Configuratie van Clientless SSL VPN (WebVPN) op Cisco IOS met DSM

Inhoud

Inleiding

Clientless SSL VPN (WebexVPN) stelt een gebruiker in staat om bronnen in het bedrijf LAN veilig te benaderen vanaf een willekeurige plaats met een SSL-enabled Webbrowser. De gebruiker verklaart eerst een gateway van WebVPN die dan de gebruiker toegang tot van tevoren gevormde netwerkmiddelen toestaat. WebVPN-gateways kunnen worden geconfigureerd op Cisco IOS mobiele routers, Cisco adaptieve security applicaties (ASA), Cisco VPN 3000 Concentrators en de Cisco WebVPN servicesmodule voor Catalyst 6500 en 7600 routers.

Secure Socket Layer (SSL) Virtual Private Network (VPN) technologie kan op Cisco-apparaten worden geconfigureerd in drie hoofdmodi: Clientloze SSL VPN (WebeVPN), Thin-Client SSL VPN (Port Forwarding) en SSL VPN-clientmodus (SVC). Dit document demonstreert de configuratie van WebVPN op Cisco IOS-routers.

Opmerking: Wijzig de IP-domeinnaam of de host-naam van de router niet, omdat dit een

regeneratie van het zelf-getekende certificaat veroorzaakt en voorrang heeft op het geconfigureerde trustpunt. Regeneratie van het zelf getekende certificaat veroorzaakt verbindingsproblemen als de router voor WebeVPN is geconfigureerd. WebVPN bindt de SSL trustpoint naam aan de gateway van WebVPN. Daarom, als een nieuw zelfgetekend certificaat wordt uitgegeven, past de nieuwe naam van het vertrouwenspunt niet aan de configuratie van WebVPN en kunnen de gebruikers geen verbinding maken.

Opmerking: Als u de **IP https-Secure server** opdracht uitvoert op een WebVPN-router die een aanhoudend zelfgetekend certificaat gebruikt, wordt er een nieuwe RSA-toets gegenereerd en wordt het certificaat ongeldig. Er wordt een nieuw knooppunt gemaakt, dat SSL WebVPN breekt. Als de router die de persistente zichzelf-ondertekende certificatenherstart gebruikt nadat u de **ip https-Secure server** opdracht hebt uitgevoerd, komt dezelfde kwestie voor.

Raadpleeg Thin-Client SSL VPN (WebVPN) IOS Configuration Voorbeeld met DSM om meer te weten te komen over de client-SSL VPN.

Raadpleeg SSL VPN Client (SVC) op IOS met het Voorbeeld van de Configuration om meer te weten te komen over de SSL VPN-client.

SSL VPN loopt op deze Cisco routerplatforms:

- Cisco 870, 1811, 1841, 2801, 2811, 2821 en 2851 Series routers
- Cisco 3725, 3745, 3825, 3845, 7200 en 7301 Series routers

Voorwaarden

Vereisten

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

- Een geavanceerde afbeelding van Cisco IOS-softwarerelease 12.4(6)T of hoger
- Een van de Cisco-routerplatforms die in de Inleiding zijn vermeld

Gebruikte componenten

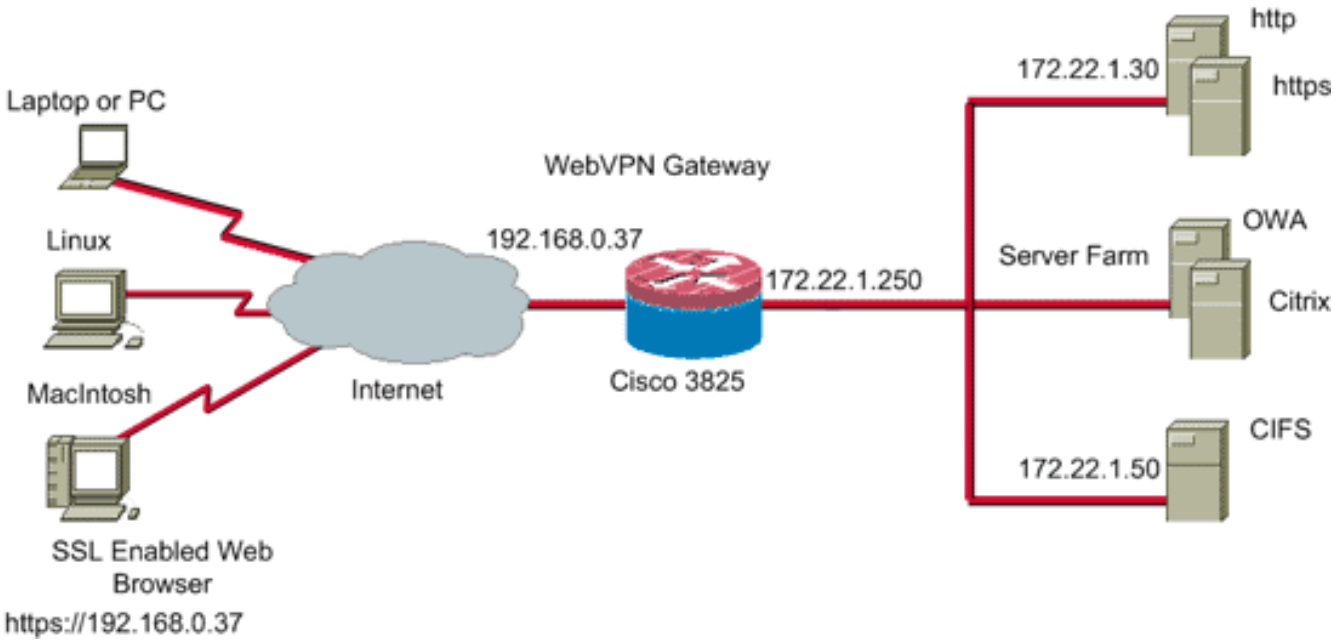
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 3825 router
- Advanced Enterprise-softwarerelease 12.4(9)T
- Cisco Router en Security Devices Manager (DSM) - versie 2.3.1

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. De IP adressen die in dit voorbeeld worden gebruikt worden genomen van RFC 1918 adressen die privaat en niet legaal zijn om op het internet te gebruiken.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Conventies

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

Preconfiguratie van taken

Voltooi de volgende taken voordat u start:

1. Configureer een naam van de host en de domeinnaam.
2. Configureer de router voor DSM. Cisco vervoert sommige routers met een voorgeïnstalleerd exemplaar van PDM.Als Cisco DSM niet reeds op uw router is geladen, kunt u een gratis exemplaar van de software verkrijgen van de Software Download (geregistreerde klanten slechts). U moet een CCO-account met een servicecontract hebben. Raadpleeg voor gedetailleerde informatie over de installatie en configuratie van het SDM de router en de veiligheidsapparaat Manager van Cisco.
3. Configureer de juiste datum, tijd en tijdzone voor de router.

WebVPN configureren op Cisco IOS

U kunt meer dan één WebVPN gateway hebben geassocieerd met een apparaat. Elke WebVPN gateway is verbonden aan slechts één IP adres op de router. U kunt meer dan één WebVPN-context maken voor een bepaalde WebVPN-gateway. Om individuele contexten te identificeren, voorzien elke context van een unieke naam. Eén beleidsgroep kan slechts met één WebVPN-context worden geassocieerd. De beleidsgroep beschrijft welke bronnen in een bepaalde WebVPN-context beschikbaar zijn.

Voltooi deze stappen om WebVPN op Cisco IOS te configureren:

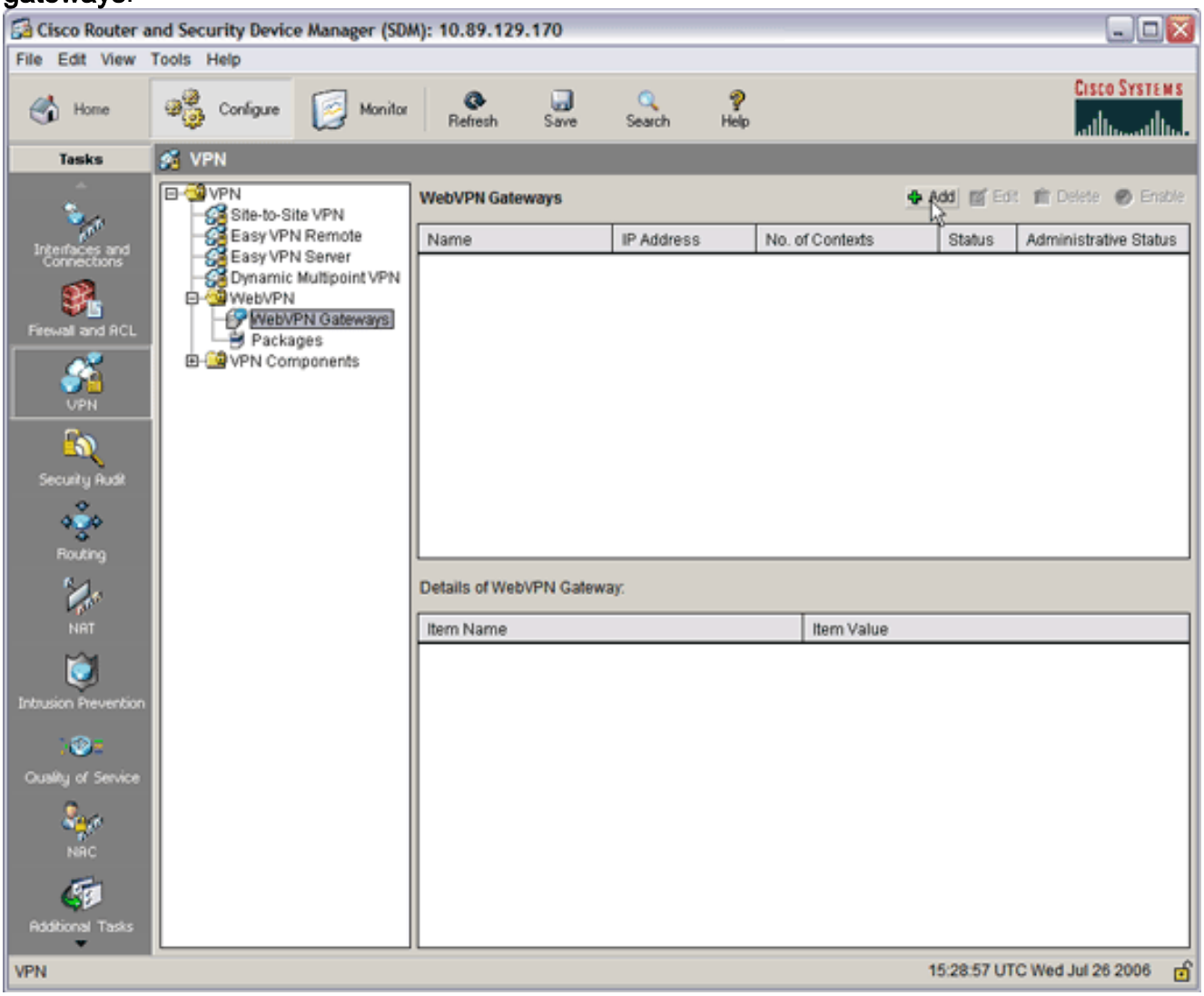
1. De WebVPN-gateway configureren
2. Configureer de voor de beleidsgroep toegestane bronnen
3. De Webex Policy Group configureren en de bronnen selecteren
4. De WebVPN-context configureren

5. De gebruikersdatabase en de verificatiemethode configureren

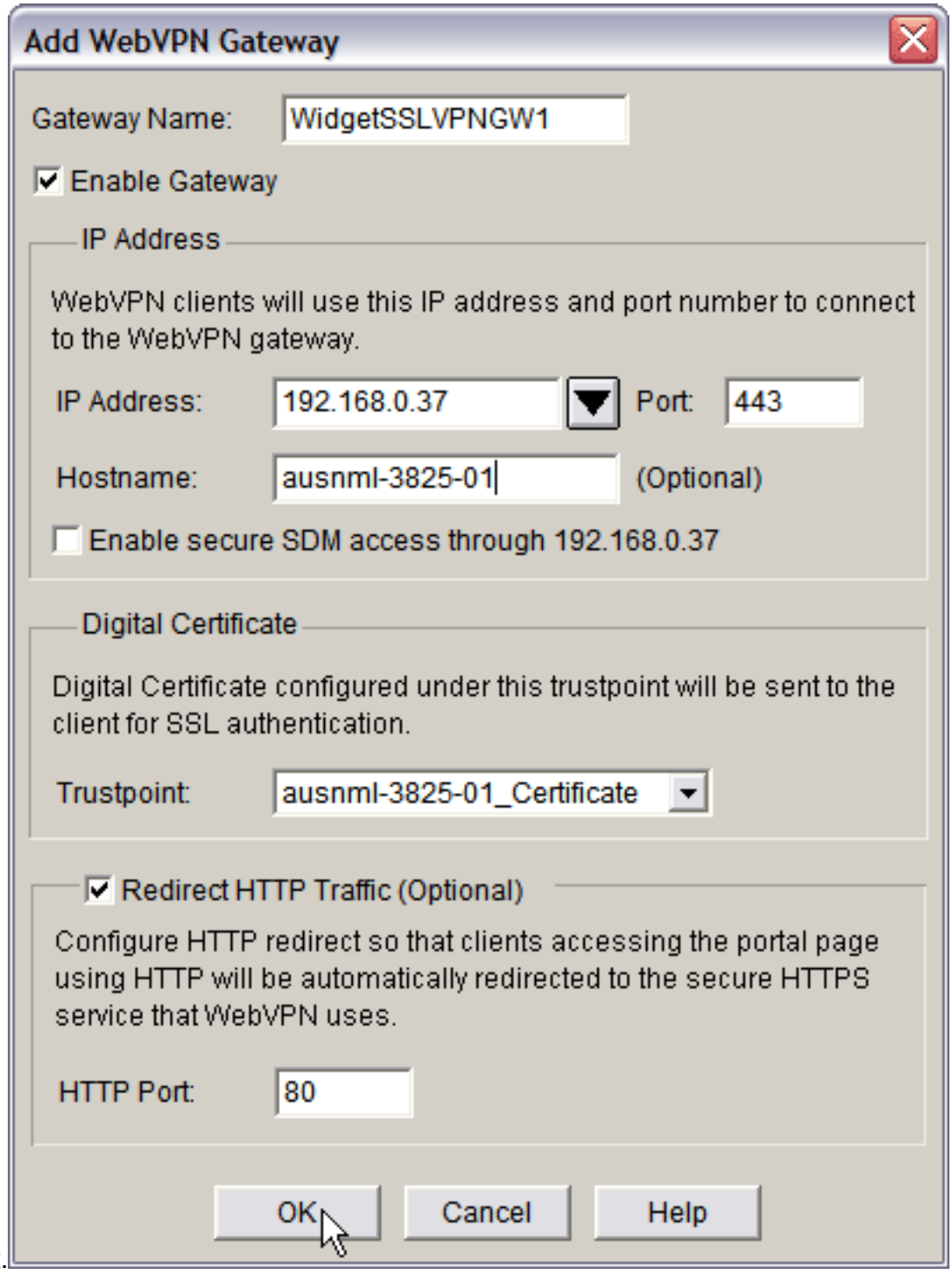
Stap 1. Het configureren van de WebVPN-gateway

Volg deze stappen om de gateway van WebVPN te configureren:

1. Binnen de toepassing sm, klik **Configureren**, en klik dan op **VPN**.
2. Vul **WebVPN** uit en kies **WebVPN gateways**.



3. Klik op **Add** (Toevoegen).Het dialoogvenster Webex Gateway toevoegen



verschijnt.

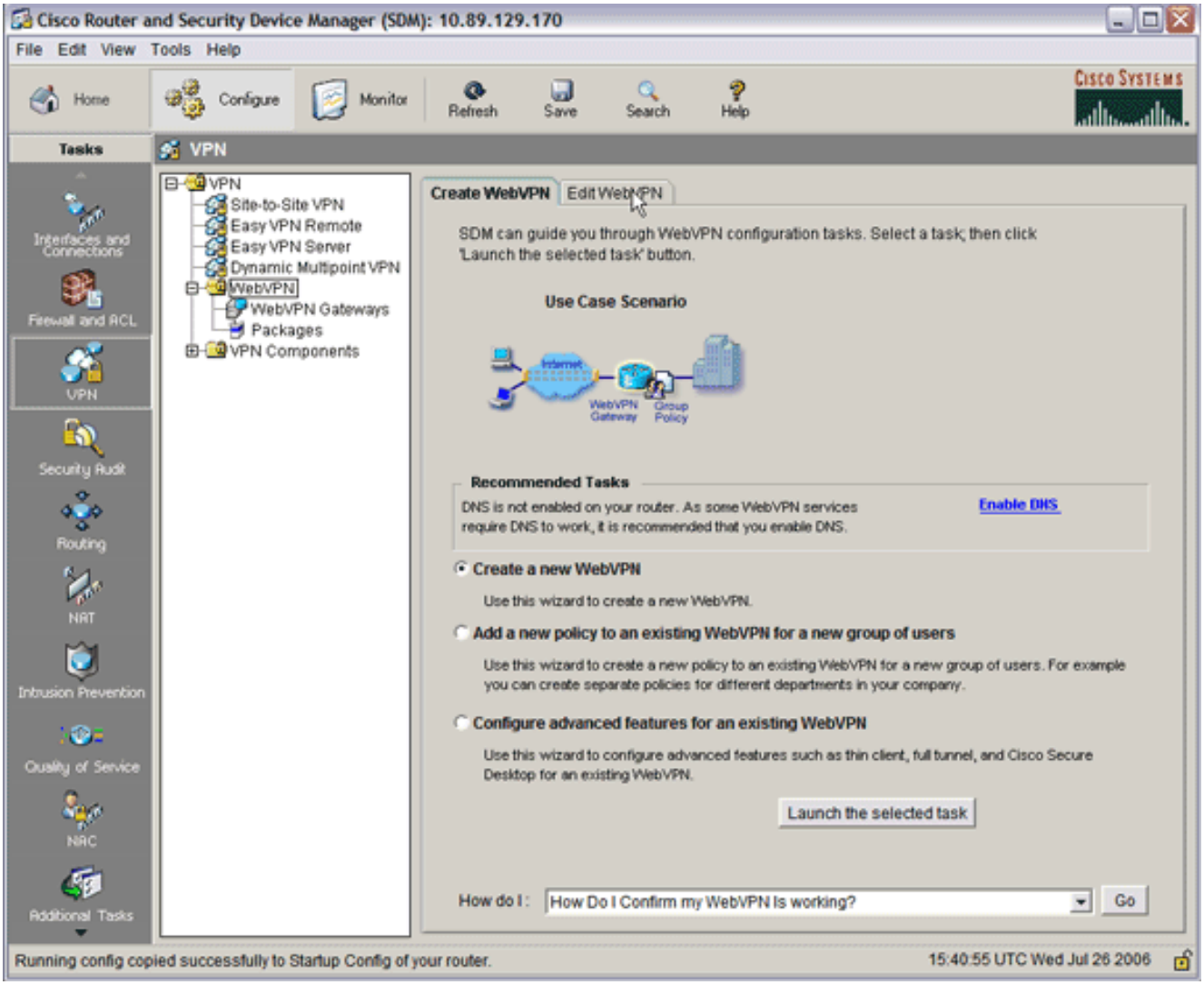
4. Voer waarden in in de velden Gateway Name en IP Address en controleer vervolgens het vakje **Enable Gateway**.
5. Controleer het aanvinkvakje **HTTP**-verkeer **omleiden** en klik vervolgens op **OK**.
6. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

Stap 2. Configureer de voor de beleidsgroep toegestane middelen

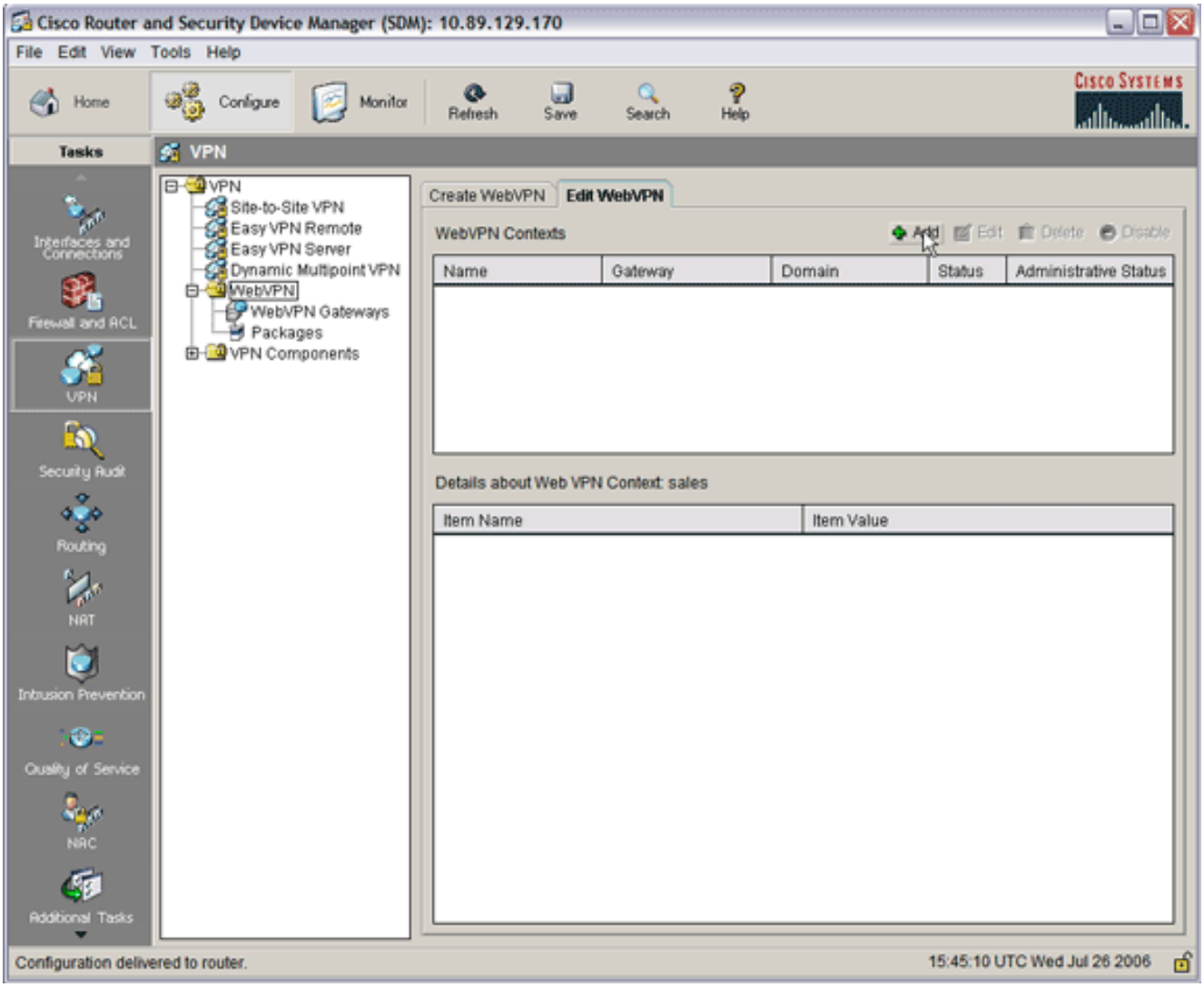
Om het gemakkelijker te maken om middelen aan een beleidsgroep toe te voegen, kunt u de middelen configureren voordat u de beleidsgroep maakt.

Voltooi deze stappen om de aan de beleidsgroep toegestane middelen te configureren:

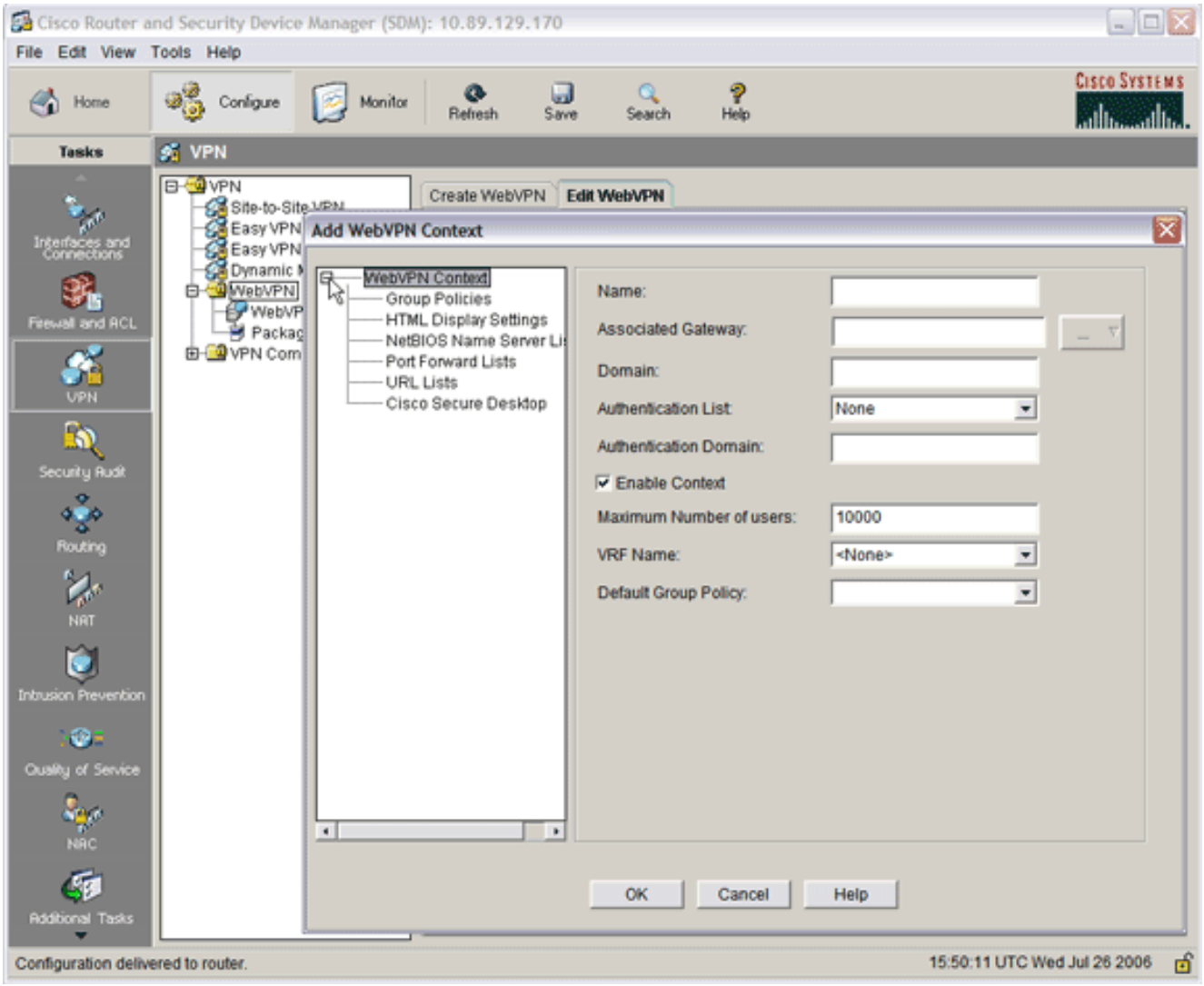
1. Klik op **Configureren** en vervolgens op **VPN**.



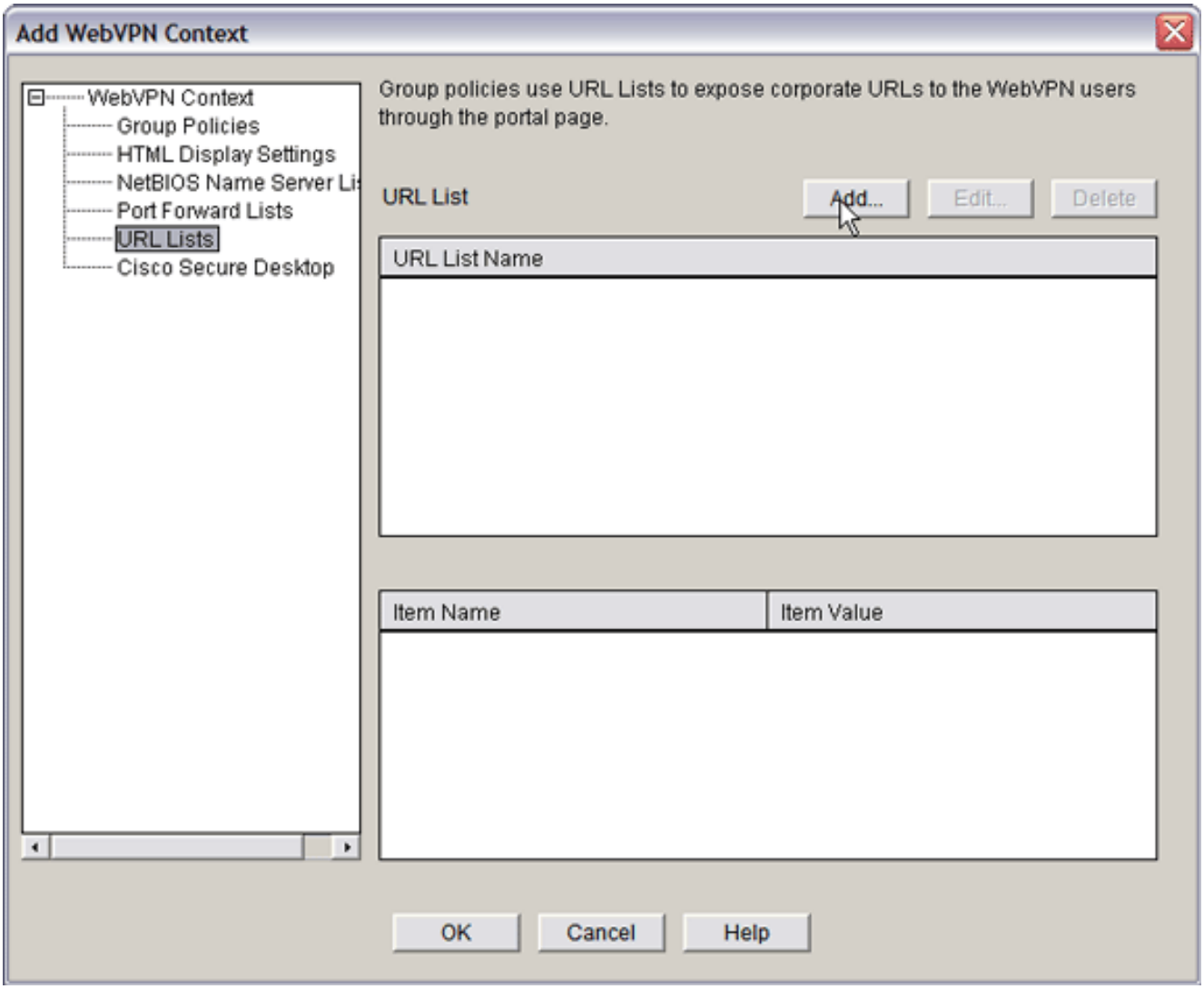
2. Kies **WebeVPN** en klik vervolgens op het tabblad **WebVPN bewerken**.**Opmerking:** WebVPN geeft u toegang tot HTTP, HTTPS, Windows-bestand dat doorbladert via het CIFS-protocol (Common Internet File System) en
Citrix.



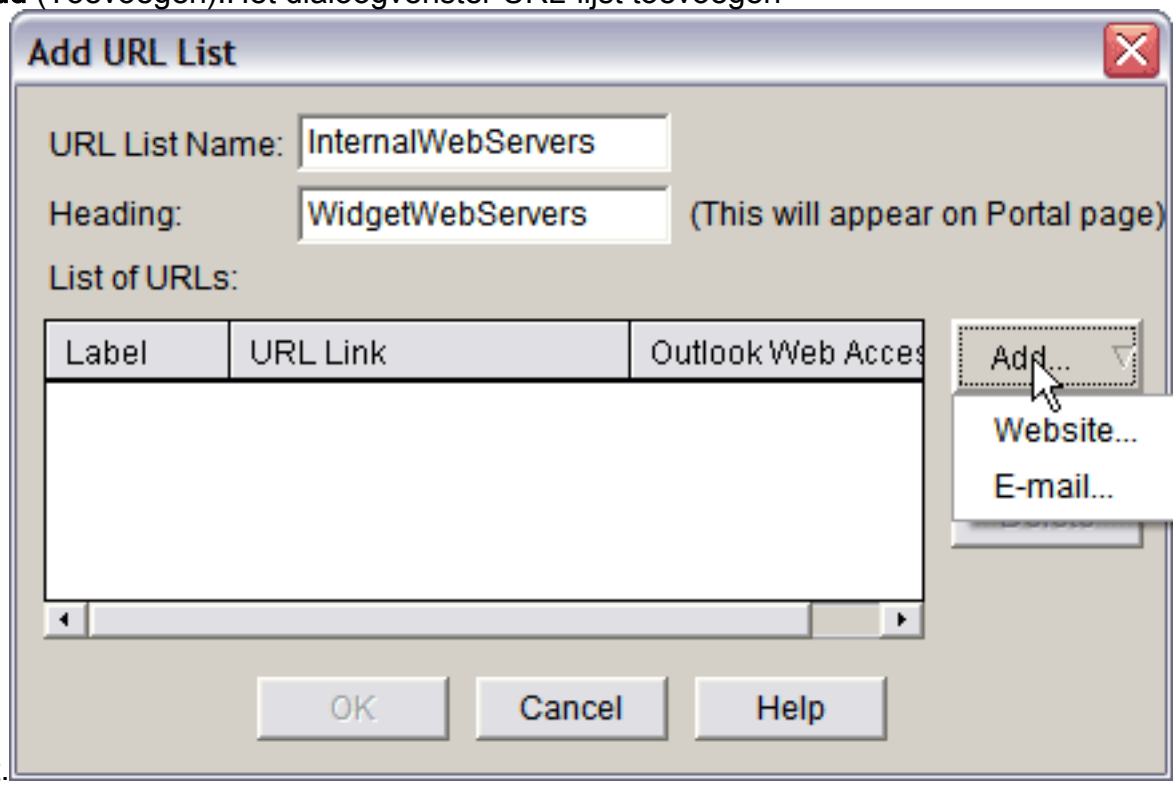
3. Klik op **Add** (Toevoegen).Het dialoogvenster Webex Context toevoegen verschijnt.



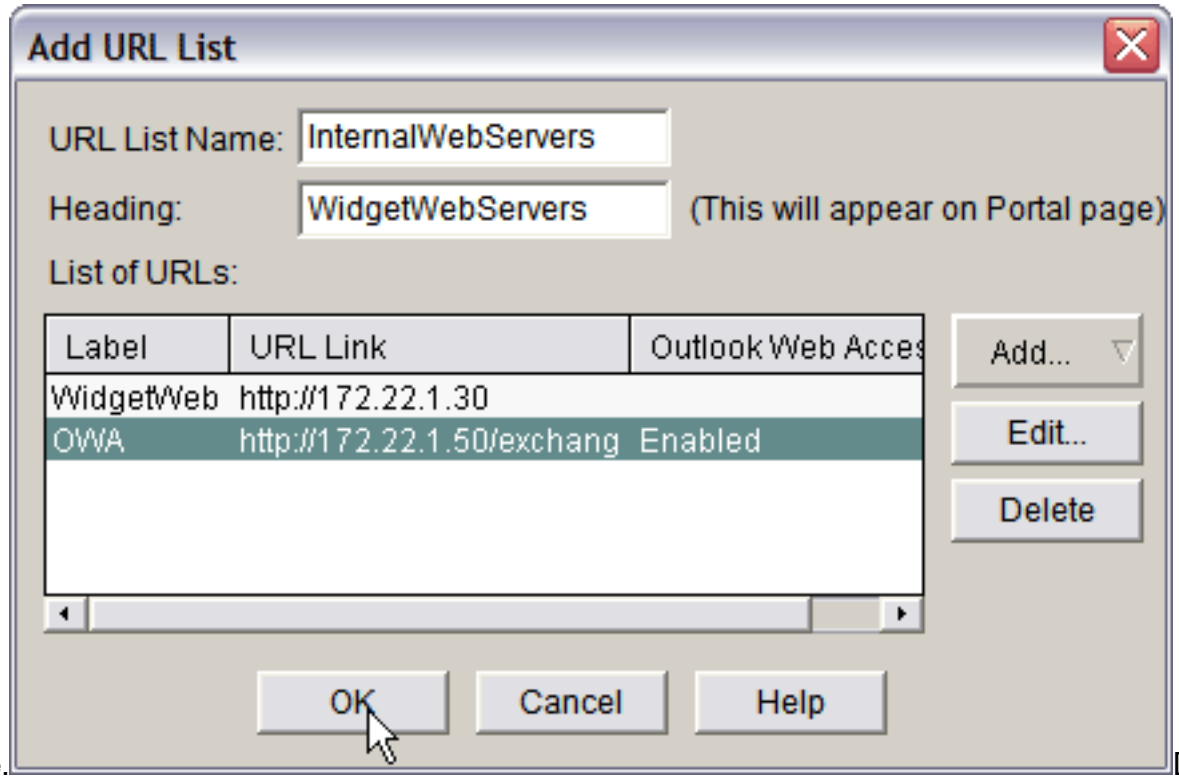
4. Vul **WebVPN-context uit** en kies **URL-lijsten**.



5. Klik op **Add** (Toevoegen).Het dialoogvenster URL-lijst toevoegen verschijnt.

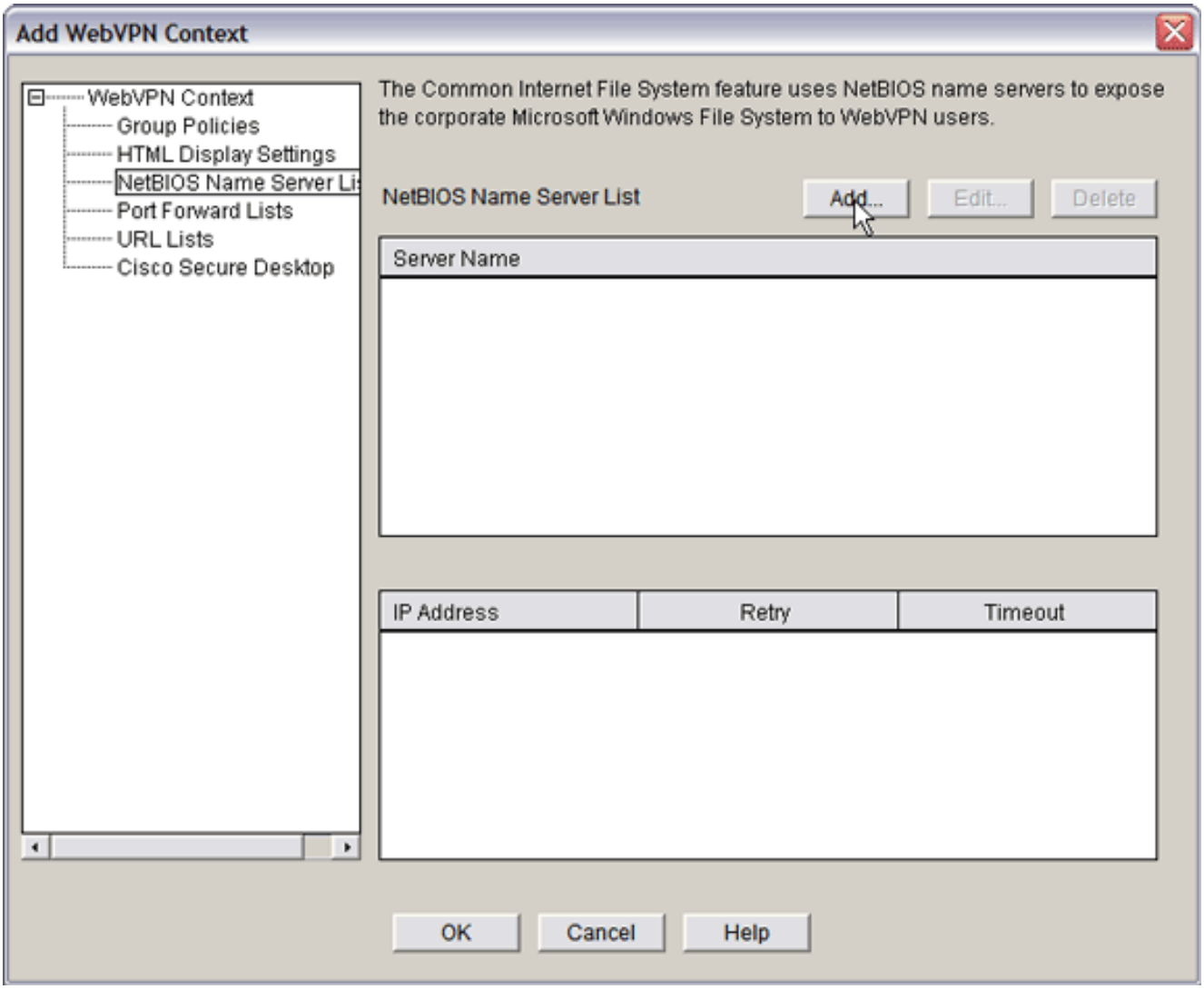


6. Voer waarden in in de velden Naam en Rubriek van de URL.
7. Klik op **Toevoegen** en kies

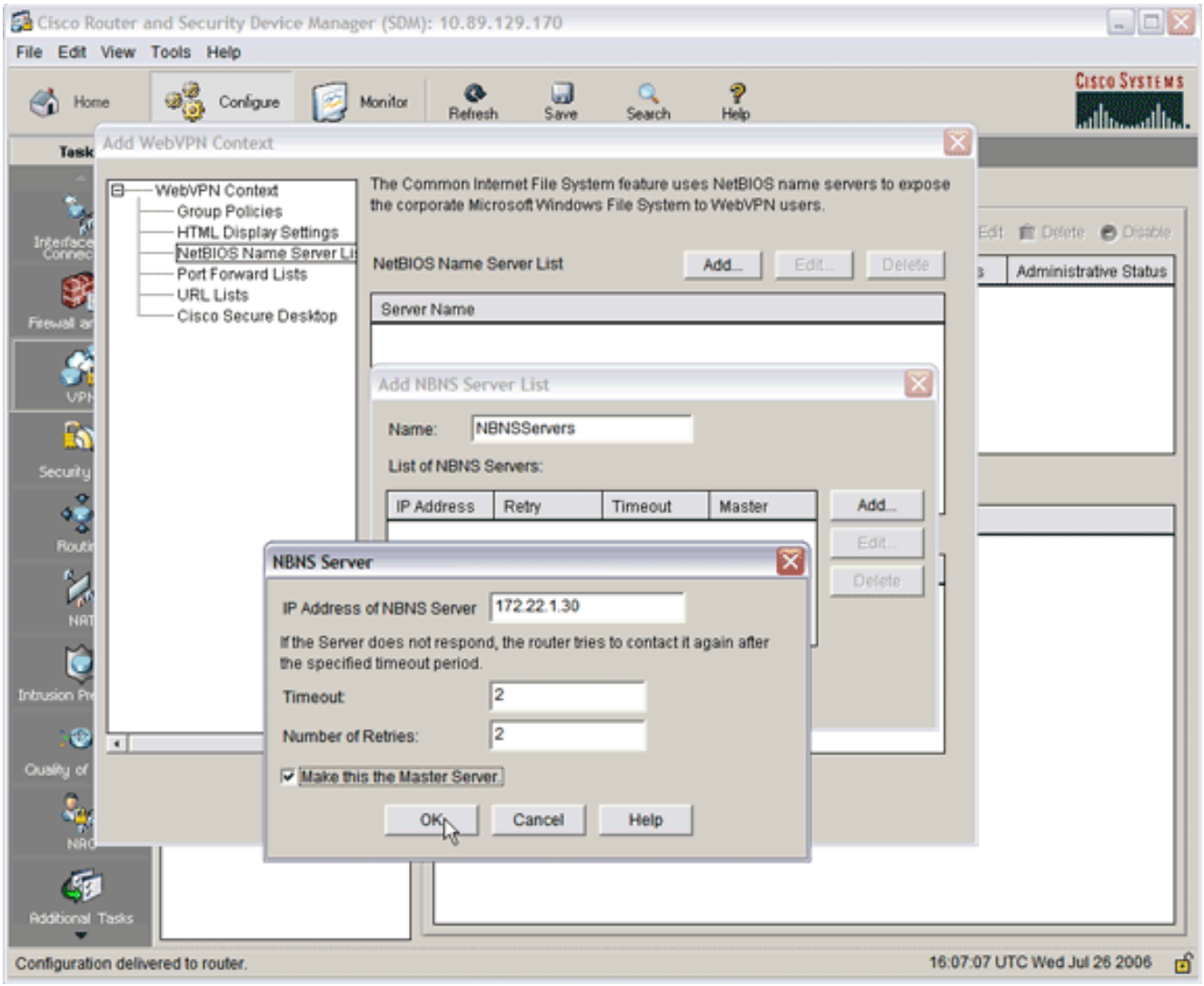


Website.Deze lijst bevat alle HTTP- en HTTPS-webservers die u voor deze WebVPN-verbinding beschikbaar wilt maken.

8. Als u toegang voor Outlook Web Access (OWA) wilt toevoegen, klikt u op **Add**, kiest u **E-mail** en vervolgens klikt u op **OK** nadat u alle gewenste velden hebt ingevuld.
9. Om Windows-bestand door CIFS te laten bladeren, kunt u eerst een NetConfiguration Name Service (NBS)-server aanwijzen en vervolgens de juiste aandelen in het Windows-domein configureren.Kies in de lijst WebVPN Context **van** de **NetConfiguration Name Server-lijsten**.



Klik op **Add** (Toevoegen).Het dialoogvenster NBS-serverlijst toevoegen verschijnt.Voer een naam in voor de lijst en klik op **Toevoegen**.Het dialoogvenster NBS Server verschijnt.

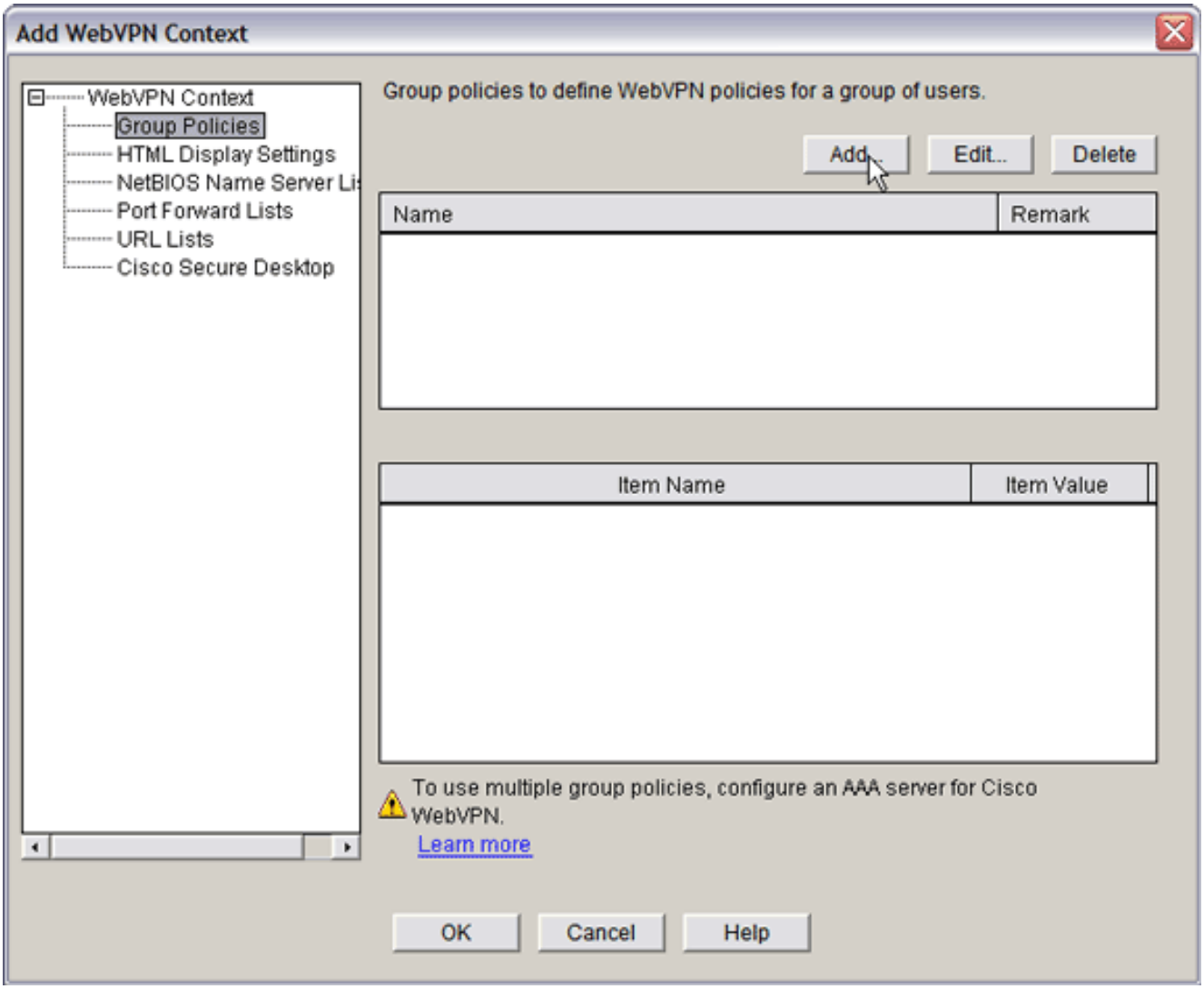


Indien van toepassing: controleer **Make this the Master Server** check box.Klik op **OK** en vervolgens op **OK**.

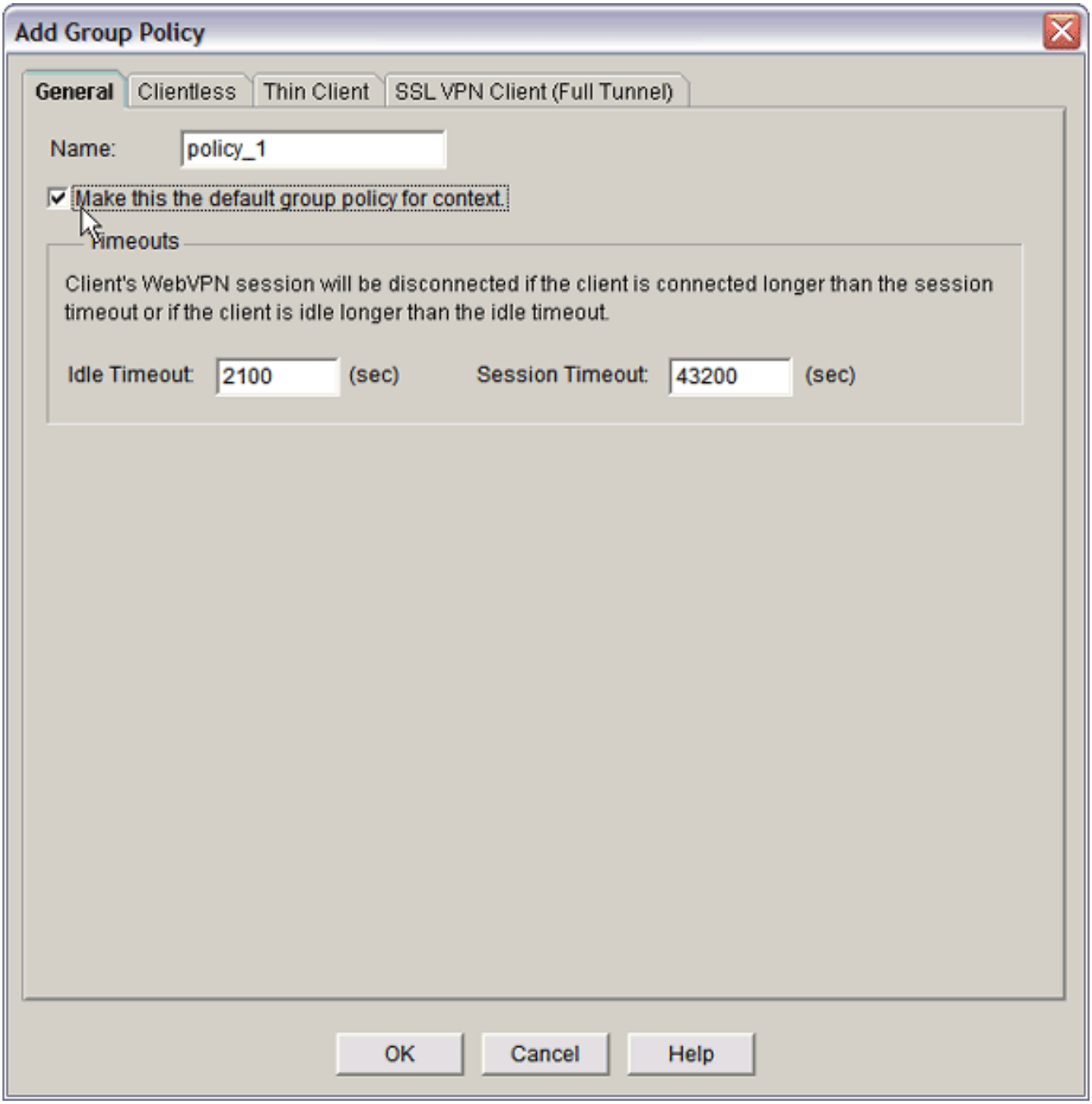
Stap 3. Het configureren van de WebeVPN-beleidsgroep en het selecteren van de bronnen

Voltooi deze stappen om de WebeVPN-beleidsgroep te configureren en de bronnen te selecteren:

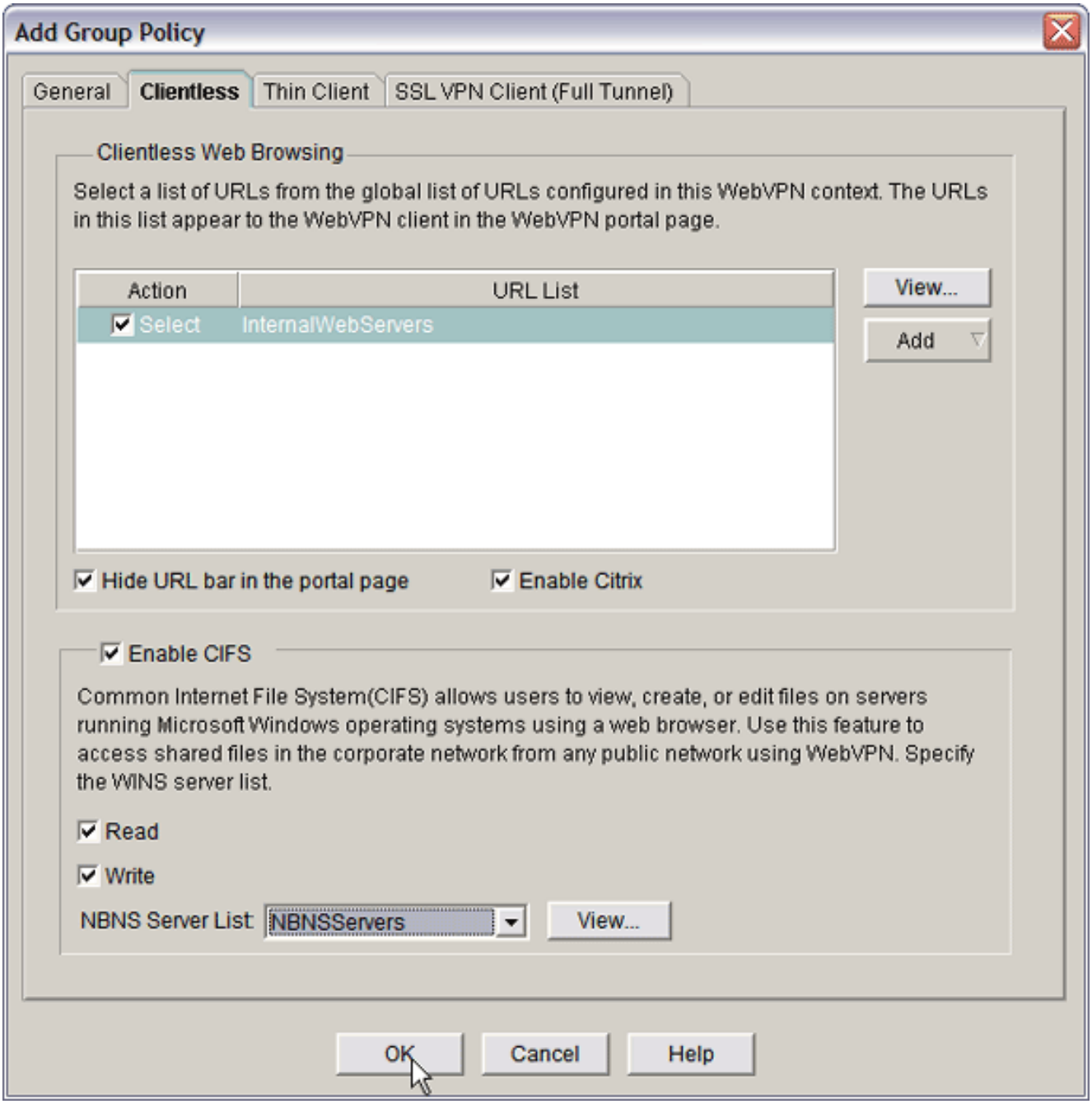
1. Klik op **Configureren** en vervolgens op **VPN**.
2. Vul **WebVPN** uit en kies **WebVPN Context**.



3. Kies **groepsbeleid** en klik op **Toevoegen**.Het dialoogvenster Gebiedsbeleid toevoegen verschijnt.



4. Voer een naam voor het nieuwe beleid in en controleer het **standaardgroepsbeleid voor** de optie **contextbeleid**.
5. Klik op het tabblad **Clientloze** boven in het dialoogvenster.

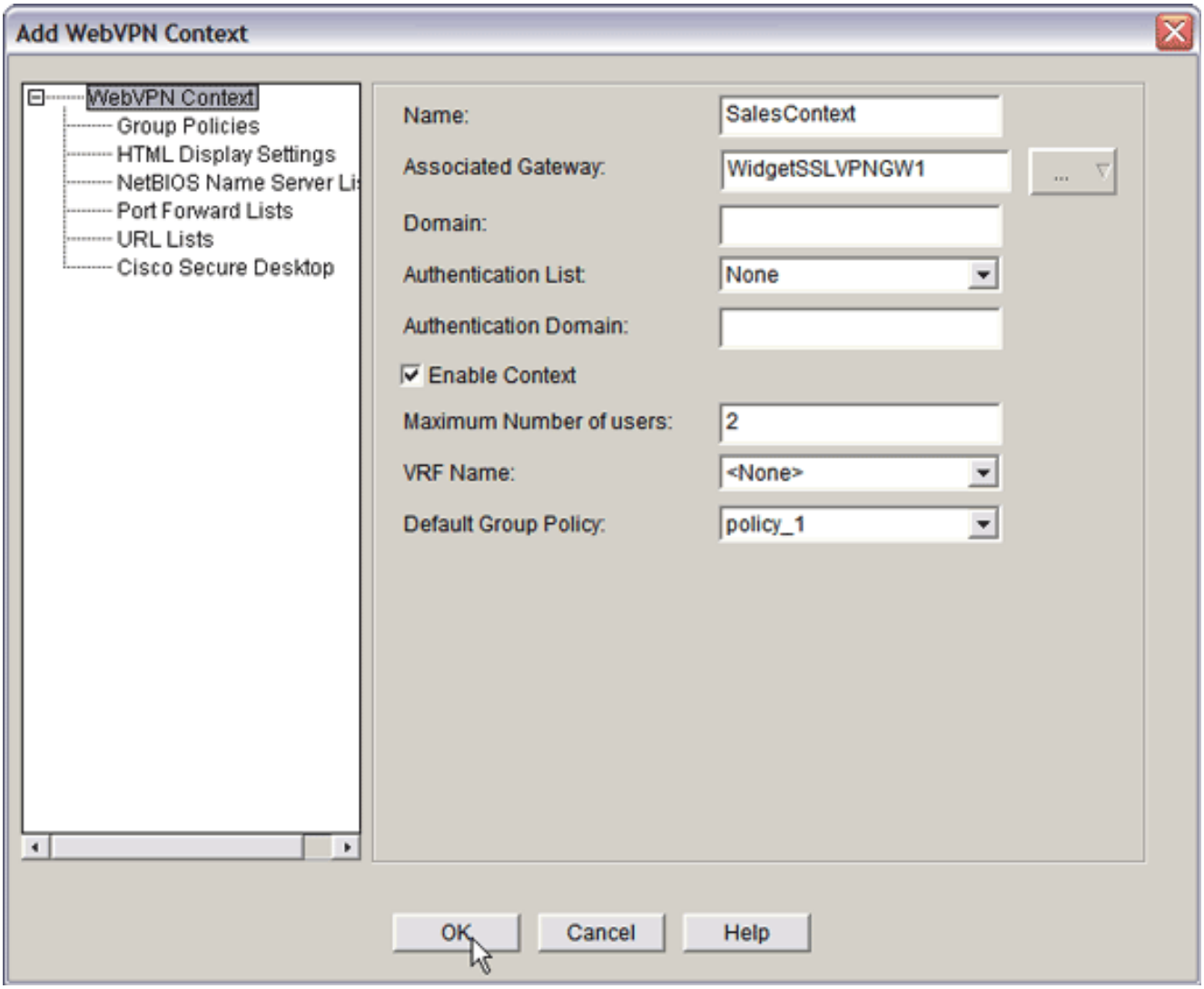


6. Controleer het selectieteken voor de gewenste URL-lijst.
7. Als uw klanten Citrix-klanten gebruiken die toegang tot Citrix-servers nodig hebben, vinkt u het aanvinkvakje **Citrix** activeren.
8. Controleer de vakjes **CIFS inschakelen**, **Lezen** en **Schrijven**.
9. Klik op de vervolgkeuzelijst **NBNS-server** en kies de NBS-serverlijst die u in Stap 2 voor Windows-bestand hebt gemaakt.
10. Klik op **OK**.

Stap 4. Configuratie van de WebVPN-context

Om de gateway WebVPN, groepsbeleid, en middelen samen te verbinden moet u de context van WebVPN configureren. Voltooi de volgende stappen om de WebVPN-context te configureren:

1. Kies **WebVPN Context** en voer een naam voor de context in.



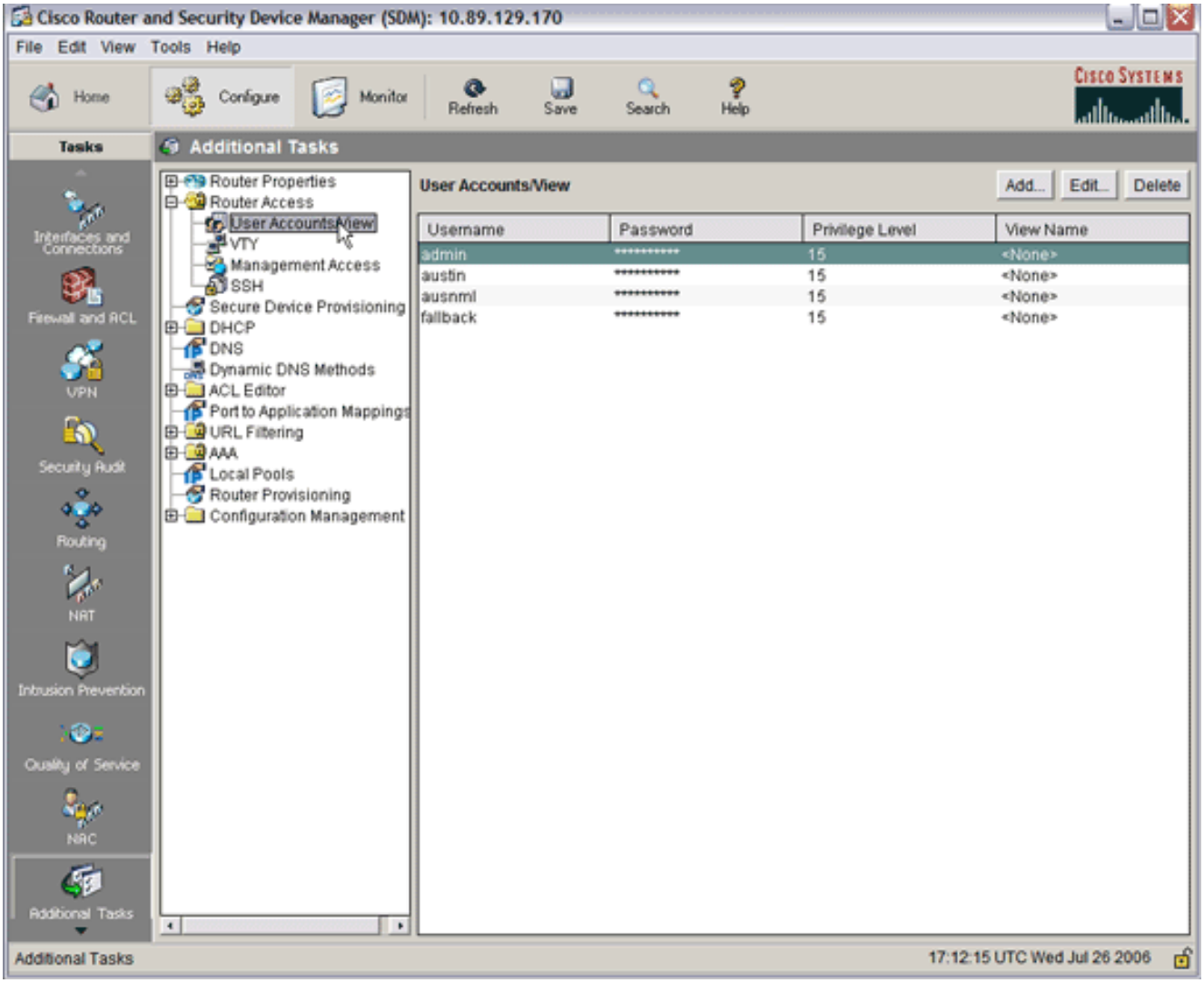
2. Klik op de vervolgkeuzpijl van de gekoppelde gateway en kies een bijbehorende gateway.
3. Als u meer dan één context wilt maken, typt u een unieke naam in het veld Domain om deze context te identificeren. Als u het veld leeg laat, hebben gebruikers toegang tot WebVPN met **https://*IPA-adres*.** Als u een domeinnaam (bijvoorbeeld *Verkoop*) invoert, moeten gebruikers verbinding maken met **https:// *IPA-adres*/verkoop**.
4. Controleer het dialoogvenster **Context inschakelen**.
5. Voer in het veld Maximum aantal gebruikers het maximale aantal gebruikers in dat door de apparaatlicentie is toegestaan.
6. Klik op de vervolgkeuzelijst **Standaardgroepsbeleid** en selecteer het groepsbeleid om deze context te associëren.
7. Klik op **OK** en vervolgens op **OK**.

Stap 5. Configureer de gebruikersdatabase en de verificatiemethode

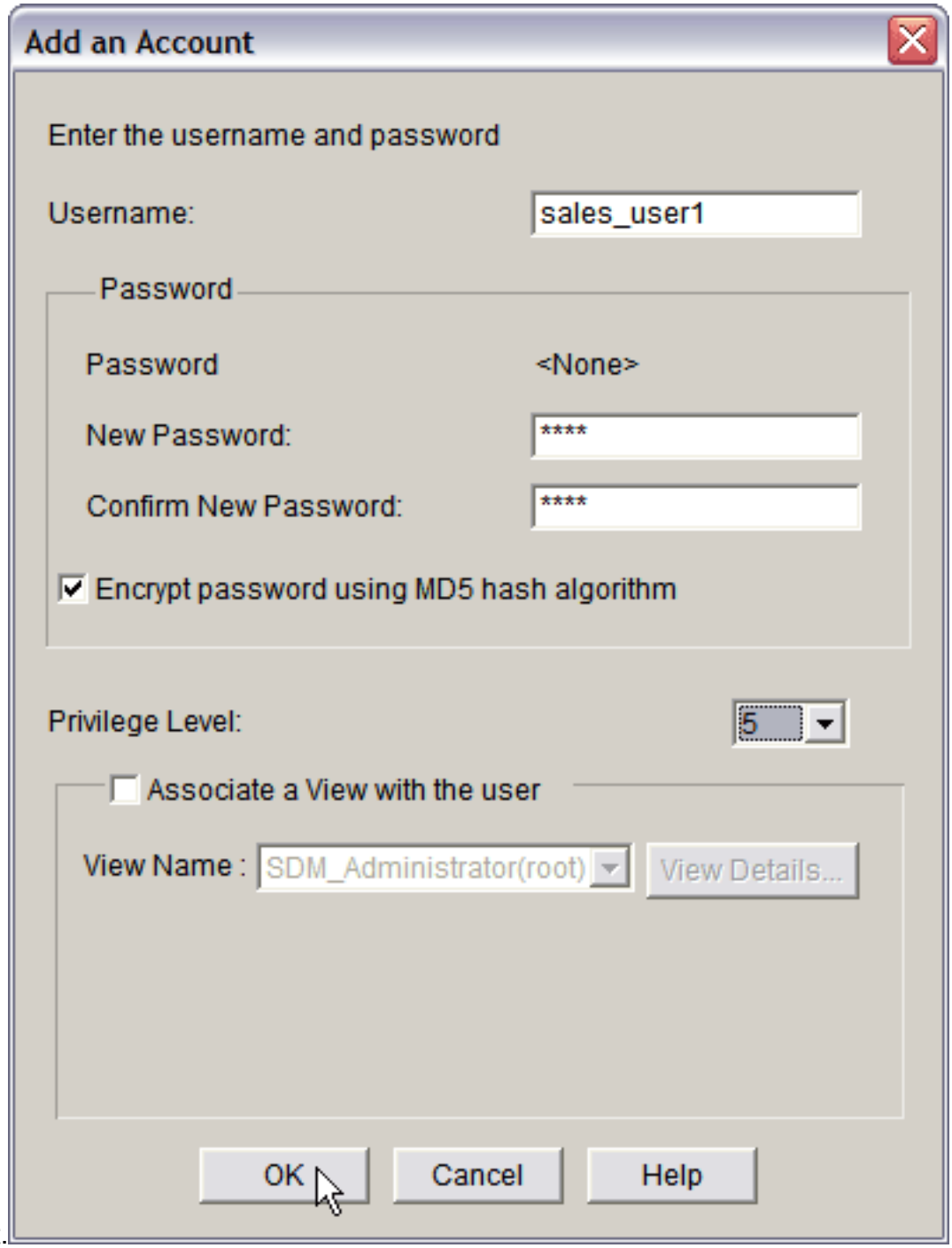
U kunt Clientless SSL VPN-sessies (WebVPN) configureren om te authenticeren met Radius, de Cisco AAA-server of een lokale database. Dit voorbeeld gebruikt een lokale databank.

Voltooi deze stappen om de gebruikersdatabase en de authenticatiemethode te configureren:

1. Klik op **Configuration** en vervolgens op **Extra taken**.
2. Uitbreidt **routertoegang** en kiest **gebruikersaccount/weergave**.



3. Klik op de knop **Toevoegen**.Het dialoogvenster Account toevoegen



verschijnt.

4. Voer een gebruikersaccount en een wachtwoord in.
5. Klik op **OK** en vervolgens op **OK**.
6. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

Resultaten

ASDM maakt deze opdrachtregel-configuraties:

ausnml-3825-01
Building configuration... Current configuration : 4190 bytes ! ! Last configuration change at 17:22:23 UTC Wed Jul 26 2006 by ausnml

```
! NVRAM config last updated at 17:22:31 UTC Wed Jul 26
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 29312730 2506092A 864886F7 0D010902
16186175 736E6D6C 2D333832 352D3031 2E636973 636F2E63
6F6D301E 170D3036 30373133 32333230 34375A17 0D323030
31303130 30303030 305A3029 31273025 06092A86 4886F70D
01090216 18617573 6E6D6C2D 33383235 2D30312E 63697363
6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A
A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B
E44753E4 0BEFDA42 FE6ED321 8EE7E811 4DEEC4E4 319C0093
C1026C0F 38D91236 6D92D931 AC3A84D4 185D220F D45A411B
09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D
BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3
78307630 0F060355 1D130101 FF040530 030101FF 30230603
551D1104 1C301A82 18617573 6E6D6C2D 33383235 2D30312E
63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1
5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D
0E041604 1403E15E AABA4779 F6C70CFB C61B0890 B26C2E3D
4E300D06 092A8648 86F70D01 01040500 03818100 6938CEA4
2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
F0A14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6
7C038112 0934A369 D44C0CF4 718A8972 2DA33C43 46E35DC6
5DCAE7E0 B0D85987 A0D116A4 600C0C60 71BB1136 486952FC
55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920
```

```
88A8A55E quit username admin privilege 15 secret 5
$1$jm6N$2xNfhupbAinq3BQZMRzrW0 username ausnml privilege
15 password 7 15071F5A5D292421 username fallback
privilege 15 password 7 08345818501A0A12 username austin
privilege 15 secret 5 $1$3xFv$W0YUsKDx1adDc.cVQF2Ei0
username sales_user1 privilege 5 secret 5
$1$2/SX$ep4fsCpodeyKaRji2mJkX/ ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! ip route
0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
authentication local ip http timeout-policy idle 600
life 86400 requests 100 ! control-plane ! line con 0
stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-
timeout 40 0 privilege level 15 password 7
071A351A170A1600 transport input telnet ssh line vty 5
15 exec-timeout 40 0 password 7 001107505D580403
transport input telnet ssh ! scheduler allocate 20000
1000 ! !--- WebVPN Gateway webvpn gateway
WidgetSSLVPNGW1 hostname ausnml-3825-01 ip address
192.168.0.37 port 443 http-redirect port 80 ssl
trustpoint ausnml-3825-01_Certificate inservice ! webvpn
context SalesContext ssl authenticate verify all ! !---
Identify resources for the SSL VPN session url-list
"InternalWebServers" heading "WidgetWebServers" url-text
"WidgetWeb" url-value "http://172.22.1.30" url-text
"OWA" url-value "http://172.22.1.50/exchange" ! nbns-
list NBNSServers nbns-server 172.22.1.30 ! !--- Identify
the policy which controls the resources available policy
group policy_1 url-list "InternalWebServers" nbns-list
"NBNSServers" functions file-access functions file-
browse functions file-entry hide-url-bar citrix enabled
default-group-policy policy_1 gateway WidgetSSLVPNGW1
max-users 2 inservice ! end
```

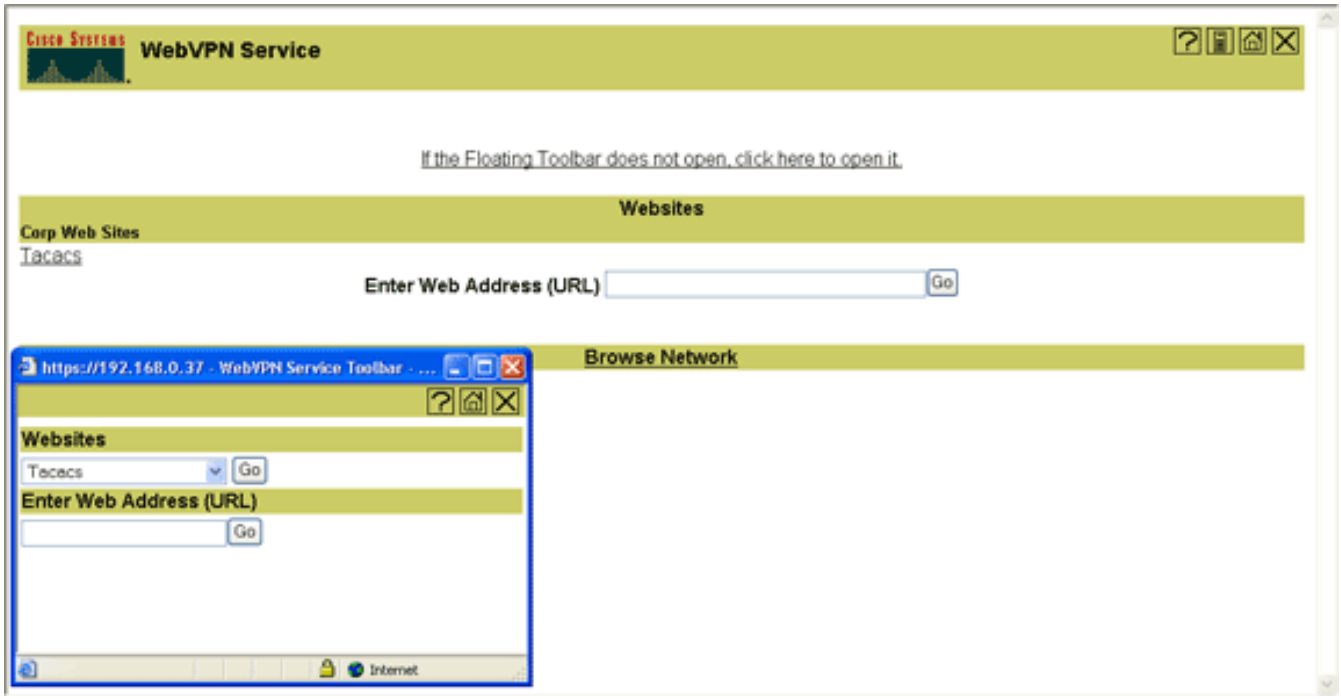
Verifiëren

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

Procedure

Volg deze procedures om te bevestigen dat de configuratie goed werkt:

- Test uw configuratie met een gebruiker. Voer **https:// *WebVPN_Gateway_IP_Address* in** een SSL-enabled Web browser in: Waar *Webex_Gateway_IP_Address* het IP-adres van de WebVPN-service is. Nadat u het certificaat accepteert en een gebruikersnaam en wachtwoord invoert, verschijnt een scherm dat vergelijkbaar is met deze afbeelding.



- Controleer de SSL VPN-sessie. Binnen de toepassing sm, klik de knop **van de monitor**, en klik dan op **VPN Status**. **WebVPN** uitvouwen **(Alle contexten)**, de juiste context uitvouwen en **gebruikers** kiezen.
- Controleer de foutmeldingen. Binnen de toepassing sm, klik de knop **van de monitor**, klik **Vastlegging**, en klik dan het **Syslog** tabblad.
- Bekijk de actieve configuratie voor het apparaat. Binnen de toepassing sm, klik de **knop Configure** en klik dan op **Extra Taken**. Uitbreidt **Configuration Management** en kiest **Config**.

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.

N.B.: Onderbreek het opdracht **Bestand kopiëren naar server** niet en navigeer naar een ander venster terwijl het kopiëren is gestart. Als de bewerking wordt onderbroken, kan er een onvolledig bestand op de server worden opgeslagen.

Opmerking: Gebruikers kunnen de nieuwe bestanden uploaden en downloaden met de WebVPN-client, maar de gebruiker mag de bestanden in het Common Internet File System (CIFS) op WebVPN niet overschrijven met de opdracht **Kopiebestand naar server**. De gebruiker ontvangt dit bericht wanneer de gebruiker probeert een bestand op de server te vervangen:

```
Unable to add the file
```

Procedure

Voltooi deze stappen om een oplossing voor uw configuratie te vinden:

1. Zorg ervoor dat klanten pop-up blokkers uitschakelen.
2. Zorg ervoor dat klanten koekjes hebben ingeschakeld.
3. Verzeker u dat klanten Netscape, Internet Explorer, Firefox of Mozilla webbrowsers gebruiken.

Opdrachten

Meerdere **debug** opdrachten zijn gekoppeld aan WebVPN. Raadpleeg Beeldopdrachten voor WebVPN gebruiken voor meer informatie over deze opdrachten.

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

- Cisco IOS VPN-SLVPN
- Cisco IOS VPN-Q&A
- Thin-Client SSL VPN (WebVPN) IOS Configuration-voorbeeld met DSM
- SSL VPN-client (SVC) op IOS met Configuratievoorbeeld
- Technische ondersteuning en documentatie – Cisco Systems