Thin-Client SSL VPN (WebVPN) op ASA met ASDM Configuratievoorbeeld

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Netwerkdiagram
Conventies
Achtergrondinformatie
Thin-Client SSL VPN-configuratie met ASDM
Stap 1. Schakel WebVPN in op de ASA
Stap 2. Specificeer de kenmerken van het doorsturen van poorten
Stap 3. Maak een groepsbeleid en koppel het aan de poortdoorsturen lijst
Stap 4. Maak een tunnelgroep en koppel het aan het groepsbeleid
Stap 5. Maak een gebruiker en voeg die gebruiker toe aan het groepsbeleid
Thin-Client SSL VPN-configuratie met CLI
Verifiëren
Procedure
Opdrachten
Problemen oplossen
Is het SSL-handdrukproces voltooid?
Is de SSL VPN Thin-Client functioneel?
Opdrachten
Gerelateerde informatie

Inleiding

De technologie van Thin-Client SSL VPN maakt veilige toegang mogelijk voor bepaalde toepassingen die statische poorten hebben, zoals telnet (23), SSH(22), POP3 (110), IMAP4 (143) en MTP(25). U kunt het Thin-Client SSL VPN gebruiken als een door de gebruiker gedreven toepassing, door beleid gedreven toepassing, of beide. U kunt toegang op gebruikersbasis configureren of groepsbeleid maken waarin u een of meer gebruikers toevoegt.

- **Clientless SSL VPN (WebVPN)** - Biedt een externe client die een SSL-enabled Web browser vereist om toegang te krijgen tot HTTP of HTTPS Web servers op een lokaal netwerk (LAN). Daarnaast heeft clientloze SSL VPN toegang tot Windows-bestand dat doorbladert door het Protocol Common Internet File System (CIFS). Outlook Web Access (OWA) is een voorbeeld van HTTP-toegang.Raadpleeg Clientless SSL VPN (WebVPN) in ASA Configuration Voorbeeld om meer te weten te komen over de Clientless SSL VPN.

- **Thin-Client SSL VPN (Port Forwarding)** — Biedt een externe client die een kleine Java-gebaseerde applicatie downloads en maakt beveiligde toegang mogelijk voor TCP-toepassingen (Transmission Control Protocol) die statische poortnummers gebruiken. Post Office Protocol (POP3), Simple Mail Transfer Protocol (MTP), Internet Message Access Protocol (IMAP), Secure Shell (SSH) en Telnet zijn voorbeelden van beveiligde toegang. Omdat bestanden op de lokale machine-wijziging moeten worden gewijzigd, moeten gebruikers lokale beheerrechten hebben om deze methode te kunnen gebruiken. Deze methode van SSL VPN werkt niet met toepassingen die dynamische port opdrachten, zoals sommige FTP-toepassingen (File Transfer Protocol) gebruiken.**Opmerking:** User Datagram Protocol (UDP) wordt niet ondersteund.
- **SSL VPN Client (Tunnel Mode)** downloads een kleine client naar het externe werkstation en maakt volledige beveiligde toegang tot resources op een intern bedrijfsnetwerk mogelijk. U kunt de SSL VPN-client (SVC) permanent naar een extern werkstation downloaden of u kunt de client verwijderen als de beveiligde sessie is gesloten.Raadpleeg SSL VPN Client (SVC) op ASA met ASDM Configuration Voorbeeld om meer te weten te komen over de SSL VPN-client.

Dit document demonstreert een eenvoudige configuratie voor Thin-Client SSL VPN op de adaptieve security applicatie (ASA). De configuratie stelt een gebruiker in staat om veilig te tellen naar een router die zich op de binnenkant van de ASA bevindt. De configuratie in dit document wordt ondersteund voor ASA versie 7.x en hoger.

Voorwaarden

Vereisten

Zorg er voordat u deze configuratie probeert voor dat u aan deze vereisten voor de externe clientstations voldoet:

- SSL-enabled-webbrowser
- SUN Java JRE versie 1.4 of hoger
- Gereedschappen
- Bevolkingsblokkers gehandicapt
- Plaatselijke administratieve voorrechten (niet vereist maar sterk voorgesteld)

Opmerking: de nieuwste versie van SUN Java JRE is beschikbaar als een gratis download van de Java-website .

Gebruikte componenten

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

- Cisco adaptieve security applicatie 5510 Series
- Cisco adaptieve security apparaatbeheer (ASDM) 5.2(1)**Opmerking:** Raadpleeg HTTPS-toegang voor ASDM om de ASA te kunnen configureren door de ASDM.
- Software voor Cisco adaptieve security applicatie, versie 7.2(1)
- Microsoft Windows XP Professional (SP2) externe client

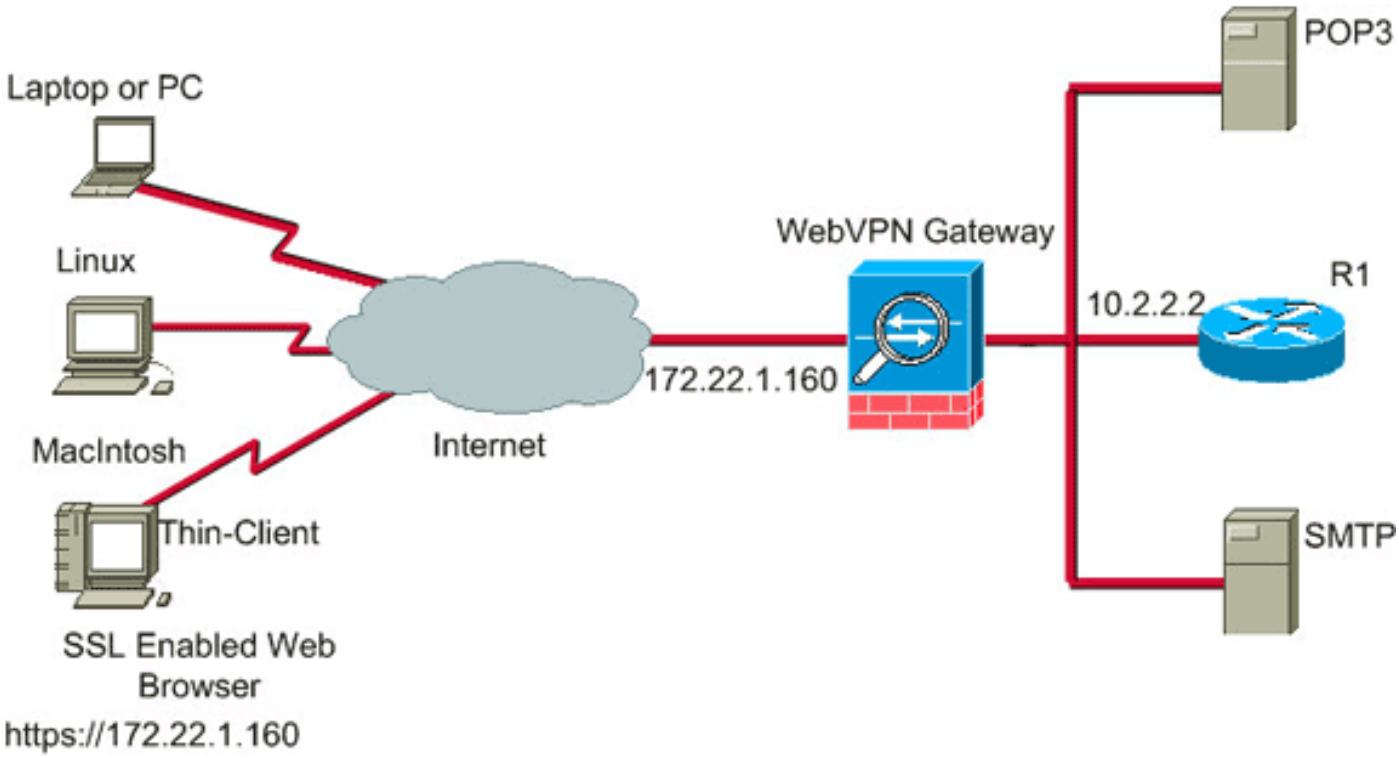
De informatie in dit document is ontwikkeld in een labomgeving. Alle apparaten die in dit document werden gebruikt, werden opnieuw ingesteld op de standaardconfiguratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt. Alle IP-

adressen die in deze configuratie gebruikt werden, zijn geselecteerd uit RFC 1918-adressen in een labomgeving; deze IP-adressen zijn niet routeerbaar op het internet en zijn alleen voor testdoeleinden.

Netwerkdiagram

Dit document gebruikt de netwerkconfiguratie die in dit hoofdstuk wordt beschreven.

Wanneer een externe client een sessie met de ASA start, downloads de client een kleine Java-applicatie naar het werkstation. De cliënt wordt voorgesteld met een lijst van vooraf gevormde middelen.



Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Om een sessie te starten, opent de externe client een SSL-browser naar de externe interface van de ASA. Nadat de sessie is vastgesteld, kan de gebruiker de parameters gebruiken die op de ASA zijn geconfigureerd om een beroep te doen op telnet of toepassingstoegang. De ASA voorziet in een veilige verbinding en geeft de gebruiker toegang tot het apparaat.

OPMERKING: Ingebonden toegangslijsten zijn niet nodig voor deze verbindingen omdat de ASA al op de hoogte is van wat een rechtszitting is.

Thin-Client SSL VPN-configuratie met ASDM

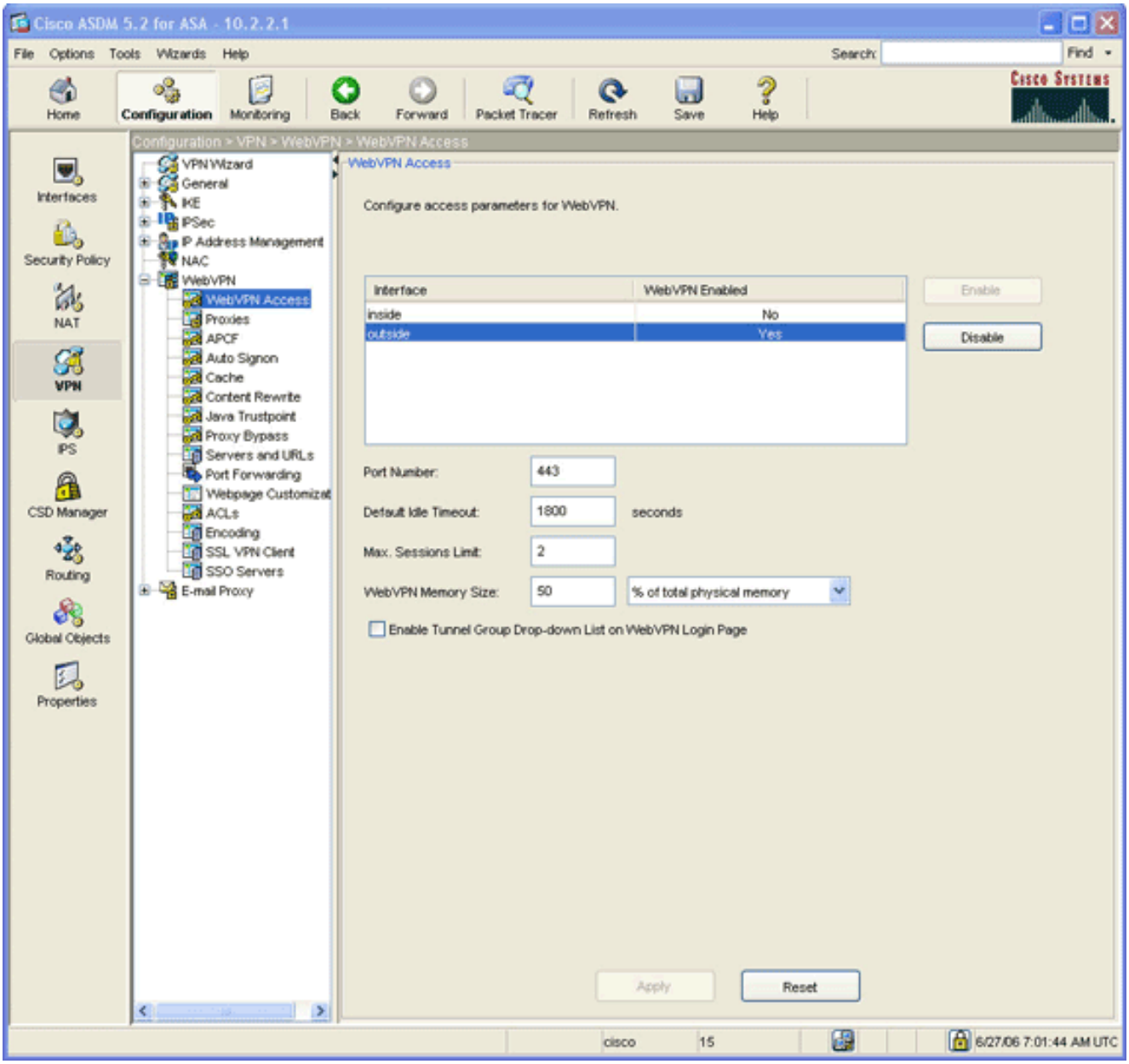
Voltooi de volgende stappen om Thin-Client SSL VPN op de ASA te configureren:

1. WebexVPN op ASA inschakelen
2. Kenmerken voor poortdoorsturen configureren
3. Maak een groepsbeleid en koppel het aan de poortdoorsturen lijst (gemaakt in stap 2)
4. Een tunnelgroep maken en deze aan het groepsbeleid koppelen (in stap 3 gemaakt)
5. Een gebruiker maken en die gebruiker aan het groepsbeleid toevoegen (dit wordt gemaakt in stap 3)

Stap 1. Schakel WebVPN in op de ASA

Voltooi de volgende stappen om WebVPN op ASA mogelijk te maken:

1. Klik in de ASDM-toepassing op **Configuration** en vervolgens op **VPN**.
2. Vul **WebVPN** uit en kies **WebVPN Access**.

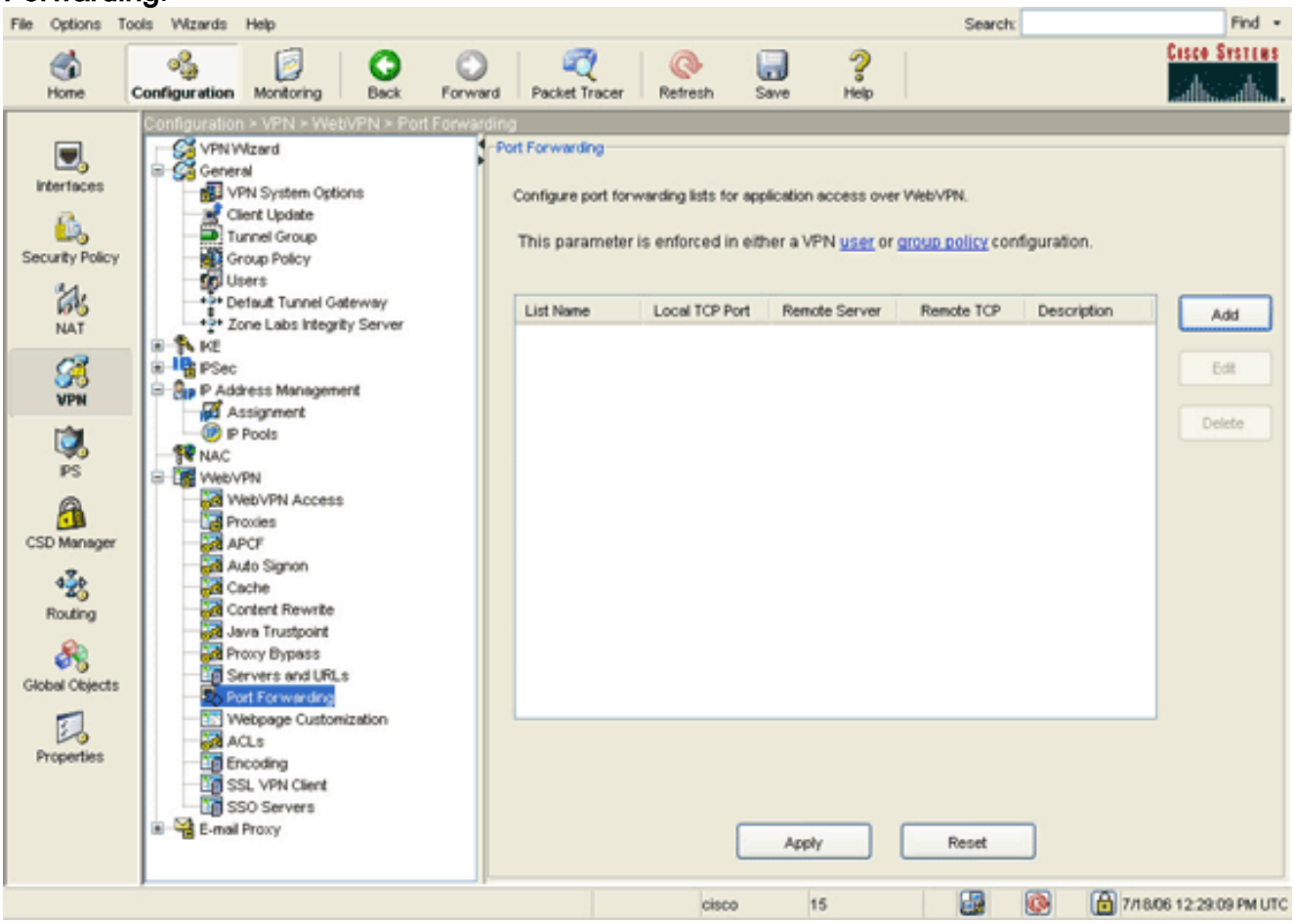


3. Markeer de interface en klik op **Inschakelen**.
4. Klik op **Toepassen**, klik op **Opslaan** en klik vervolgens op **Ja** om de wijzigingen te aanvaarden.

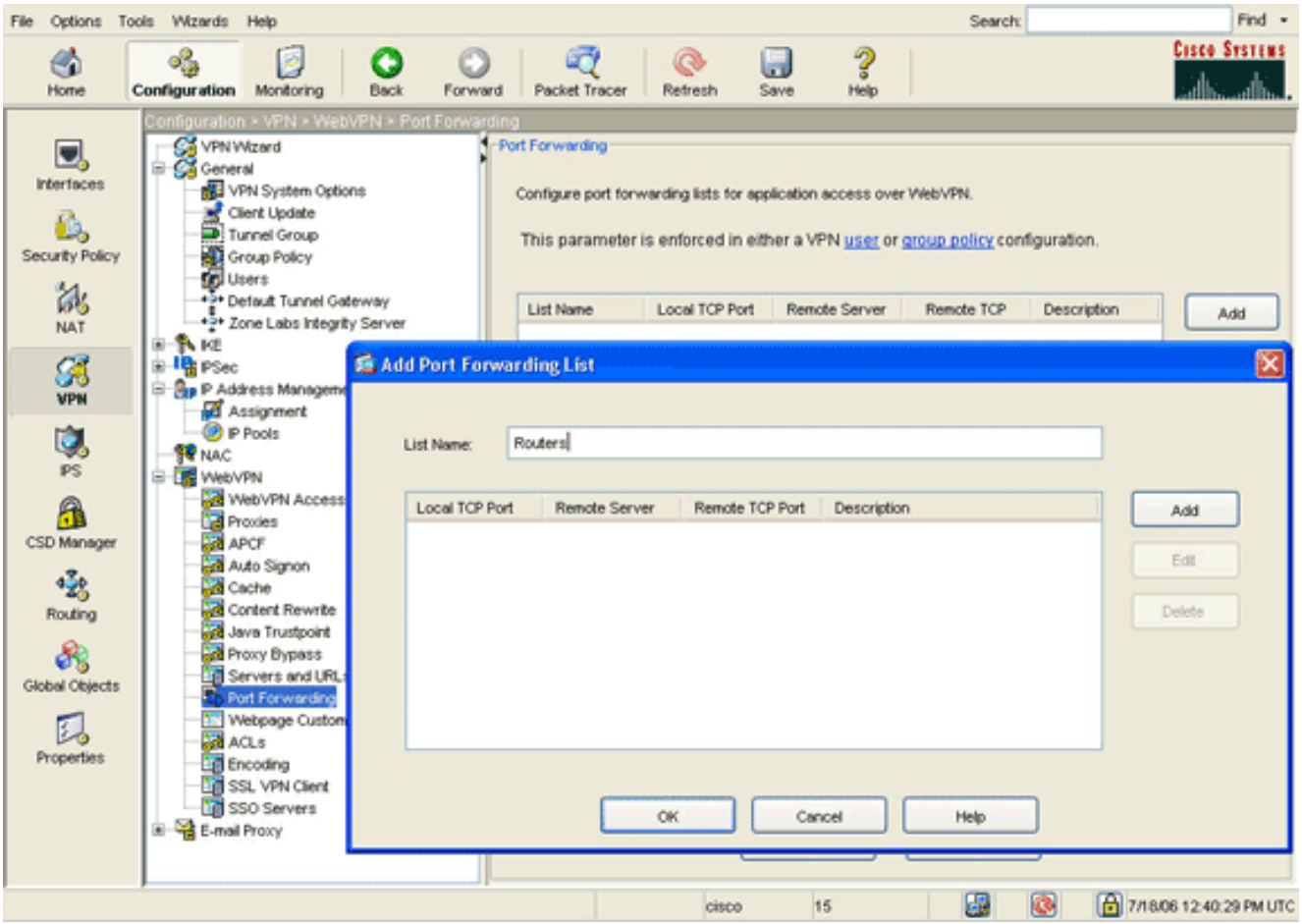
Stap 2. Specificeer de kenmerken van het doorsturen van poorten

Voltooi de volgende stappen om de eigenschappen van het poorttransport te configureren:

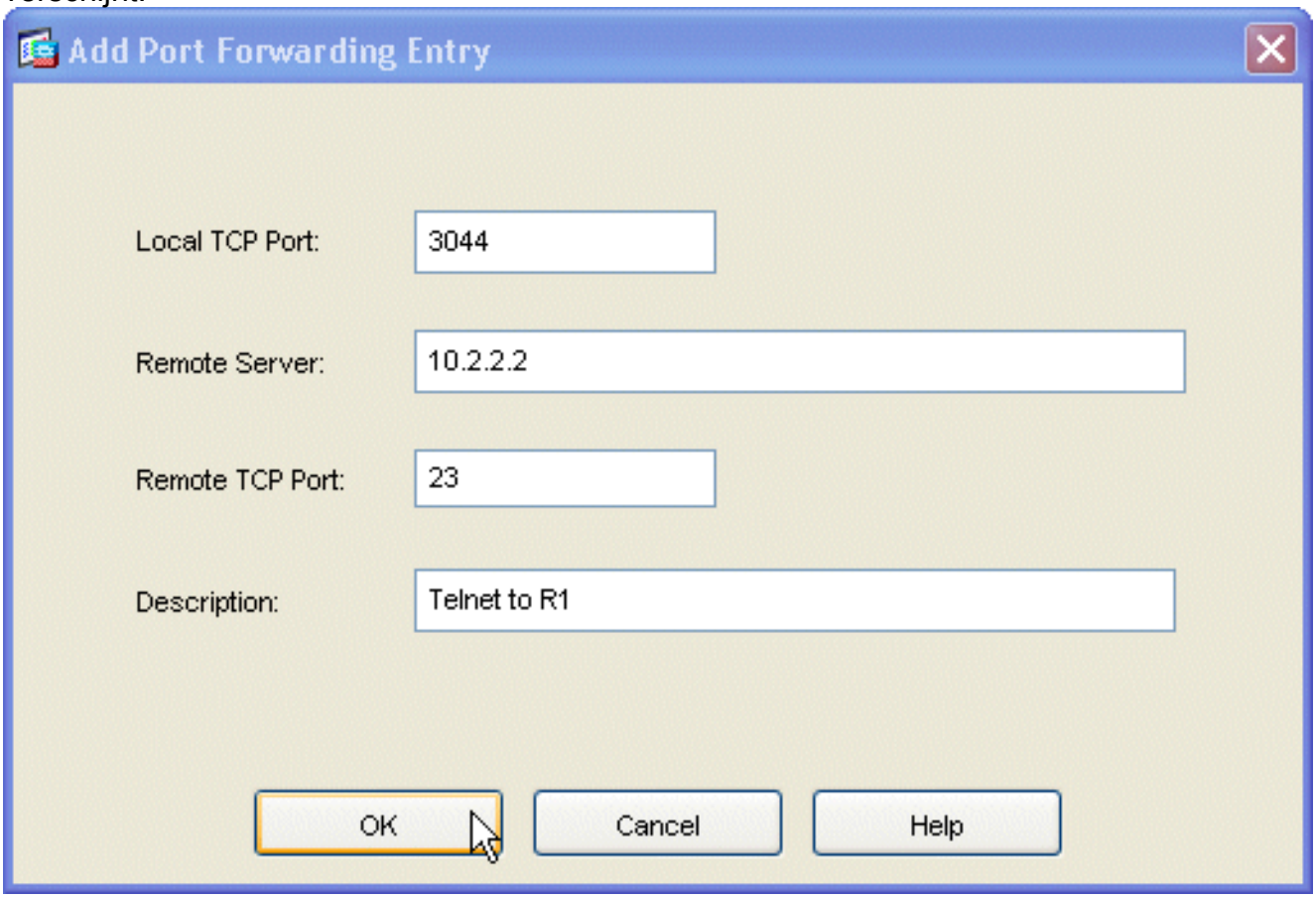
1. Vul **WebVPN** uit en kies **Port Forwarding**.



2. Klik op de knop **Toevoegen**.



3. Typ in het dialoogvenster Lijst voor doorsturen van poorten en klik op **Toevoegen**.Het dialoogvenster Toegang voor poortdoorsturen verschijnt.



4. Geef in het dialoogvenster Ingang doorsturen de volgende opties op:Typ in het veld Local TCP Port een poortnummer of accepteer de standaardwaarde.De waarde die u invoert, kan

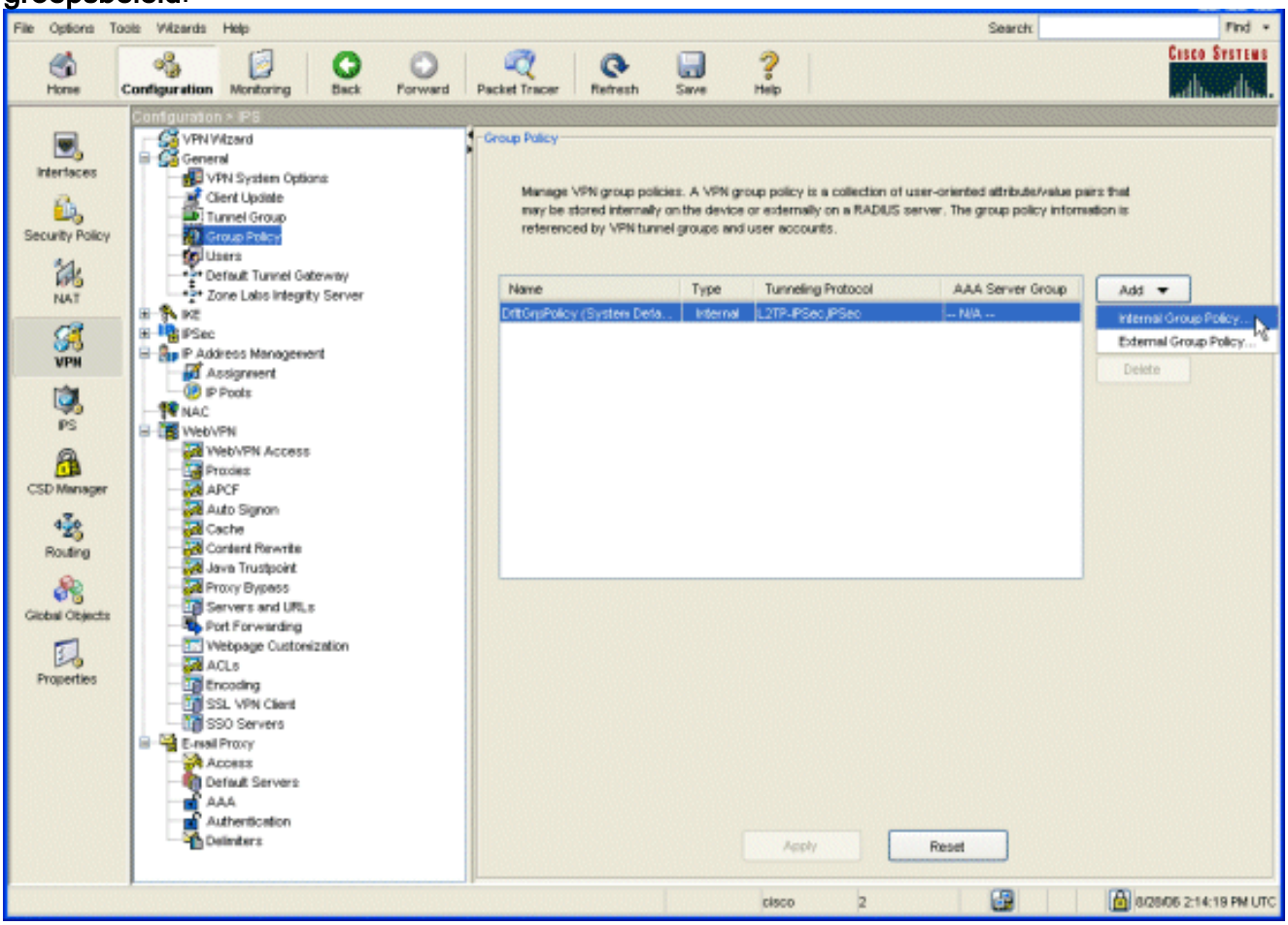
een willekeurig nummer zijn van 1024 tot 65535.Voer in het veld Remote Server een IP-adres in.Dit voorbeeld gebruikt het adres van de router.Voer in het veld Remote TCP-poort een poortnummer in.Dit voorbeeld gebruikt haven 23.Typ in het veld Description een omschrijving en klik op **OK**.

5. Klik op **OK** en vervolgens op **Toepassen**.
6. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

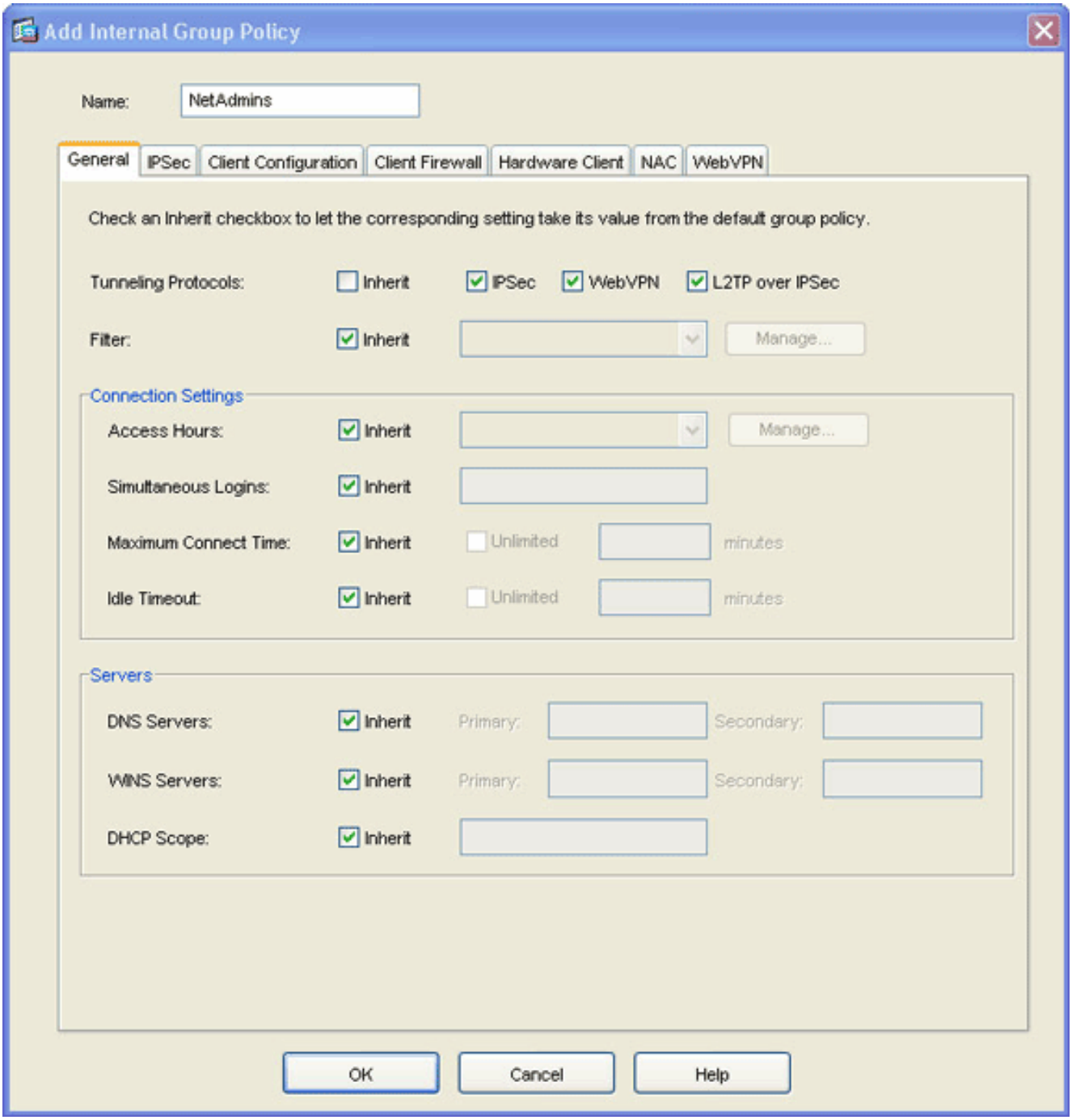
Stap 3. Maak een groepsbeleid en koppel het aan de poortdoorsturen lijst

Voltooi de volgende stappen om een groepsbeleid te maken en het te koppelen aan de lijst van het verzenden van havens:

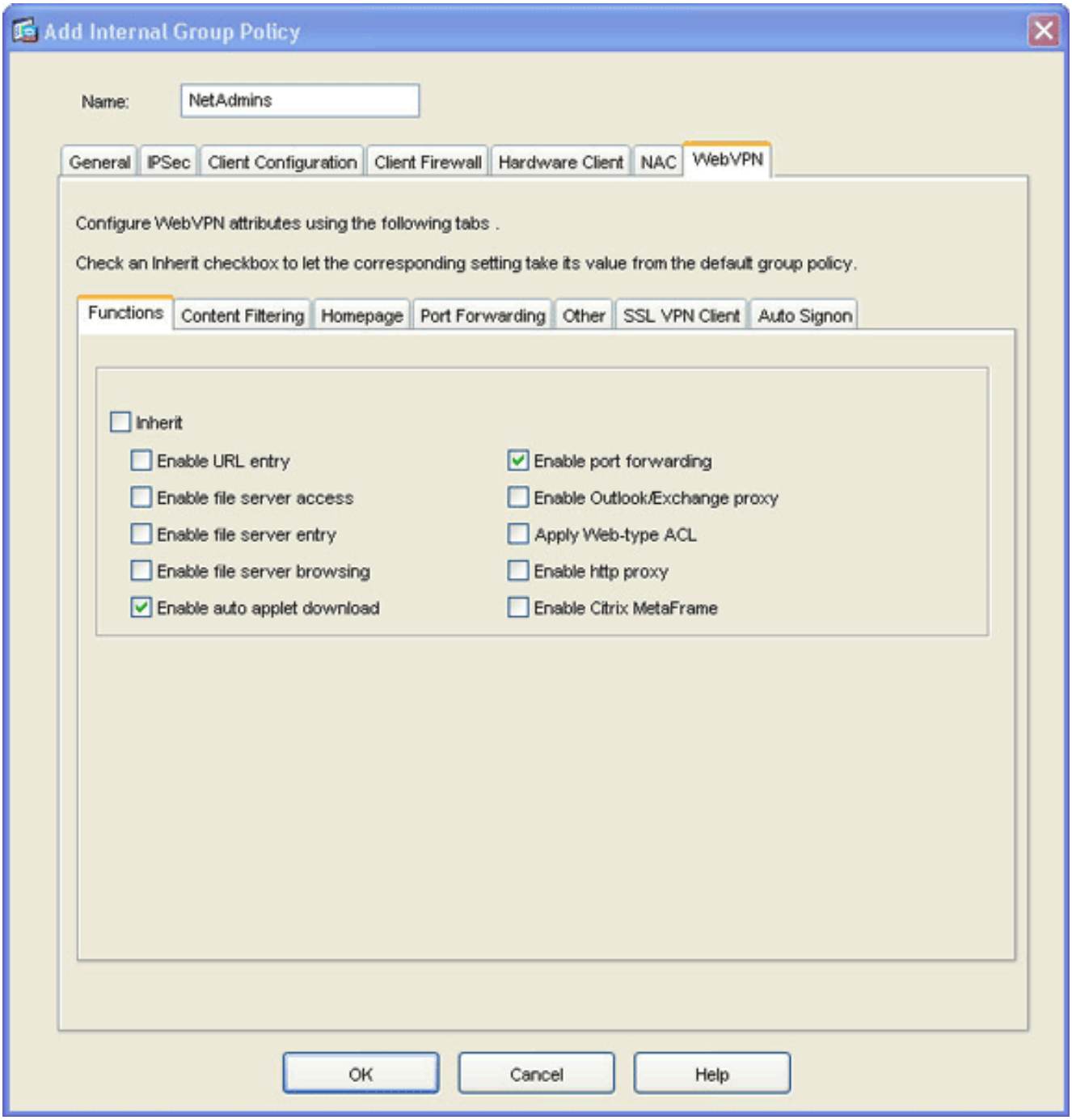
1. Vul het **groepsbeleid** uit en kies **het groepsbeleid**.



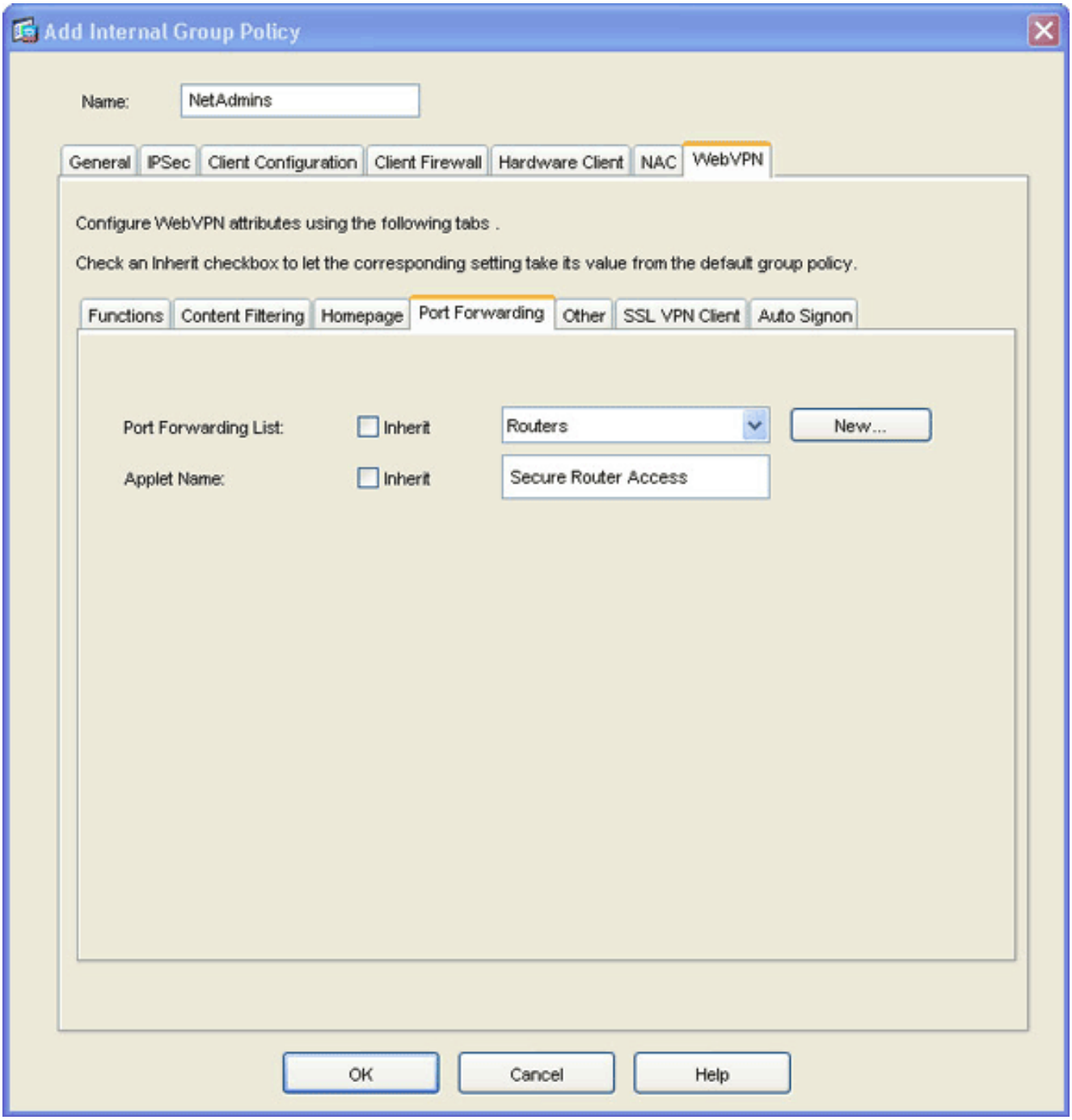
2. Klik op **Toevoegen** en kies **intern groepsbeleid**.Het dialoogvenster Intern groepsbeleid toevoegen verschijnt.



3. Voer een naam in of accepteer de standaardnaam van het groepsbeleid.
4. Schakel het vakje voor **inherkende** protocollen uit en controleer het vakje **WebeVPN** aan.
5. Klik op het tabblad **WebeVPN** boven in het dialoogvenster en klik vervolgens op het tabblad **Functies**.
6. Schakel het aanvinkvakje **Inherit uit** en controleer de aankruisvakjes voor **automatische applet inschakelen** en **Poorttransport** inschakelen zoals in dit beeld wordt weergegeven:



7. Klik ook in het tabblad WebVPN op het tabblad **Port Forwarding** en Schakel het vakje Port Forwarding List **Inherit**
uit.



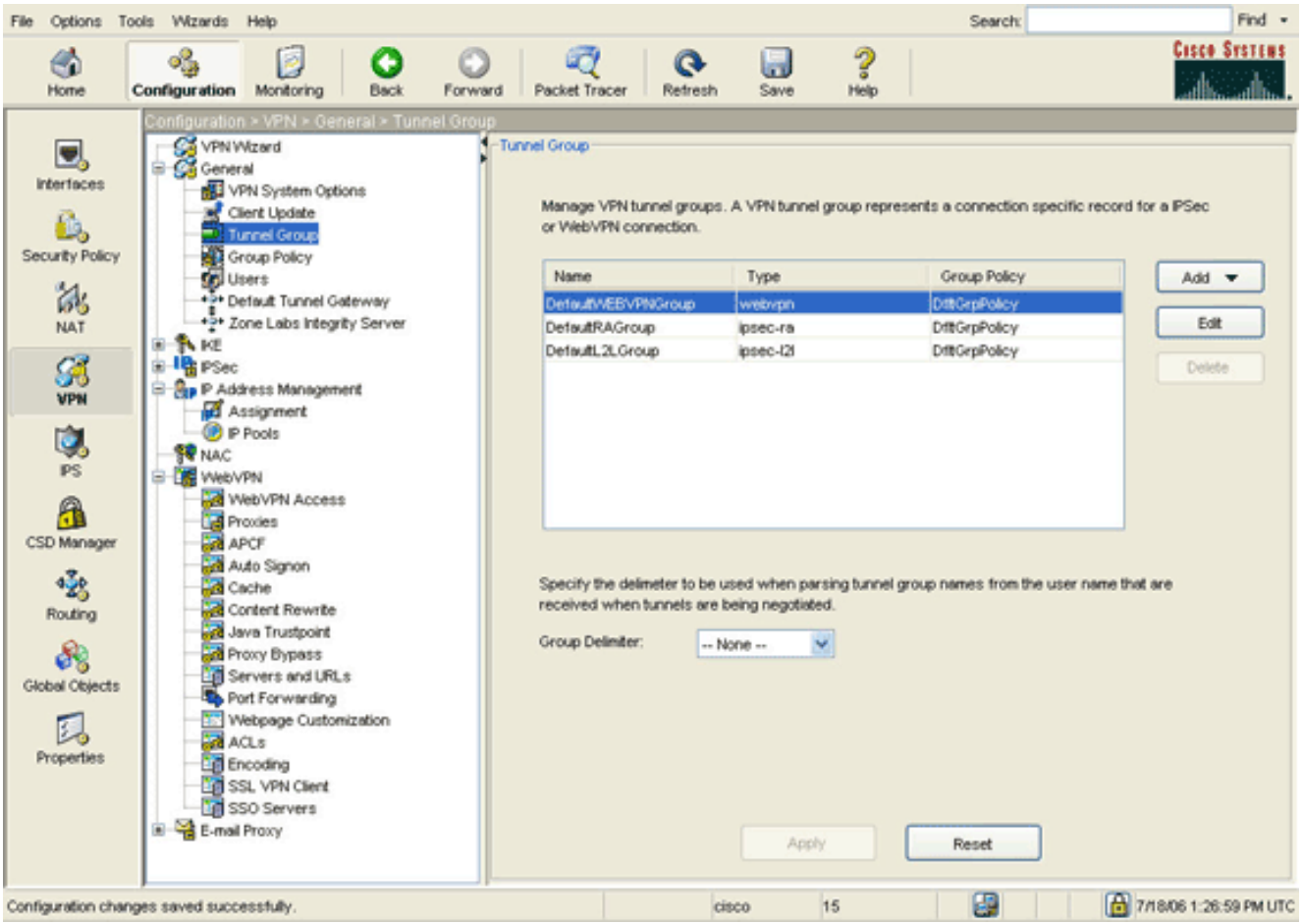
8. Klik op de vervolgkeuzelijst **Port Forwarding List** en kies de lijst **voor** poortverzending die u in Stap 2 hebt gemaakt.
9. Schakel het aankruisvakje Naam toepassen uit en verander de naam in het tekstveld.De client geeft de Applet Name weer bij een verbinding.
10. Klik op **OK** en vervolgens op **Toepassen**.
11. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

Stap 4. Maak een tunnelgroep en koppel het aan het groepsbeleid

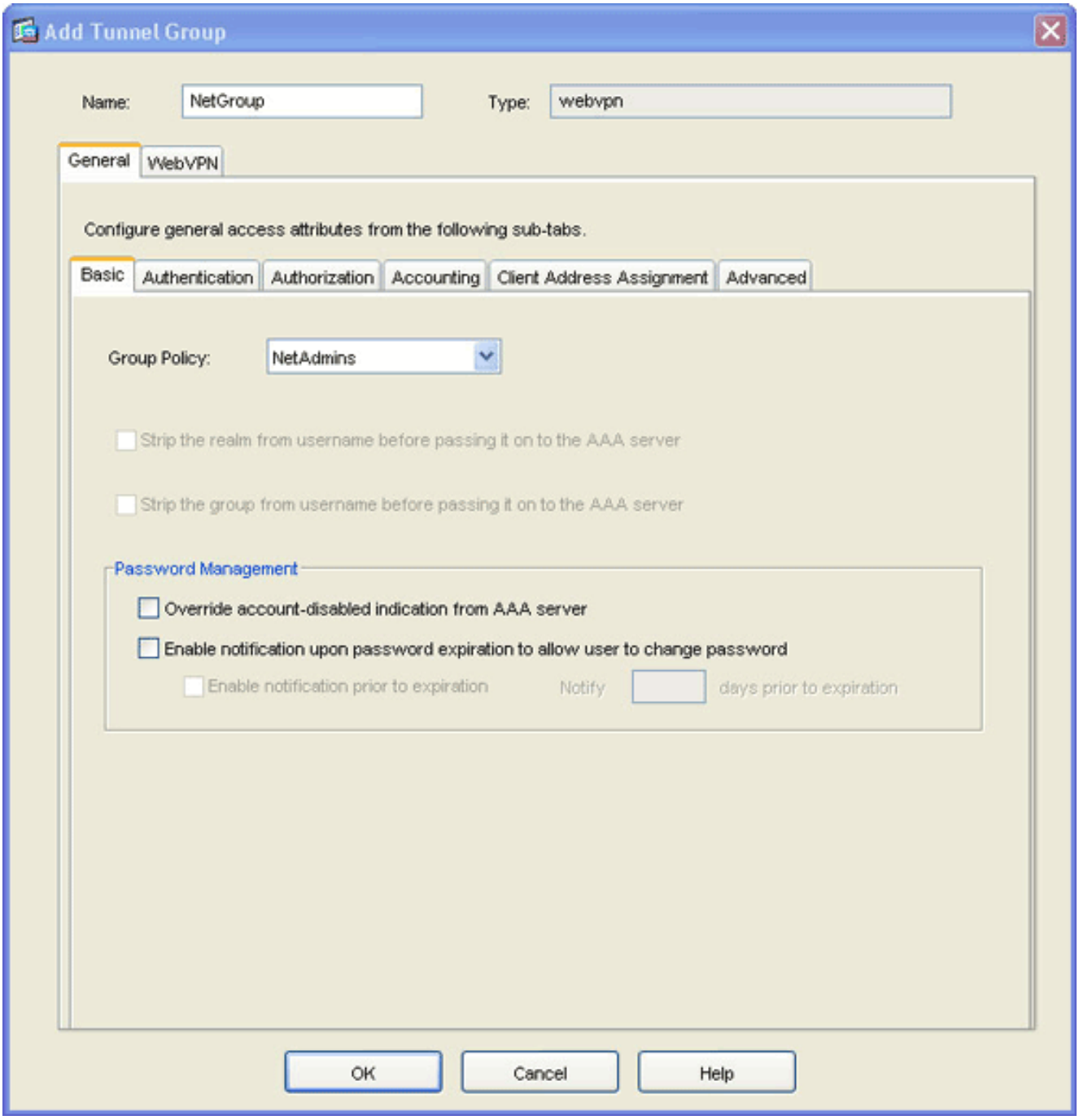
U kunt de standaardgroep *DefaultWebVPN* bewerken of een nieuwe tunnelgroep maken.

Voltooi de volgende stappen om een nieuwe tunnelgroep te maken:

1. Vul het **menu Algemeen uit** en kies **Tunnelgroep**.



2. Klik op **Add** en kies **WebVPN Access**.Het dialoogvenster Tunnelgroep toevoegen verschijnt.

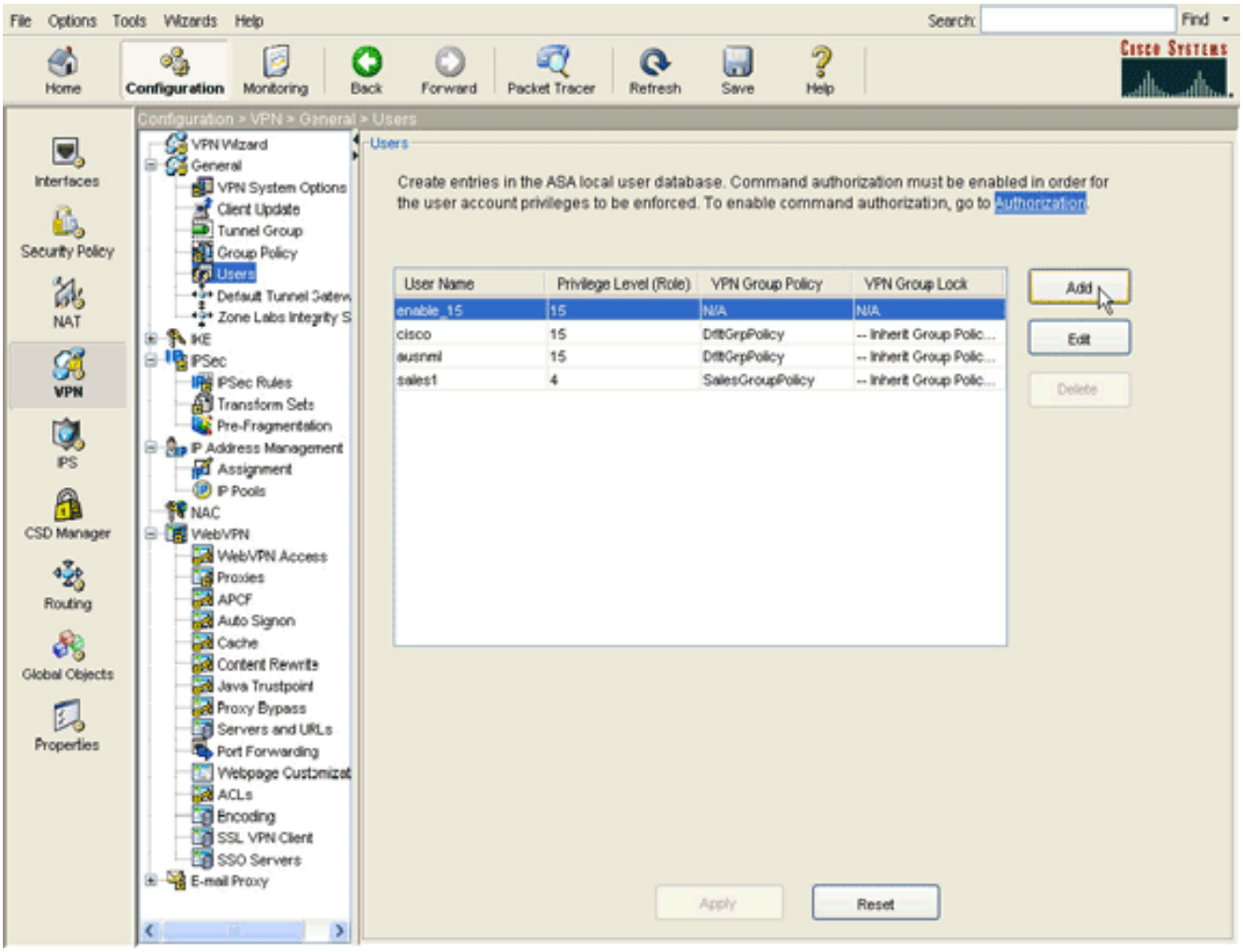


3. Voer een naam in het veld Naam in.
4. Klik op de vervolgkeuzelijst **Groepsbeleid** en kies het groepsbeleid dat u in Stap 3 hebt gemaakt.
5. Klik op **OK** en vervolgens op **Toepassen**.
6. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.De tunnelgroep, het groepsbeleid en de eigenschappen van de havenverzending zijn nu met elkaar verbonden.

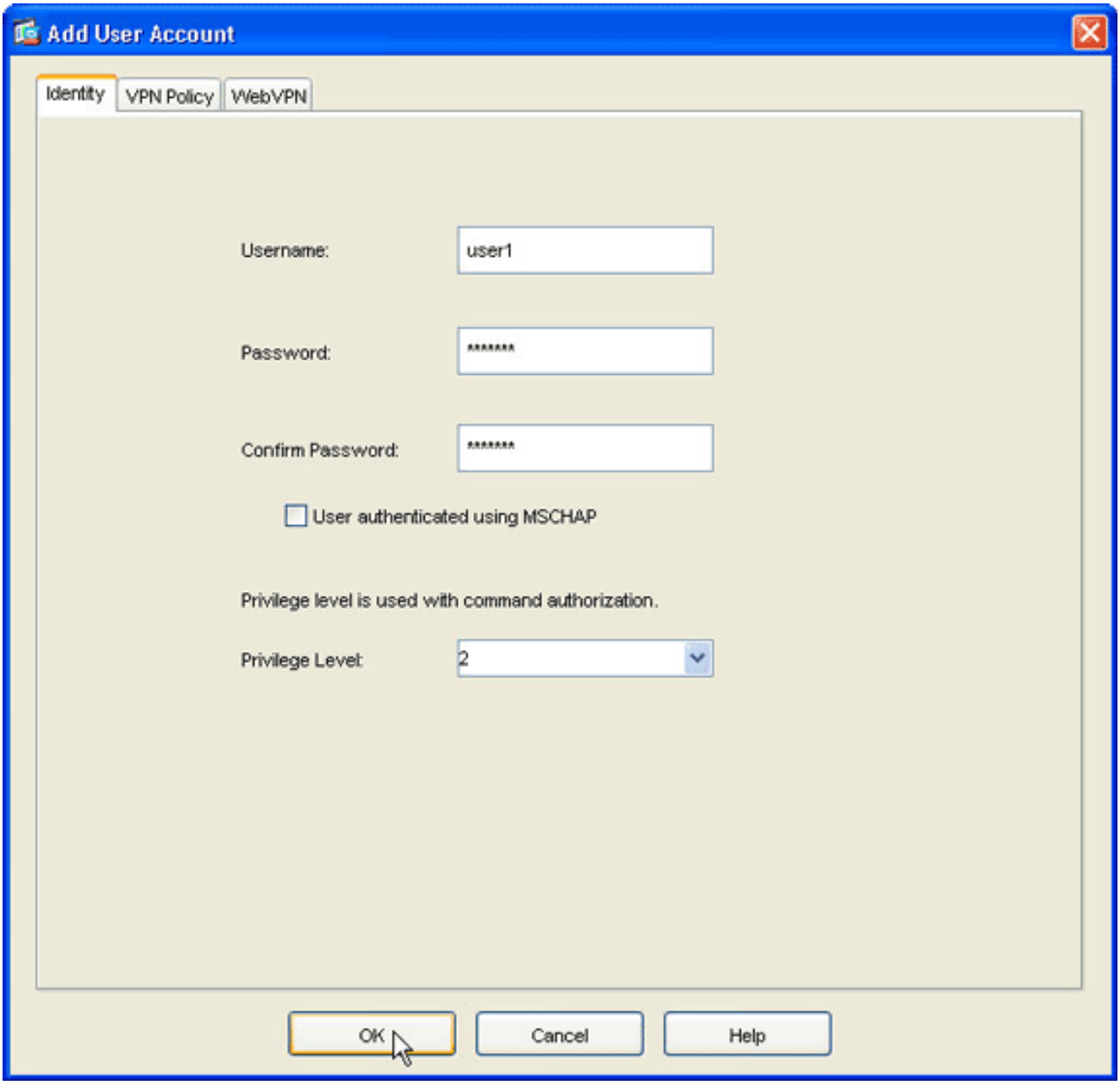
Stap 5. Maak een gebruiker en voeg die gebruiker toe aan het groepsbeleid

Voltooi de volgende stappen om een gebruiker te maken en die gebruiker aan het groepsbeleid toe te voegen:

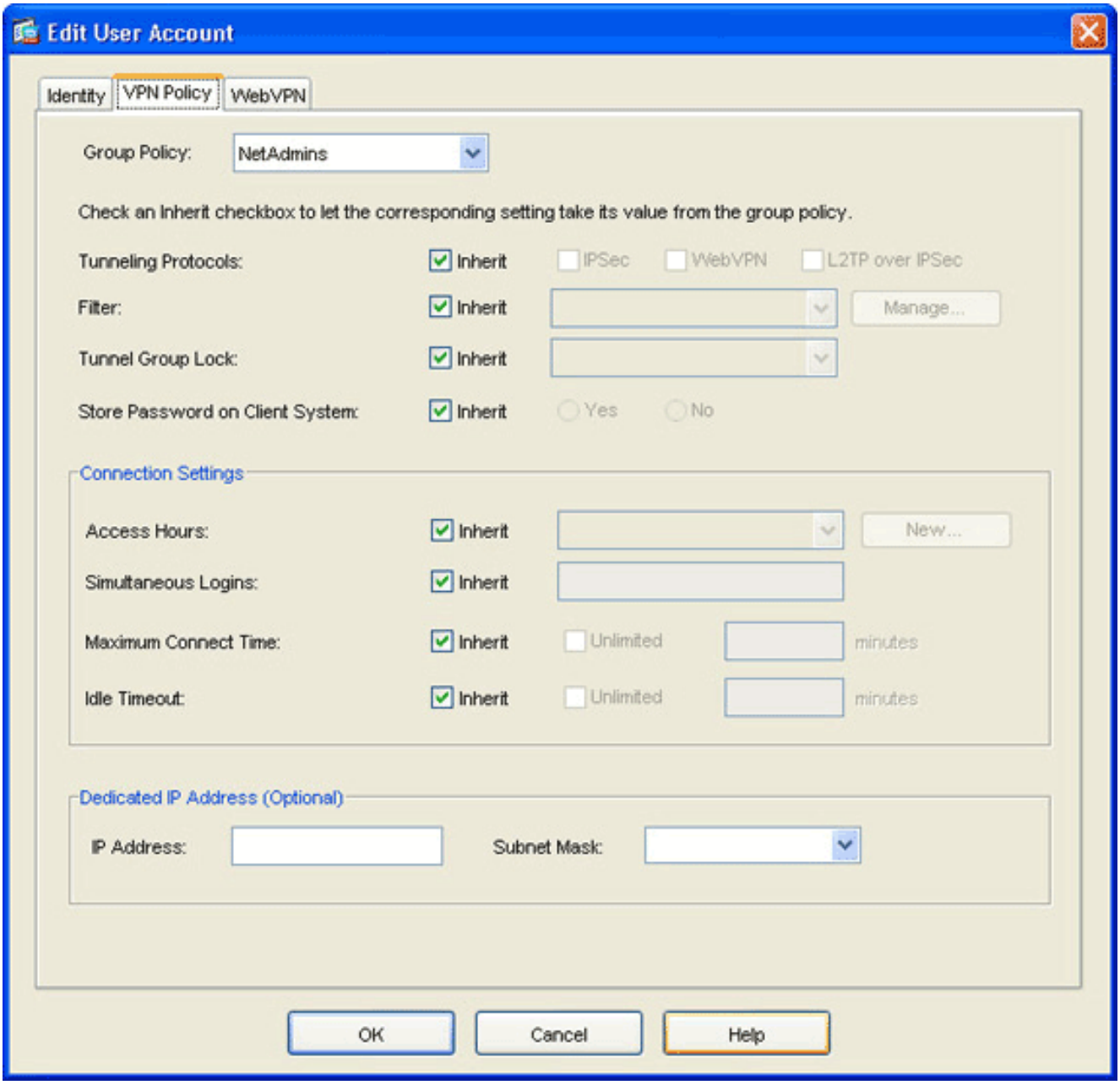
1. **Algemeen uitvouwen** en **gebruikers** kiezen.



2. Klik op de knop **Toevoegen**.Het dialoogvenster Gebruikersaccount toevoegen verschijnt.



3. Voer waarden in voor de gebruikersnaam, het wachtwoord en de informatie over toegangsrechten en klik vervolgens op het tabblad **VPN Policy**.



4. Klik op de vervolgkeuzelijst **Groepsbeleid** en kies het groepsbeleid dat u in Stap 3 hebt gemaakt.Deze gebruiker erft de eigenschappen en het beleid van WebVPN van het geselecteerde groepsbeleid.
5. Klik op **OK** en vervolgens op **Toepassen**.
6. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

Thin-Client SSL VPN-configuratie met CLI

ASA
ASA Version 7.2(1) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside

```
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!--- Output truncated  port-forward portforward 3044
10.2.2.2 telnet Telnet to R1
!--- Configure the set of applications that WebVPN
users !--- can access over forwarded TCP ports group-
policy NetAdmins internal
!--- Create a new group policy for enabling WebVPN
access group-policy NetAdmins attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
!--- Configure group policy attributes webvpn
  functions port-forward auto-download
!--- Configure group policies for WebVPN   port-forward
value portforward
!--- Configure port-forward to enable WebVPN
application access !--- for the new group policy  port-
forward-name value Secure Router Access
!--- Configure the display name that identifies TCP
port !--- forwarding to end users username user1
password tJsDL6po9m1UFs.h encrypted
username user1 attributes
 vpn-group-policy NetAdmins
!--- Create and add User(s) to the new group policy
http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart tunnel-group NetGroup type webvpn
tunnel-group NetGroup general-attributes
 default-group-policy NetAdmins
!--- Create a new tunnel group and link it to the group
policy 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 Web VPN on Outside interface port-forward
portforward 3044 10.2.2.2 telnet Telnet to R1 prompt
hostname context
```

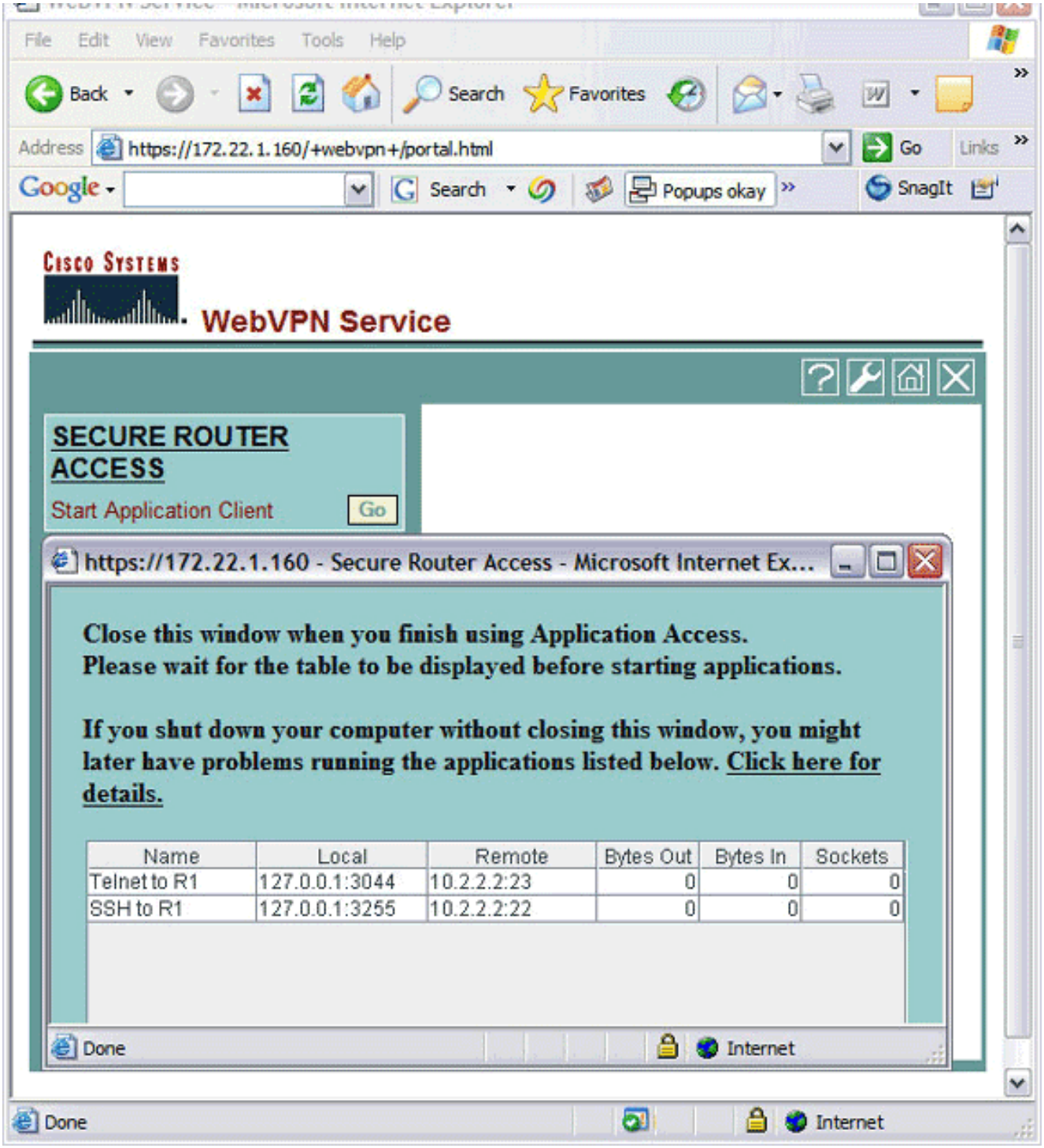
Verifiëren

Gebruik dit gedeelte om te controleren of de configuratie goed werkt.

Procedure

In deze procedure wordt beschreven hoe de geldigheid van de configuratie wordt bepaald en hoe de configuratie wordt getest.

1. Voer vanaf een clientwerkstation **https:// *externe_ASA_IP-adres in***; waar *buiten_ASA_IPAdjurk* de SSL URL van de ASA is.Zodra het digitale certificaat wordt geaccepteerd en de gebruiker is echt bevonden, verschijnt de webpagina voor WebVPN Service.

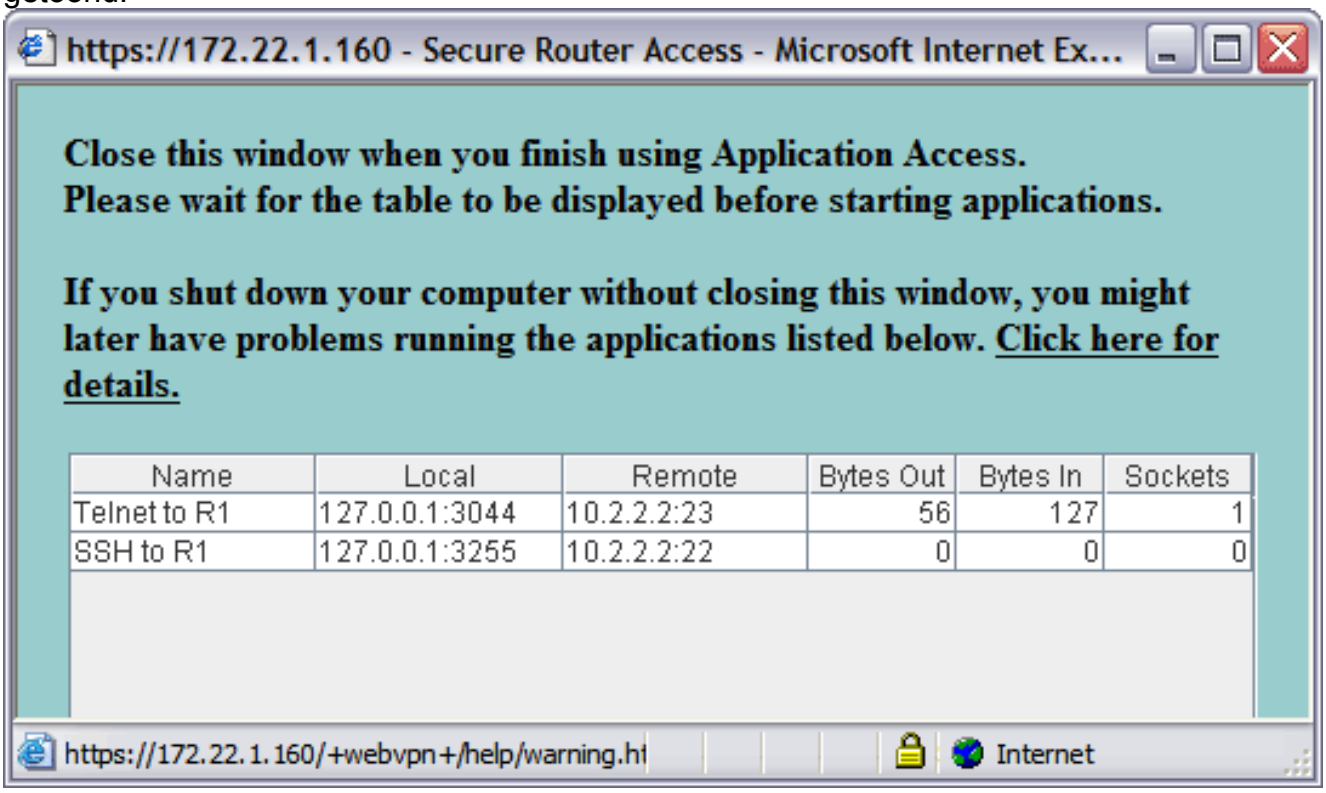


Het adres en de haveninformatie die nodig zijn om toegang tot de toepassing te krijgen verschijnt in de lokale kolom. De Bytes Out en Bytes In kolommen vertonen geen activiteit omdat de toepassing op dit moment niet is ingeroepen.

2. Gebruik de DOS-prompt of een andere Telnet-toepassing om een Telnet-sessie te starten.
3. Voer **telnet 127.0.0.1 3044** in **als** opdracht.**Opmerking:** deze opdracht geeft een voorbeeld van hoe u toegang kunt verkrijgen tot de lokale poort die in het WebVPN Service Web pagina-afbeelding in dit document is weergegeven. *Deze opdracht bevat geen colon (:).* Typ de opdracht zoals in dit document beschreven wordt.ASA ontvangt de opdracht over de beveiligde sessie en omdat het een kaart van de informatie opslaat, weet de ASA direct om de beveiligde teletensessie naar het in kaart gebrachte apparaat te openen.

Zodra u uw gebruikersnaam en wachtwoord hebt ingevoerd, is de toegang tot het apparaat voltooid.

4. Om de toegang tot het apparaat te controleren, controleert u de Bytes Out en Bytes in kolommen zoals in deze afbeelding wordt getoond:



Opdrachten

Verschillende **tonen** opdrachten worden geassocieerd met WebVPN. U kunt deze opdrachten uitvoeren op de opdrachtregel-interface (CLI) om statistieken en andere informatie weer te geven. Raadpleeg voor gedetailleerde informatie over opdrachten **voor het** weergeven van de configuratie van WebVPN.

Opmerking: Uitvoer Tolk (alleen geregistreerde klanten) (OIT) ondersteunt bepaalde **show**

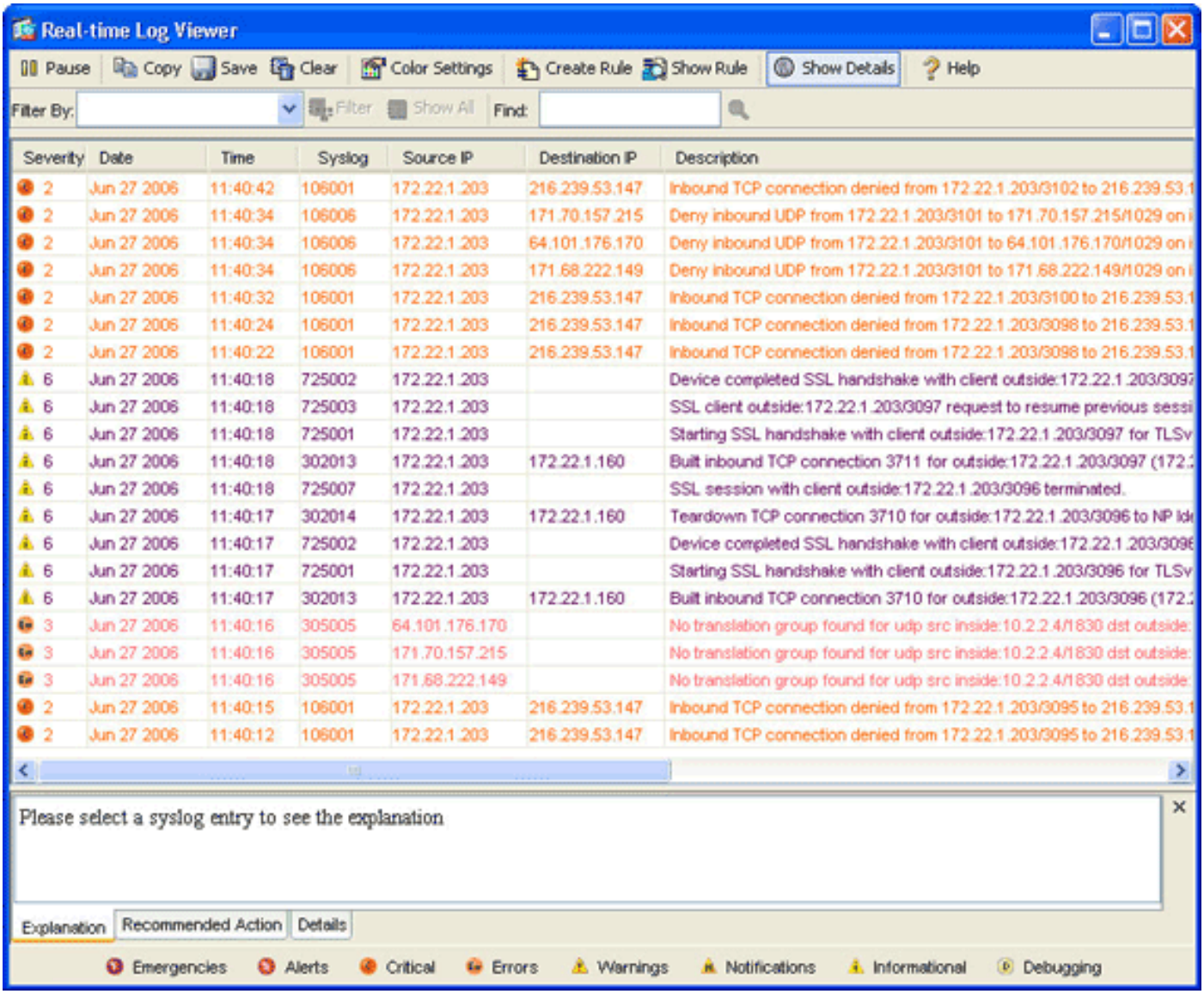
opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Is het SSL-handdrukproces voltooid?

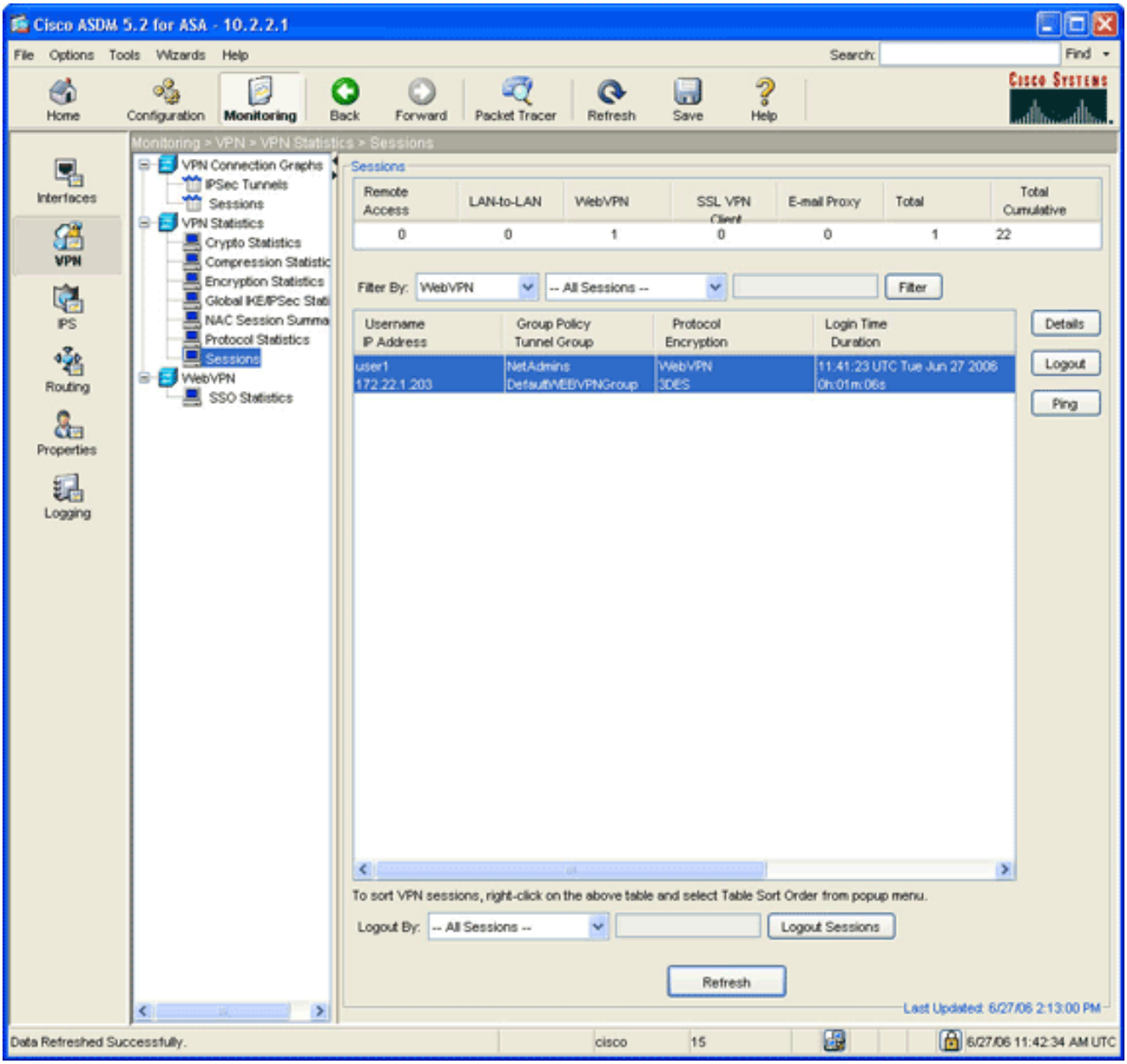
Zodra u verbinding met de ASA hebt gemaakt, controleer of het real-time logbestand de voltooiing van de SSL handdruk toont.



Is de SSL VPN Thin-Client functioneel?

Voltooi de volgende stappen om te controleren of de SSL VPN-client functioneel is:

1. Klik op **Monitoring** en klik vervolgens op **VPN**.
2. **VPN-statistieken** uitvouwen en op **sessies** klikken.Uw SSL VPN Thin-Client-sessie moet in de sessielijst worden weergegeven. Vergeet niet via WebVPN te filteren, zoals in deze afbeelding:



Opdrachten

Meerdere **debug** opdrachten zijn gekoppeld aan WebVPN. Raadpleeg voor gedetailleerde informatie over deze opdrachten het gebruik van Debug Commands van WebVPN.

Opmerking: het gebruik van **debug**-opdrachten kan een negatieve invloed hebben op uw Cisco-apparaat. Voordat u **debug**-opdrachten gebruikt, raadpleegt u Belangrijke informatie over Debug Commands.

Gerelateerde informatie

- Clientloze SSL VPN (WebVPN) op ASA Configuration Voorbeeld
- SSL VPN-client (SVC) op ASA met ASDM Configuratievoorbeeld
- Adaptieve security applicaties van Cisco ASA 5500 Series
- ASA met WebVPN en Single aanmelding bij gebruik van ASDM en NTLMv1 Configuration Voorbeeld
- Technische ondersteuning en documentatie – Cisco Systems