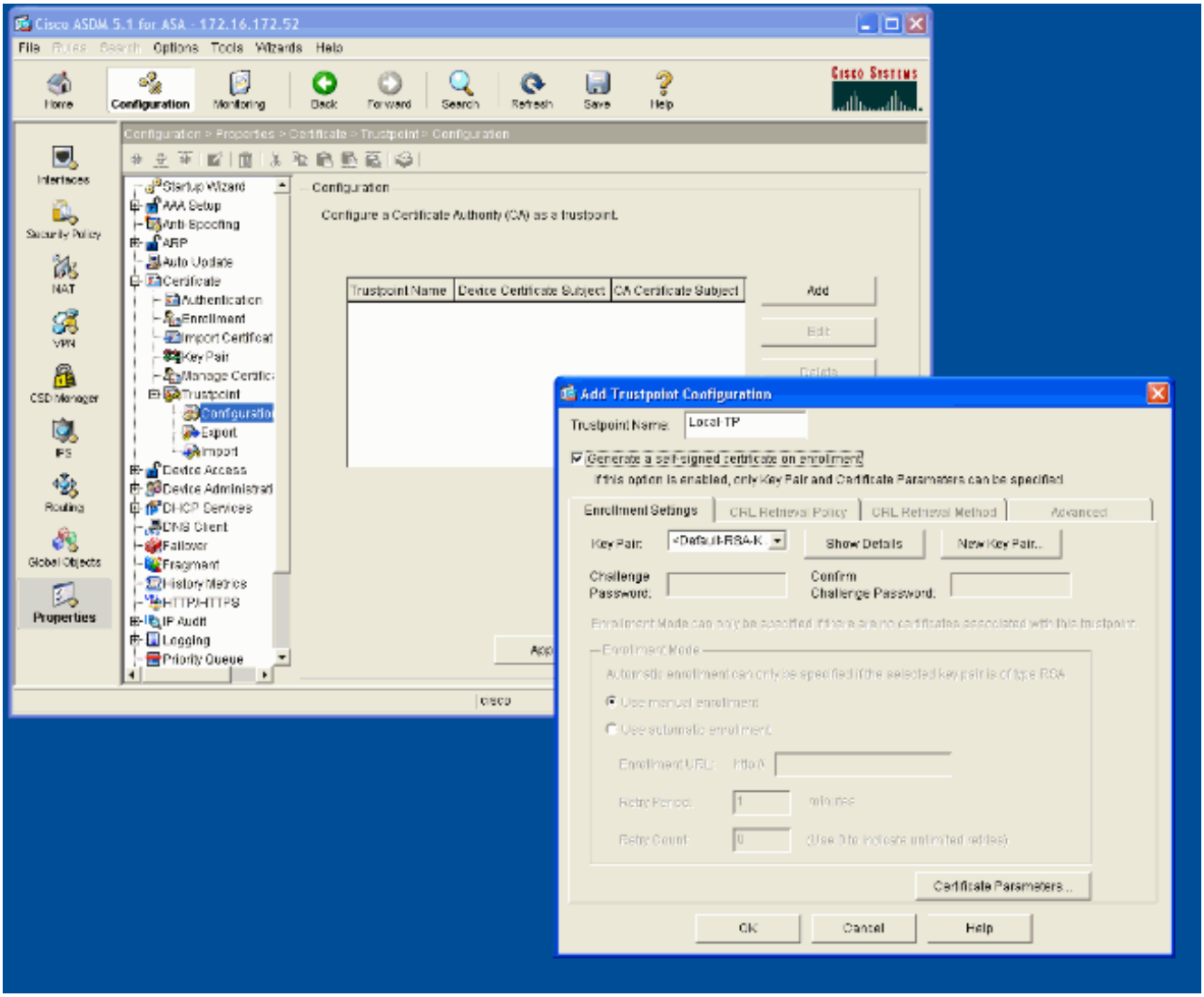


Een zelfondertekend certificaat maken

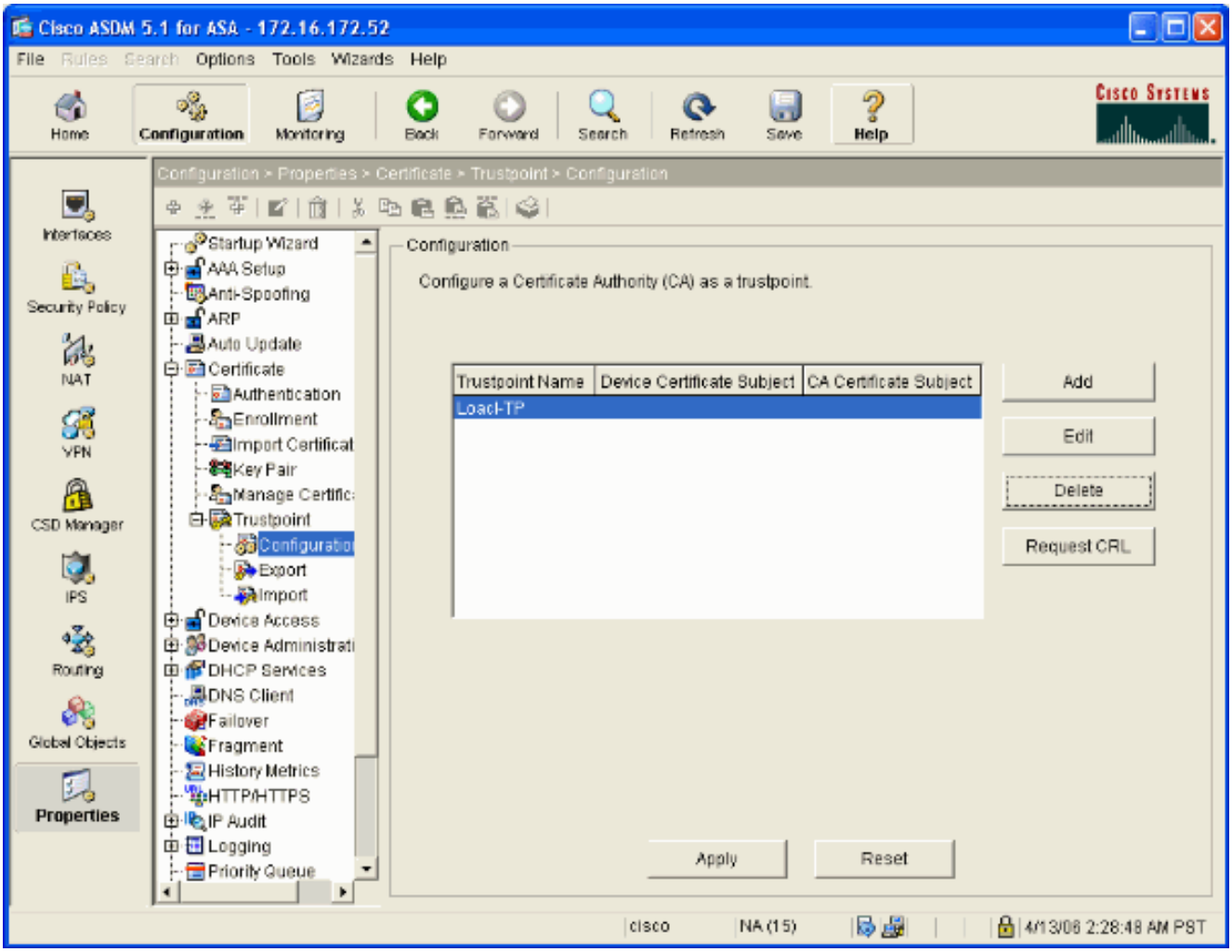
Voltooi deze stappen om de ASA te configureren om een zelfondertekend certificaat te gebruiken.

Opmerking: In dit voorbeeld wordt een zelfgetekend certificaat gebruikt voor eenvoud. Raadpleeg voor andere opties voor het invoeren van certificaten, zoals inschrijven bij een externe certificeringsinstantie, de configuratie van certificaten.

1. Selecteer **Configuratie > Eigenschappen > Certificaat > Trustpunt > Configuratie** en klik op **Toevoegen**.
2. In het venster dat verschijnt typt u een Trustpoint Name zoals Local-TP en controleer **Generate een zelfgetekend certificaat over inschrijving**. Andere opties kunnen met hun standaardinstellingen worden gelaten. Klik op **OK** wanneer u klaar bent.



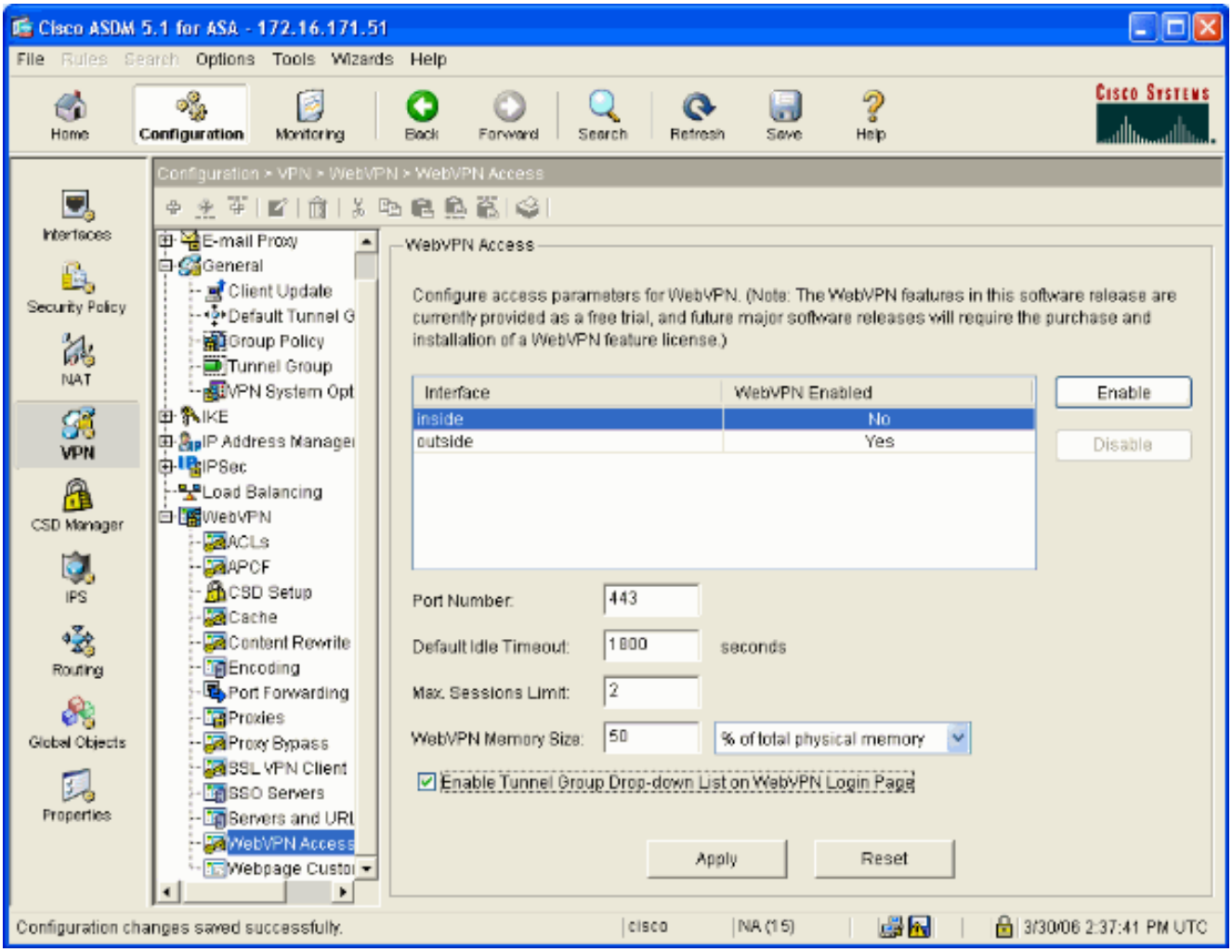
Dit venster toont de voltooide configuratie van het schaalpunt:



WebexVPN op de externe interface inschakelen

Voltooi deze stappen om gebruikers buiten uw netwerk toe te staan om verbinding te maken met WebVPN.

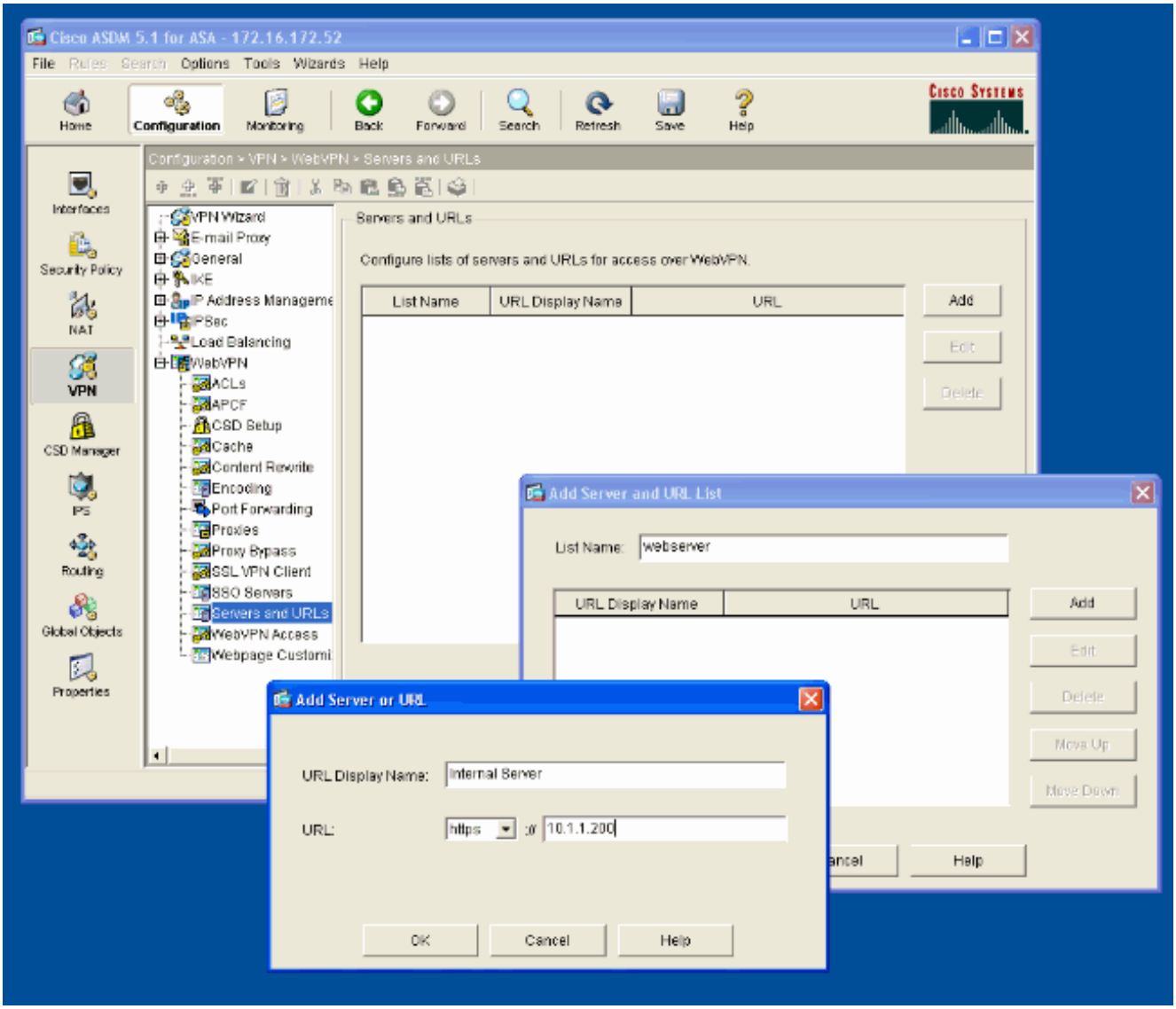
1. Selecteer **Configuratie > VPN > WebVPN > WebVPN Access**.
2. Selecteer de gewenste interface, klik op **Enable** en controleer **de vervolgkeuzelijst voor tunnelgroep inschakelen op de weblogpagina van VPN**.**Opmerking:** Als dezelfde interface wordt gebruikt voor WebVPN- en ASDM-toegang, moet u de standaardpoort voor ASDM-toegang van poort 80 naar een nieuwe poort zoals 8080 wijzigen. Dit gebeurt onder **Configuratie > Eigenschappen > Apparaattoegang > HTTPS/ASDM.Opmerking:** U kunt een gebruiker automatisch doorsturen naar poort 443 als een gebruiker navigeert naar **http://<ip_adres>** in plaats van **https://<ip_adres>**. Selecteer **Configuratie > Eigenschappen > HTTP/HTTPS**, kies de gewenste interface, klik op **Bewerken** en selecteer **HTTP opnieuw richten naar**
HTTPS.



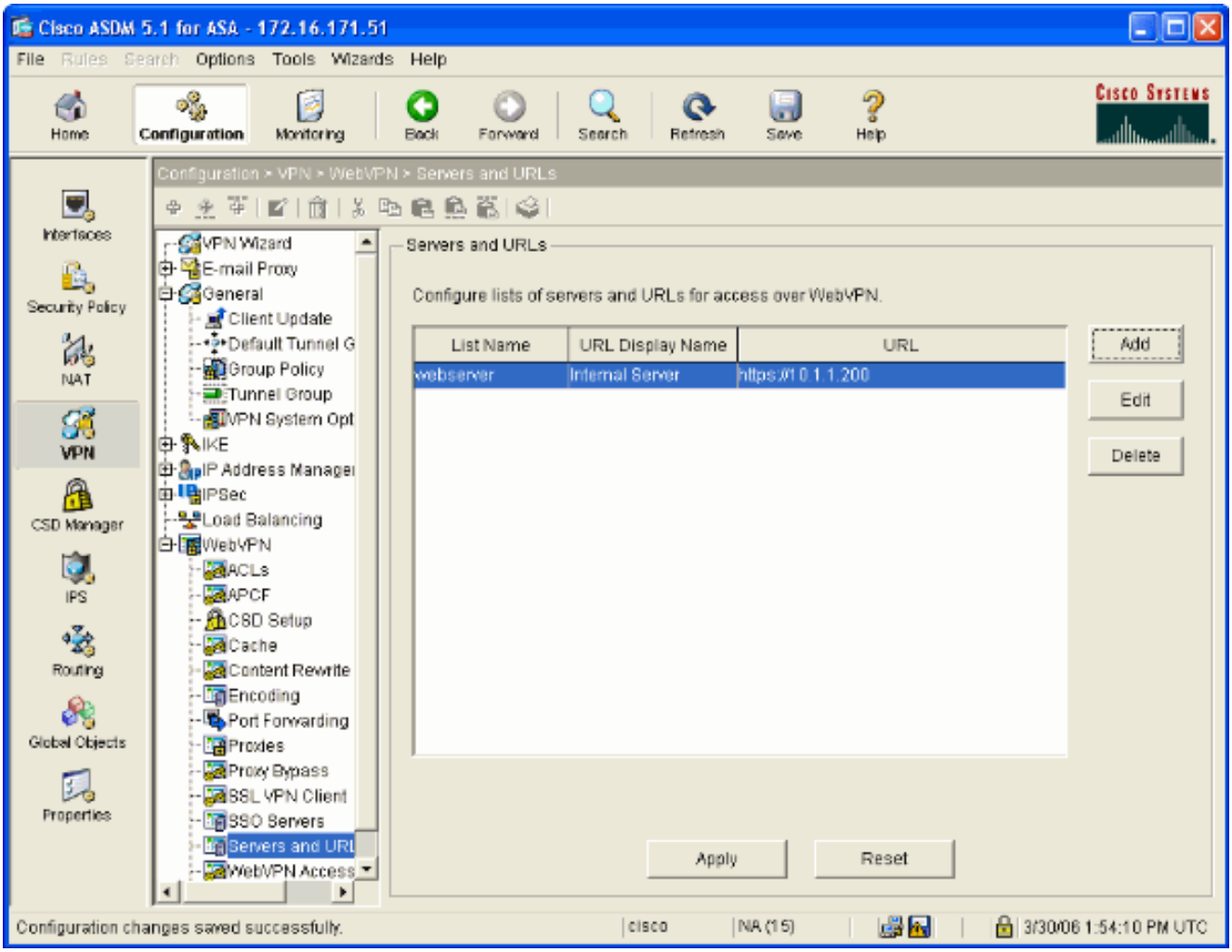
Een URL-lijst configureren voor uw interne server(s)

Voltooi deze stappen om een lijst te maken die de servers bevat waarvoor u uw WebVPN-gebruikers toegang wilt geven.

1. Selecteer **Configuratie > VPN > WebVPN > servers en URL**'s en klik op **Add**.
2. Voer een naam in voor de URL-lijst. Deze naam is niet zichtbaar voor eindgebruikers. Klik op **Toevoegen**.
3. Voer de URL Display Name in zoals deze aan gebruikers moet worden weergegeven. Voer de URL-informatie van de server in. Dit zou moeten zijn hoe u normaal toegang tot de server heeft.



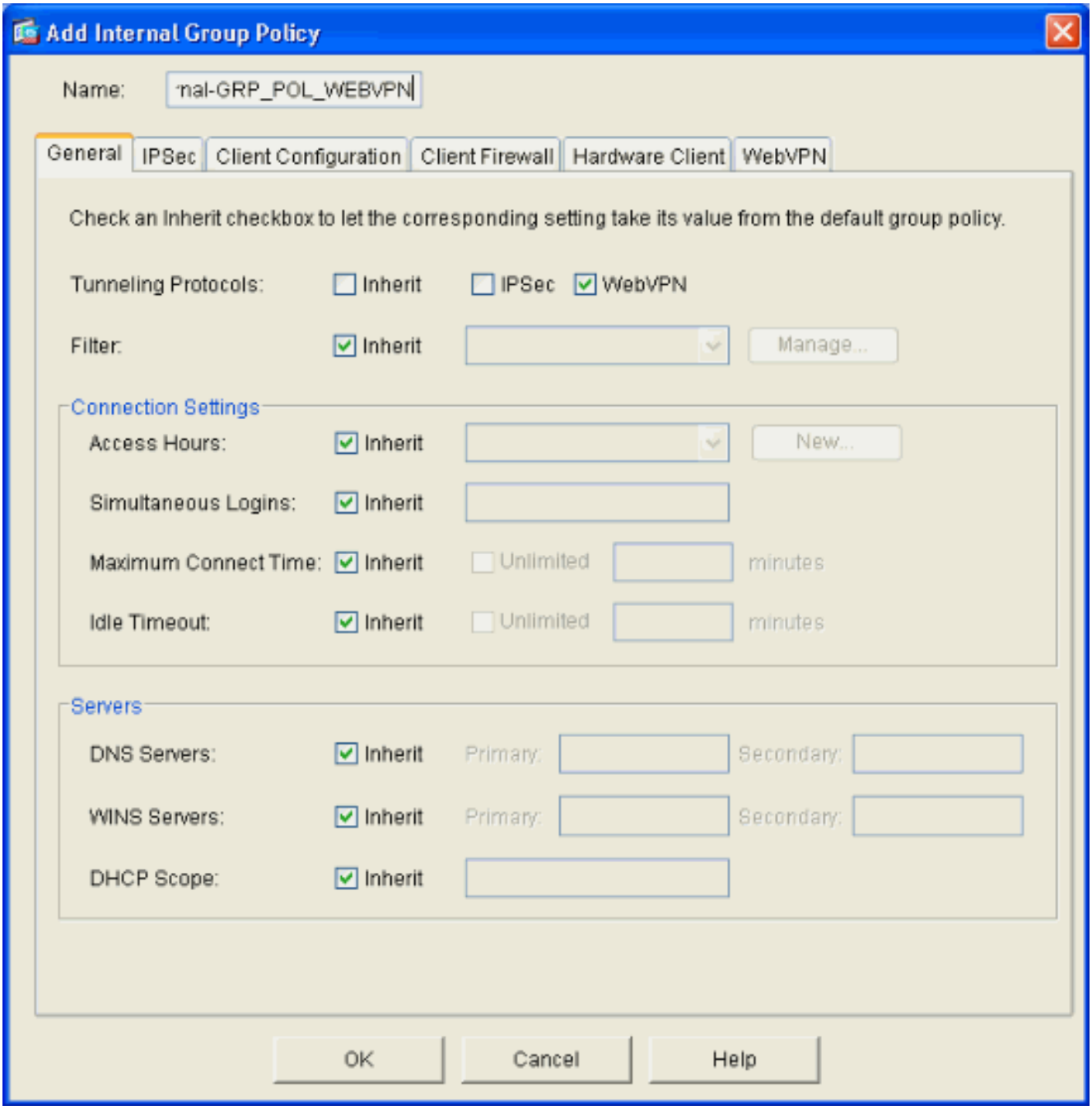
4. Klik op **OK**, **OK**, en **Toepassen**.



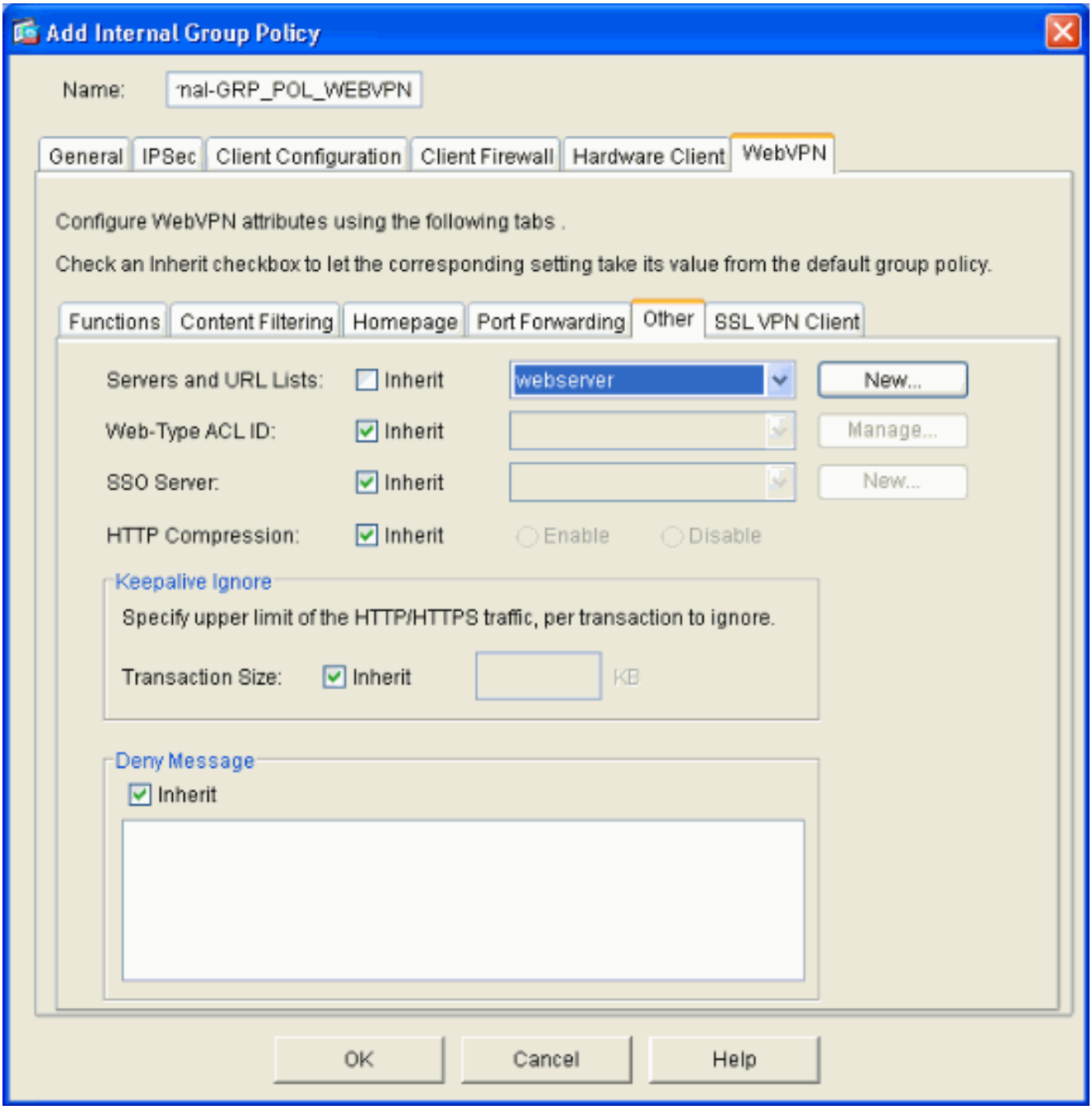
Een intern groepsbeleid configureren

Voltooi deze stappen om een groepsbeleid voor uw gebruikers van WebVPN te configureren.

1. Selecteer **Configuratie > VPN > Algemeen > Groepsbeleid**, klik op **Toevoegen** en selecteer **Intern groepsbeleid**.
2. Specificeer op het tabblad General een beleidsnaam, zoals Interne-Group_POL_WEBVPN. Schakel de **inloop** vervolgens naast de tunneling-protocollen uit en controleer **WebVPN**.



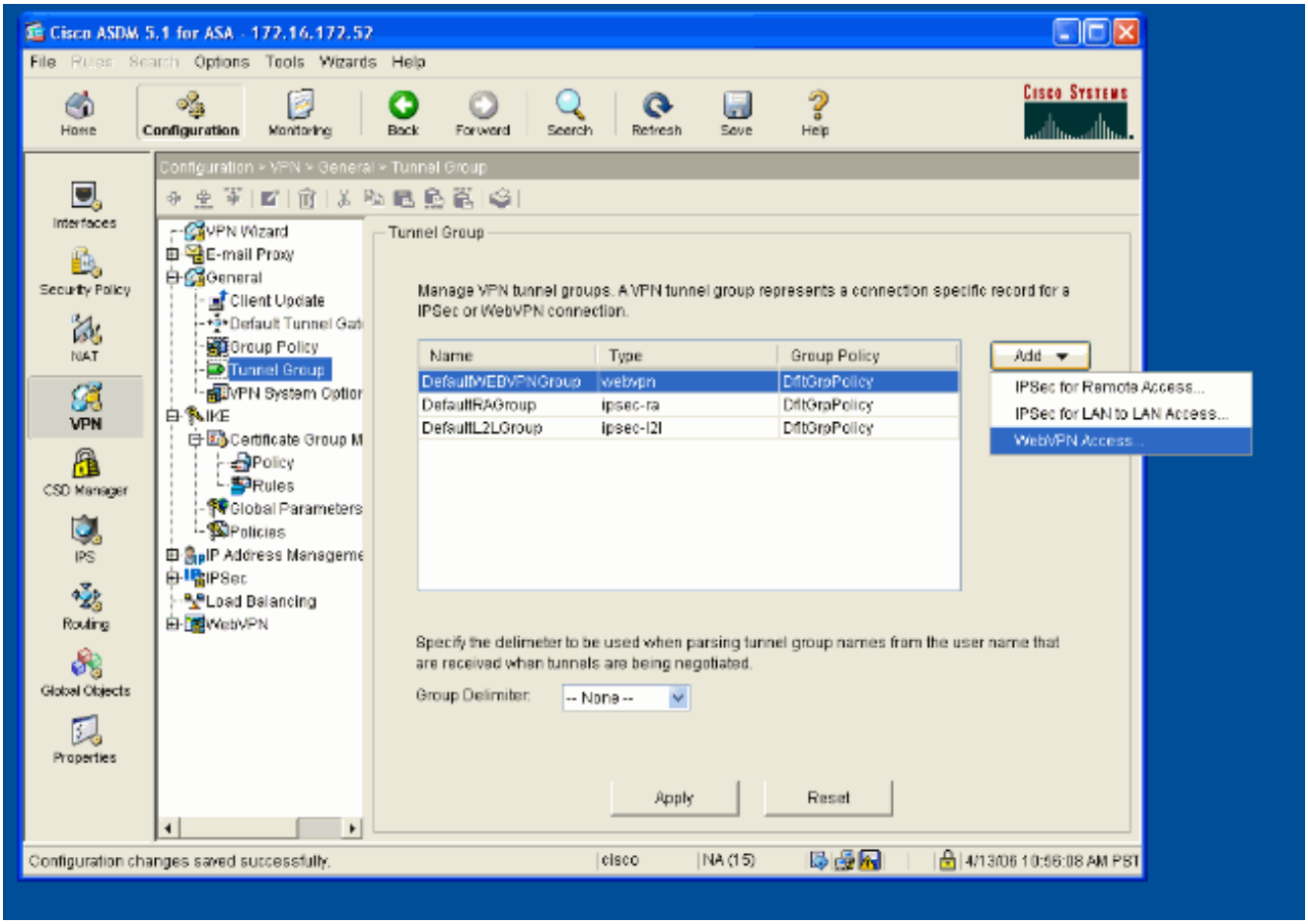
3. Selecteer in het tabblad WebVPN het tabblad **Overige** subtabblad. Schakel de **opdracht** naast servers en URL-lijsten uit en selecteer de URL-lijst die u hebt ingesteld in de vervolgkeuzelijst. Klik op **OK** wanneer u klaar bent.



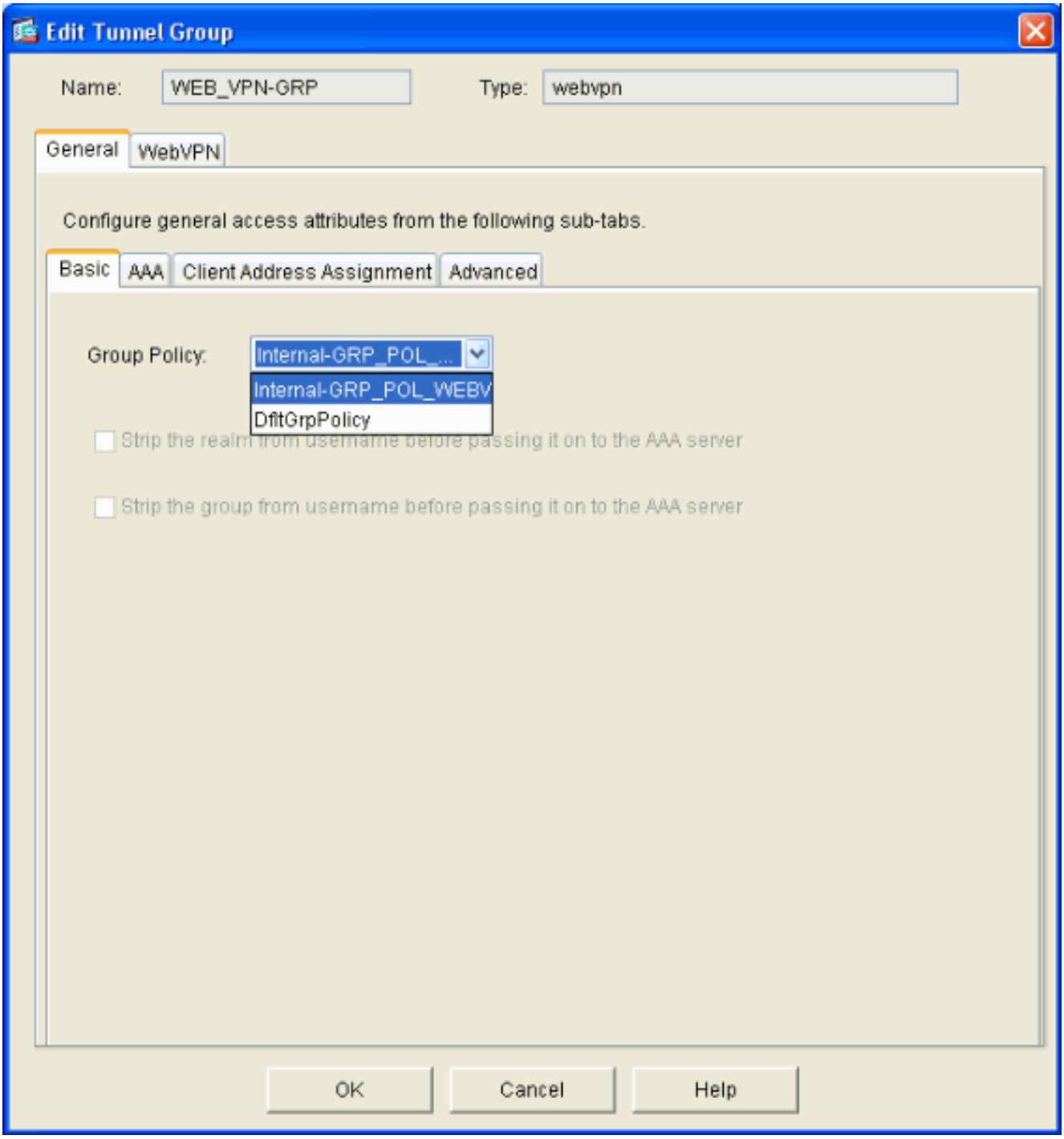
Een tunnelgroep configureren

Voltooi deze stappen om een Tunnelgroep voor uw WebVPN-gebruikers te configureren.

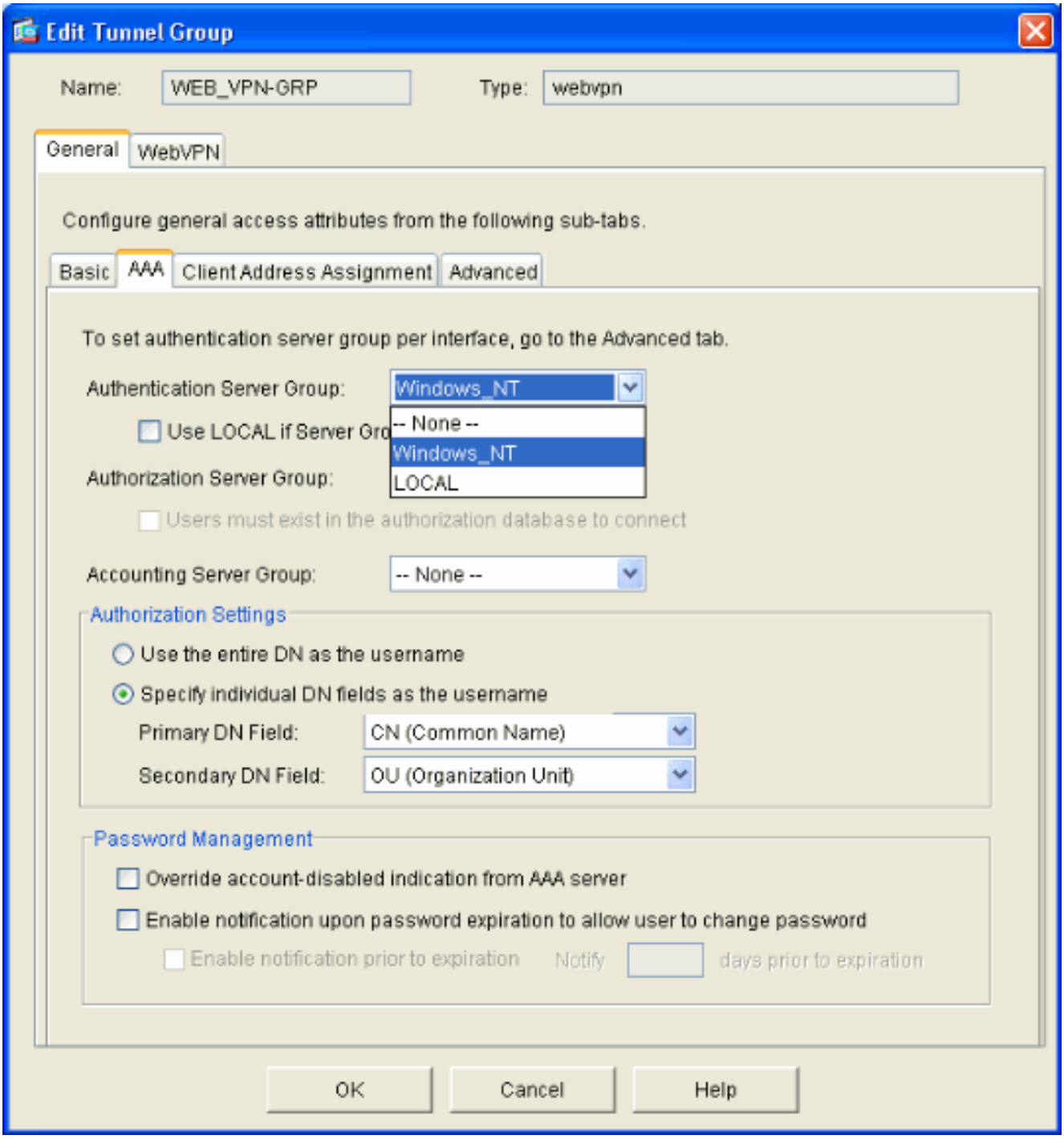
1. Selecteer **Configuration > VPN > General > Tunnel Group**, klik op **Add** en selecteer **WebeVPN Access...**



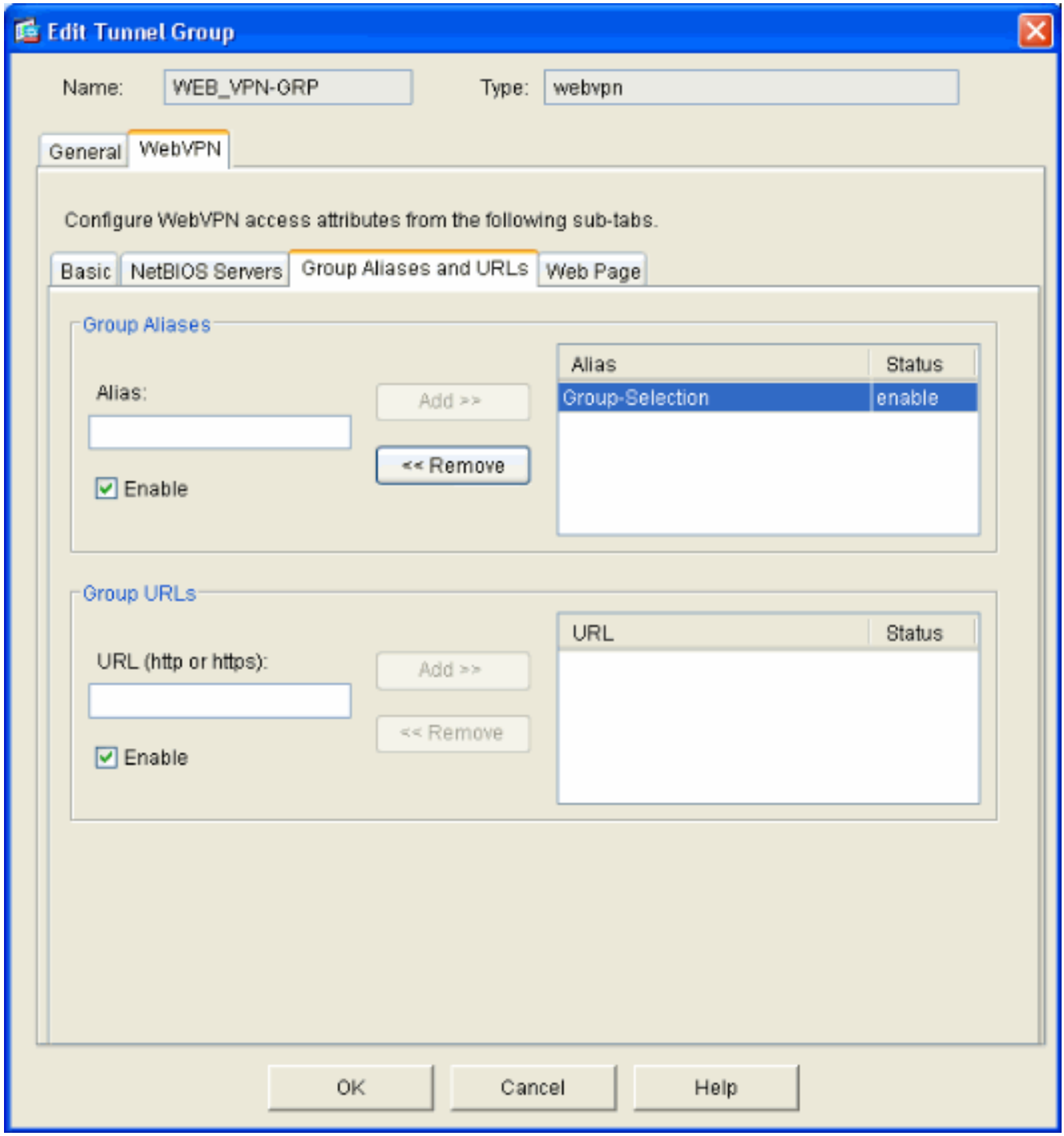
2. Voer een naam in voor de Tunnelgroep, zoals WEB_VPN-GRP. Selecteer in het tabblad Basic het groepsbeleid dat u hebt gemaakt en controleer of het groepstype **webvpn** is.



3. Ga naar het tabblad AAA.Voor de Groep van de Verificatieserver, kies de groep die u hebt ingesteld om NTLMv1-verificatie met uw domeincontroller mogelijk te maken.**Optioneel:** Controleer **LOKAAL als de servergroep er niet** in slaagt het gebruik van de LOKALE gebruikersdatabase in te schakelen voor het geval de geconfigureerde AAA-groep niet werkt. Dit kan u helpen bij het oplossen van problemen op een later tijdstip.



4. Ga naar het tabblad WebVPN en ga vervolgens naar het subtabblad **Group Aliases en URLs**.
5. Voer een alias in onder Group Aliases en klik op **Add**. Deze alias verschijnt in de vervolgkeuzelijst die bij inloggen aan WebVPN-gebruikers wordt gepresenteerd.



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

Automatische handtekeningen voor een server configureren

Schakelt over naar de opdrachtregel zodat de BF beschikbaar is voor uw interne server(s).

Opmerking: deze stap kan niet in de ASDM-indeling worden voltooid en moet met de opdrachtregel worden voltooid. Raadpleeg De opdrachtregel-interface gebruiken voor meer informatie.

Gebruik de opdracht **automatisch** verzenden om de netwerkbron op te geven, zoals een server, waartoe u de gebruikers toegang wilt geven. Er wordt hier één IP-adres voor de server ingesteld, maar er kan ook een netwerkbereik worden opgegeven zoals **10.1.1.0/24**. Raadpleeg de opdracht automatisch tekenen voor meer informatie.

```
ASA>enable
ASA#configure terminal
ASA(config)#webvpn
ASA(config-webpvn)#auto-signon allow ip 10.1.1.200 255.255.255.255 auth-type ntlm
ASA(config-webvpn)#quit
ASA(config)#exit
ASA#write memory
```

In deze voorbeelduitvoer wordt de **auto-signaalopdracht** mondiaal ingesteld voor WebVPN. Deze opdracht kan ook worden gebruikt in de configuratiemodus van de WebVPN-groep of in de modus voor de gebruikersnaam van Webex. Het gebruik van deze opdracht in de WebVPN groepsconfiguratie modus beperkt het tot een bepaalde groep. Vergelijkbaar beperkt het gebruik van deze opdracht in de gebruikersnaam voor de configuratie van WebVPN deze tot een individuele gebruiker. Raadpleeg de opdracht automatisch tekenen voor meer informatie.

Definitieve ASA-configuratie

Dit document gebruikt deze configuratie:

ASA versie 7.1(1)

```
ASA# show running-config
: Saved
:
ASA Version 7.1(1)
!
terminal width 200
hostname ASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.171.51 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 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
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm512.bin
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 172.16.171.1 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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- AAA server configuration aaa-server Windows_NT
protocol nt aaa-server Windows_NT host 10.1.1.200 nt-
auth-domain-controller ESC-SJ-7800 !--- Internal group
policy configuration group-policy Internal-
GRP_POL_WEBVPN internal group-policy Internal-
GRP_POL_WEBVPN attributes vpn-tunnel-protocol webvpn
webvpn url-list value webserver username cisco password
Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa
authentication http console LOCAL aaa authentication ssh
console LOCAL aaa authentication enable console LOCAL
http server enable 8181 http 0.0.0.0 0.0.0.0 outside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart !--- Trustpoint/certificate configuration
crypto ca trustpoint Local-TP enrollment self crl
configure crypto ca certificate chain Local-TP
certificate 31 308201b0 30820119 a0030201 02020131
300d0609 2a864886 f70d0101 04050030 1e311c30 1a06092a
864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30
1e170d30 36303333 30313334 3930345a 170d3136 30333237
31333439 30345a30 1e311c30 1a06092a 864886f7 0d010902
160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86
4886f70d 01010105 0003818d 00308189 02818100 e47a29cd
56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4
a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f
30add0b5 81f6801a 766c9404 9cabcbde 44b221f9 b6d6dc18
496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3 d8802efc
ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748 e4cda3b7
4f007d4f 02030100 01300d06 092a8648 86f70d01 01040500
03818100 c6f87c61 534bb544 59746bdb 4e01680f 06a88a15
e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38 7f75928e
1b1b6300 940b8dff 69eac16b af551d7f 286bc79c e6944e21
49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700 fd6acc16
a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d 4c298076
294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group
configuration tunnel-group WEB_VPN-GRP type webvpn
tunnel-group WEB_VPN-GRP general-attributes
authentication-server-group Windows_NT default-group-
policy Internal-GRP_POL_WEBVPN tunnel-group WEB_VPN-GRP
webvpn-attributes group-alias Group-Selection enable
telnet timeout 5 ssh timeout 5 console timeout 0 !
class-map inspection_default match default-inspection-
traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512
```

```
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 Configuration webvpn enable outside url-list
webserver "Internal Server" https://10.1.1.200 1 tunnel-
group-list enable auto-signon allow ip 10.1.1.200
255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6
: end
```

Verifiëren

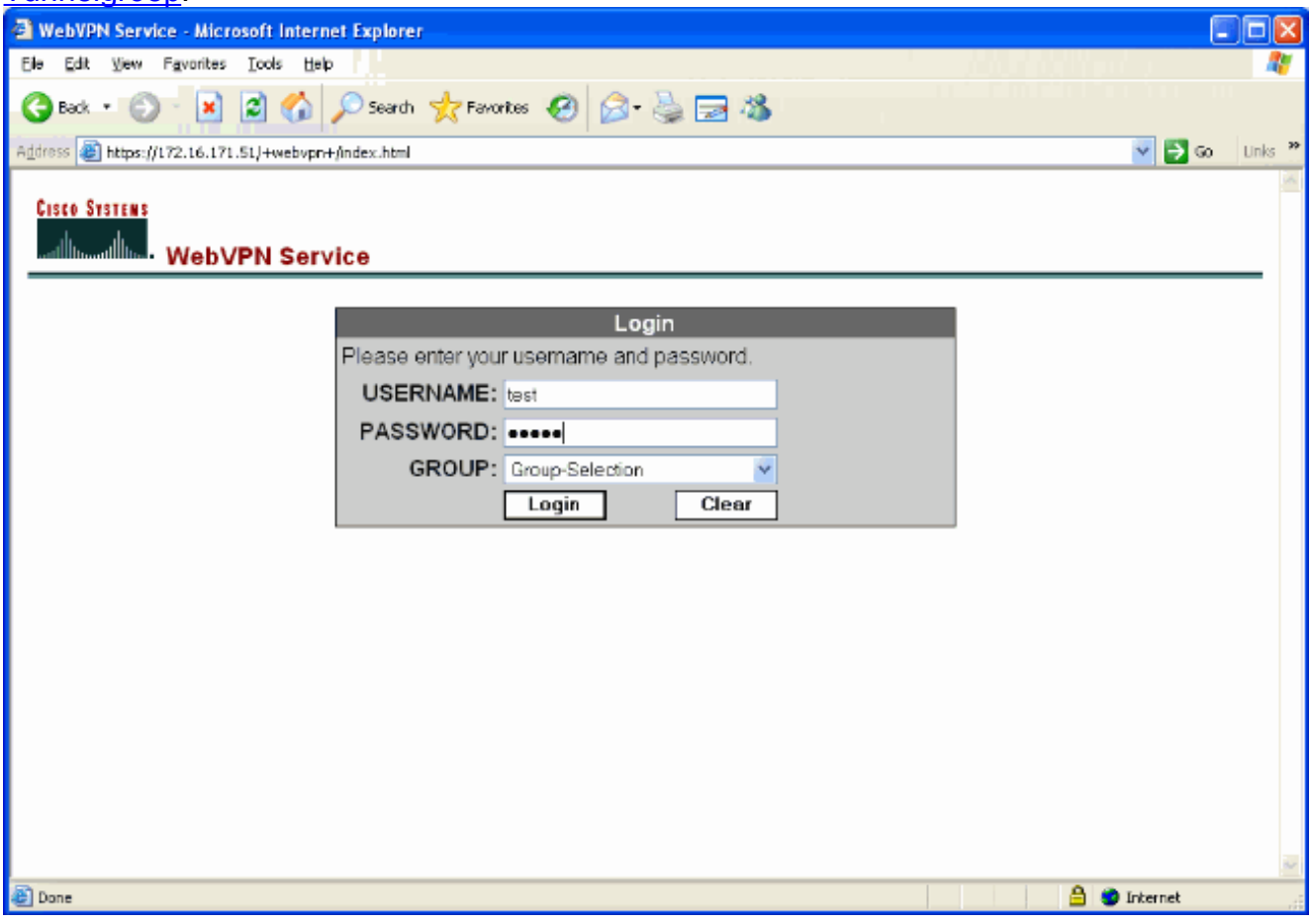
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

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

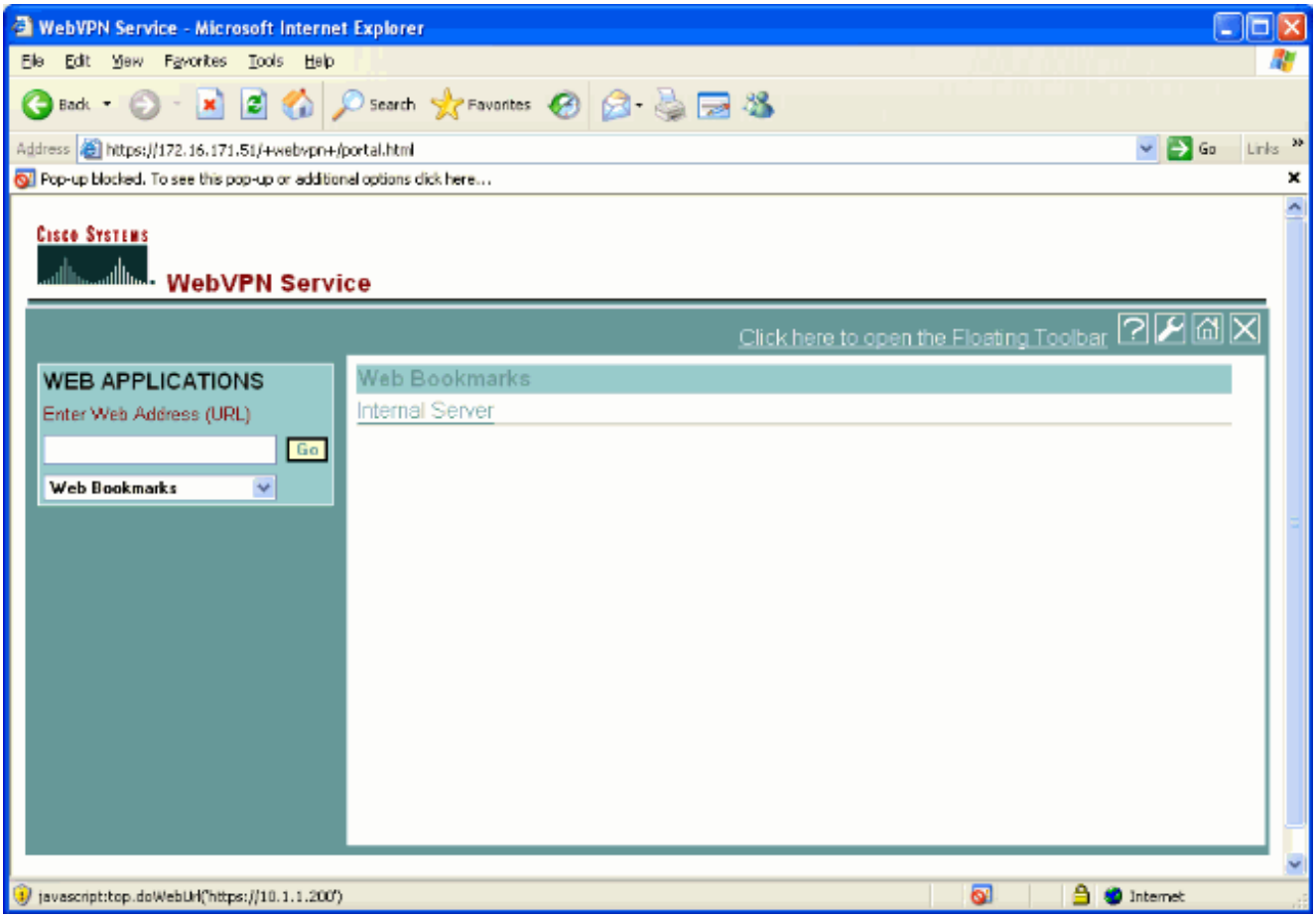
Een WebVPN-aanmelding testen

Meld u aan als gebruiker om de configuratie te testen.

1. Probeer met gebruikersinformatie uit uw NT-domein in te loggen op de ASA. Selecteer de groepsalias die in stap 5 is geconfigureerd onder Configuratie van een Tunnelgroep.

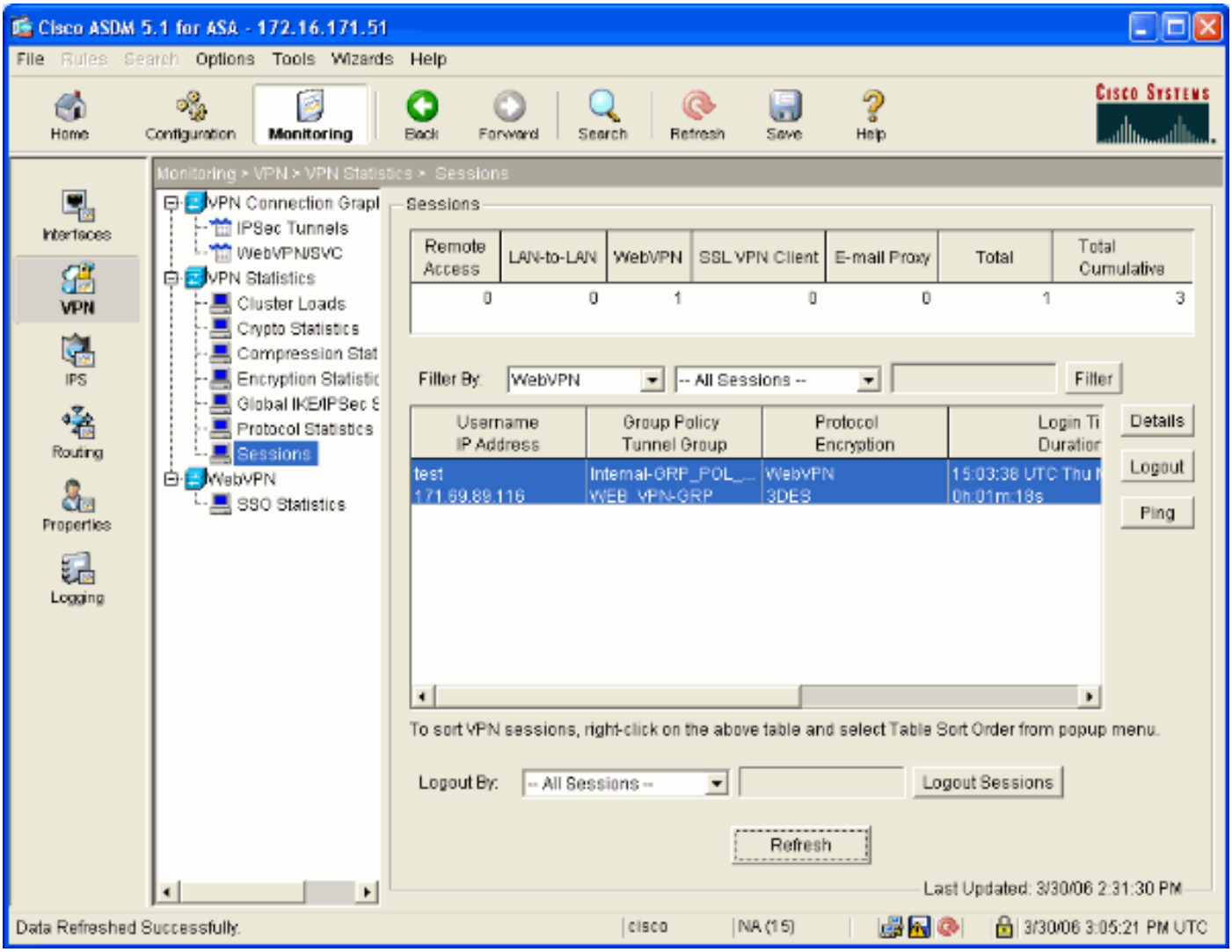


2. Zoek de link(s) die is (zijn) ingesteld op de interne server(s). Klik op de link om het te controleren.



Monitorsessies

Selecteer **Monitoring > VPN > VPN Statistieken > Sessies** en kijk naar een WebVPN-sessie die behoort tot de groep die in dit document is ingesteld.



WebVPN-sessie verwijderen

Deze uitvoer is een voorbeeld van het debug van een succesvolle WebVPN-sessie.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug**-opdrachten gebruikt.

```
ASA#debug webvpn 255
INFO: debug webvpn enabled at level 255
ASA#
ASA# webvpn_portal.c:ewaFormServe_webvpn_login[1570]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286]
WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782]
!--- Begin AAA WebVPN: calling AAA with ewsContext (78986968) and nh (78960800)! WebVPN: started
user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422]
WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095]
WebVPN: user: (test) authenticated.
!--- End AAA webvpn_auth.c:http_webvpn_auth_accept[2093]
webvpn_session.c:http_webvpn_create_session[159] webvpn_session.c:http_webvpn_find_session[136]
```

```
WebVPN session created!
webvpn_session.c:http_webvpn_find_session[136]
webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202]
traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421]
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
!--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

Problemen oplossen

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

- Als het vervolgkeuzevenster Group niet aanwezig is op de inlogpagina van WebVPN, zorg er dan voor dat u stap 2 hebt voltooid onder WebeVPN inschakelen op de buiteninterface en stap 5 onder Een tunnelgroep configureren. Als deze stappen niet zijn voltooid en de uitrollijst ontbreekt, valt de authenticatie onder de Standaardgroep en zal deze waarschijnlijk mislukken.
- Alhoewel u geen toegangsrechten aan de gebruiker in ASDM of op de ASA kunt toewijzen, kunt u gebruikers met Microsoft Windows toegangsrechten op uw domeincontroller beperken. Voeg de benodigde NT groepsrechten toe voor de webpagina waaraan de gebruiker echt verklaart. Zodra de gebruiker zich in Webex met de rechten van de groep inlogt, wordt de toegang tot de opgegeven pagina's dienovereenkomstig verleend of ontkend. De ASA treedt alleen op als proxy-authenticatie host namens de domeincontroller en alle communicatie hier is NTLMv1.
- U kunt SSO voor Sharepoint via WebVPN niet configureren omdat de Sharepoint Server geen op formulieren gebaseerde verificatie ondersteunt. Als gevolg daarvan zijn de bladwijzers met de post of de post-plug-procedure hier niet van toepassing.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Technische ondersteuning en documentatie – Cisco Systems