Clientless-SSL-VPN (WebVPN) auf Cisco IOS mit SDM-Konfigurationsbeispiel

Inhalt

Einführung

Clientless-SSL-VPN (WebVPN) ermöglicht Benutzern den sicheren Zugriff auf Ressourcen im Unternehmens-LAN von jedem Ort aus über einen SSL-fähigen Webbrowser. Der Benutzer authentifiziert sich zunächst über ein WebVPN-Gateway, das dann dem Benutzer den Zugriff auf vorkonfigurierte Netzwerkressourcen ermöglicht. WebVPN-Gateways können auf Cisco IOS® Routern, Cisco Adaptive Security Appliances (ASA), Cisco VPN 3000 Concentrators und dem Cisco WebVPN Services Module für Catalyst 6500- und 7600-Router konfiguriert werden.

Secure Socket Layer (SSL) Virtual Private Network (VPN)-Technologie kann auf Cisco Geräten in drei Hauptmodi konfiguriert werden: Clientless SSL VPN (WebVPN), Thin-Client SSL VPN (Port Forwarding) und SSL VPN Client (SVC)-Modus. Dieses Dokument veranschaulicht die Konfiguration des WebVPN auf Cisco IOS-Routern.

Hinweis: Ändern Sie weder den IP-Domänennamen noch den Hostnamen des Routers, da dies

eine Regeneration des selbstsignierten Zertifikats auslöst und den konfigurierten Trustpoint überschreibt. Die Neuerstellung des selbstsignierten Zertifikats verursacht Verbindungsprobleme, wenn der Router für WebVPN konfiguriert wurde. WebVPN verknüpft den SSL Trustpoint-Namen mit der WebVPN-Gateway-Konfiguration. Wenn also ein neues selbstsigniertes Zertifikat ausgegeben wird, stimmt der neue Trustpoint-Name nicht mit der WebVPN-Konfiguration überein, und die Benutzer können keine Verbindung herstellen.

Hinweis: Wenn Sie den Befehl **ip https-secure server** auf einem WebVPN-Router ausführen, der ein persistentes, selbstsigniertes Zertifikat verwendet, wird ein neuer RSA-Schlüssel generiert, und das Zertifikat wird ungültig. Es wird ein neuer Trustpoint erstellt, der SSL WebVPN unterbricht. Wenn der Router, der das persistente selbstsignierte Zertifikat verwendet, nach der Ausführung des Befehls **ip https-secure server** neu startet, tritt dasselbe Problem auf.

Weitere Informationen zum Thin-Client SSL VPN (WebVPN) IOS Configuration Example with SDM (Thin-Client SSL VPN (WebVPN) finden Sie unter SDM.

Weitere Informationen zum SSL VPN Client finden Sie unter SSL VPN Client (SVC) on IOS with SDM Configuration Example (Beispiel für eine SDM-Konfiguration).

SSL VPN wird auf den folgenden Cisco Router-Plattformen ausgeführt:

- Cisco Router der Serien 870, 1811, 1841, 2801, 2811, 2821 und 2851
- Cisco Router der Serien 3725, 3745, 3825, 3845, 7200 und 7301

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Ein erweitertes Image der Cisco IOS Software, Version 12.4(6)T oder höher
- Eine der in der Einführung aufgeführten Cisco Router-Plattformen

Verwendete Komponenten

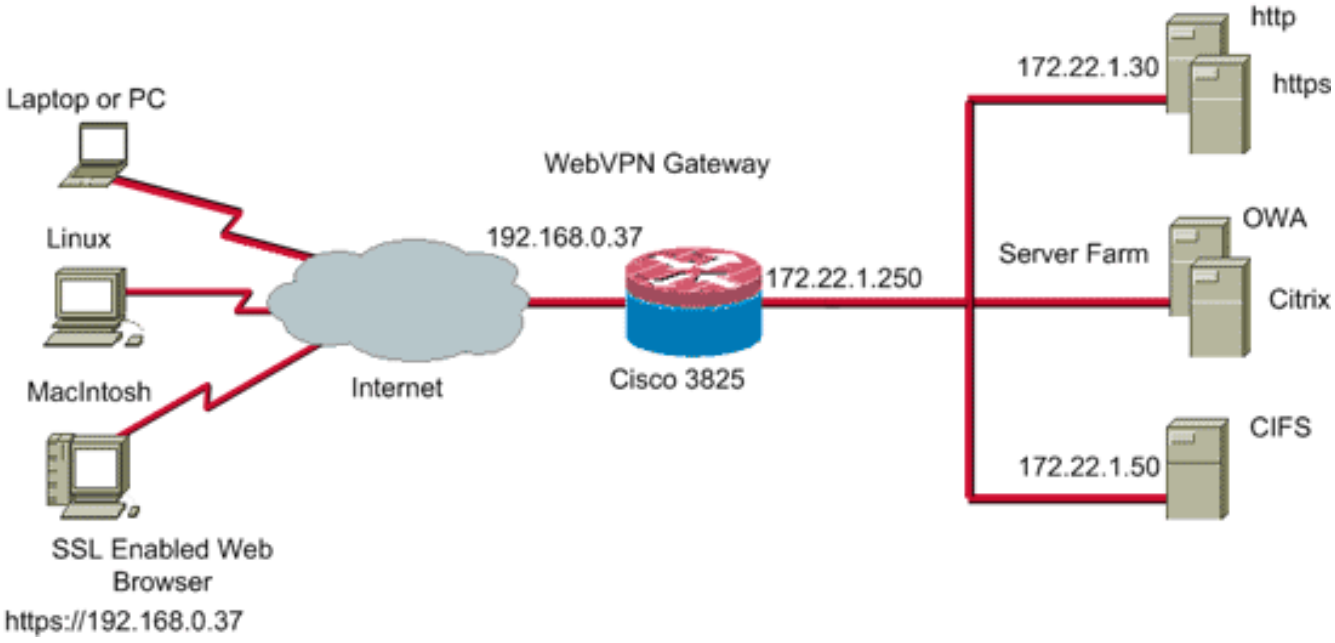
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Router 3825
- Erweitertes Software-Image für Unternehmen - Cisco IOS Software, Version 12.4(9)T
- Cisco Router and Security Device Manager (SDM) - Version 2.3.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen. Die in diesem Beispiel verwendeten IP-Adressen stammen von RFC 1918-Adressen, die privat sind und im Internet nicht verwendet werden dürfen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Vorkonfigurationsaufgaben

Führen Sie die folgenden Schritte aus, bevor Sie beginnen:

1. Konfigurieren Sie einen Hostnamen und einen Domänennamen.
2. Konfigurieren Sie den Router für SDM. Cisco liefert einige Router mit einer vorinstallierten SDM-Kopie aus.Wenn das Cisco SDM nicht bereits auf Ihrem Router geladen ist, können Sie eine kostenlose Kopie der Software vom Software Download beziehen (nur registrierte Kunden). Sie müssen über ein CCO-Konto mit einem Servicevertrag verfügen. Detaillierte Informationen zur Installation und Konfiguration von SDM finden Sie unter Cisco Router und Security Device Manager.
3. Konfigurieren Sie das richtige Datum, die richtige Uhrzeit und die richtige Zeitzone für Ihren Router.

Konfigurieren von WebVPN auf Cisco IOS

Sie können einem Gerät mehr als ein WebVPN-Gateway zugeordnet haben. Jedes WebVPN-Gateway ist mit nur einer IP-Adresse auf dem Router verknüpft. Sie können mehr als einen WebVPN-Kontext für ein bestimmtes WebVPN-Gateway erstellen. Um einzelne Kontexte zu identifizieren, geben Sie jedem Kontext einen eindeutigen Namen. Eine Richtliniengruppe kann nur einem WebVPN-Kontext zugeordnet werden. Die Richtliniengruppe beschreibt, welche Ressourcen in einem bestimmten WebVPN-Kontext verfügbar sind.

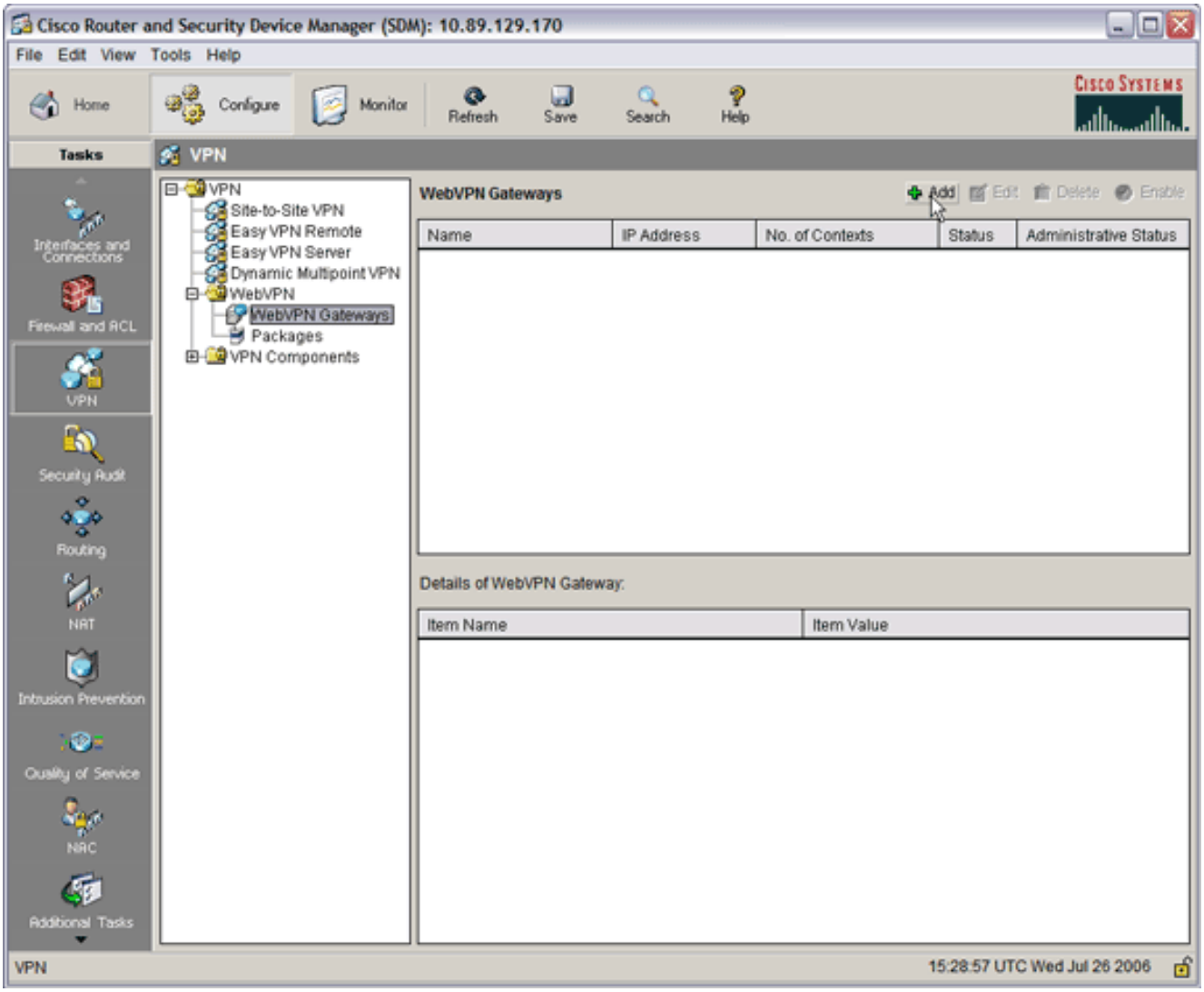
Gehen Sie wie folgt vor, um WebVPN auf Cisco IOS zu konfigurieren:

1. Konfigurieren des WebVPN-Gateways
2. Konfigurieren der für die Richtliniengruppe zulässigen Ressourcen
3. Konfigurieren der WebVPN-Richtliniengruppe und Auswählen der Ressourcen
4. Konfigurieren des WebVPN-Kontexts
5. Konfigurieren der Benutzerdatenbank und der Authentifizierungsmethode

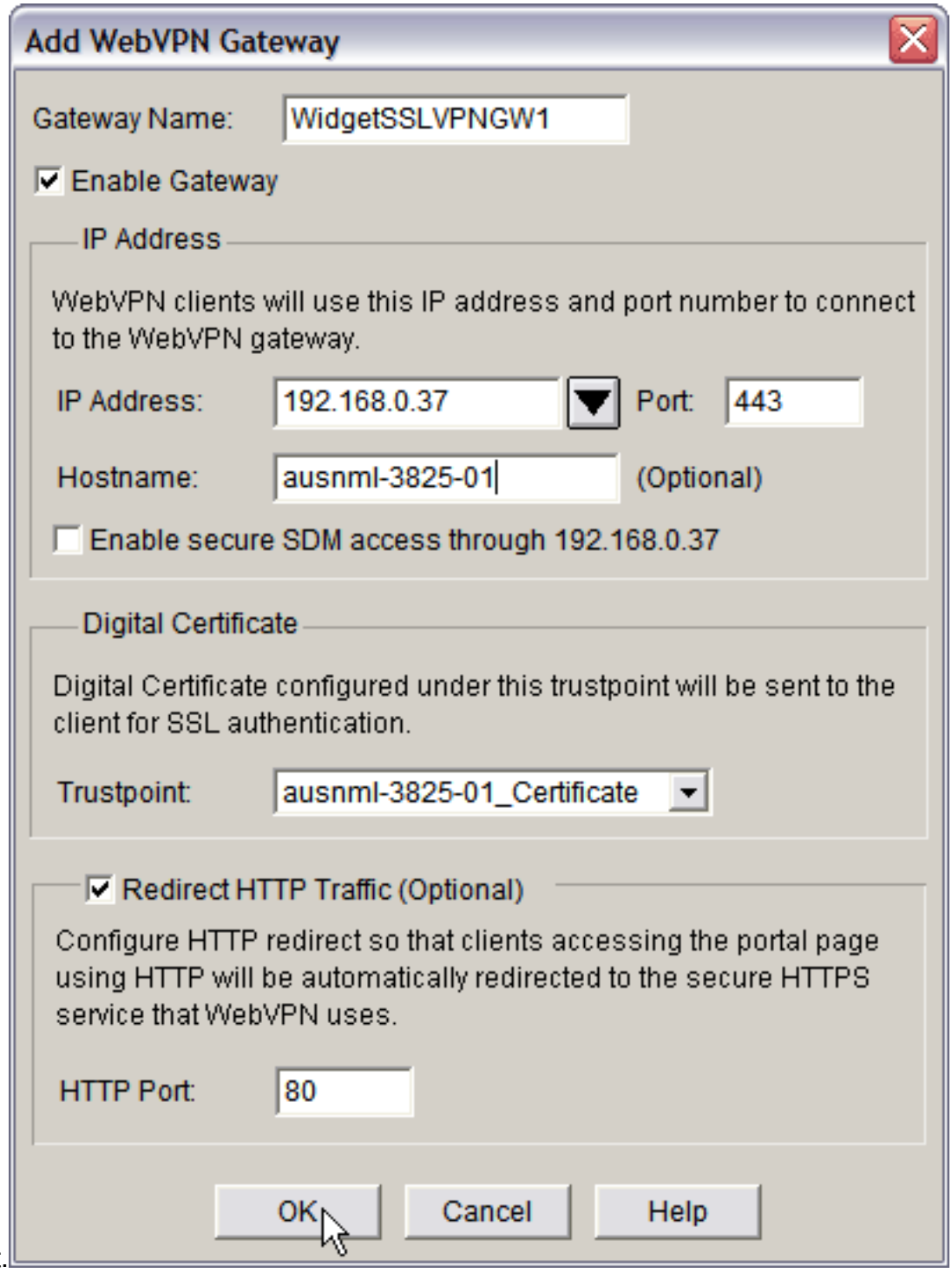
Schritt 1: Konfigurieren des WebVPN-Gateways

Gehen Sie wie folgt vor, um das WebVPN-Gateway zu konfigurieren:

1. Klicken Sie in der SDM-Anwendung auf **Konfigurieren** und dann auf **VPN**.
2. Erweitern Sie **WebVPN**, und wählen Sie **WebVPN-Gateways aus**.



3. Klicken Sie auf **Hinzufügen**.Das Dialogfeld WebVPN-Gateway hinzufügen wird



angezeigt.

4. Geben Sie Werte in die Felder Gateway-Name und IP-Adresse ein, und aktivieren Sie das Kontrollkästchen **Enable Gateway** (Gateway aktivieren).
5. Aktivieren Sie das Kontrollkästchen **HTTP-Datenverkehr umleiten**, und klicken Sie dann auf **OK**.
6. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

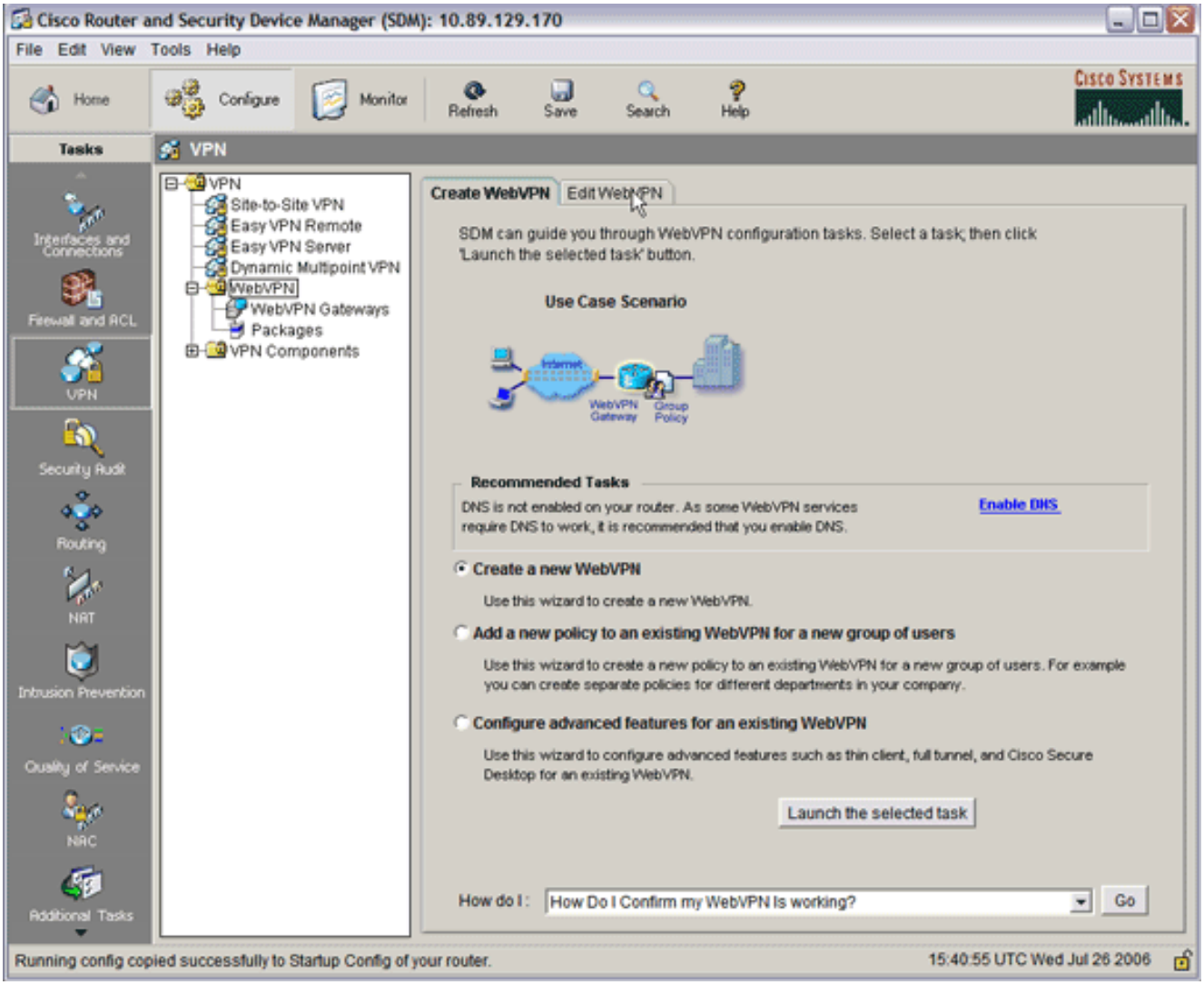
Schritt 2: Konfigurieren der für die Richtliniengruppe zulässigen Ressourcen

Um das Hinzufügen von Ressourcen zu einer Richtliniengruppe zu vereinfachen, können Sie die Ressourcen konfigurieren, bevor Sie die Richtliniengruppe erstellen.

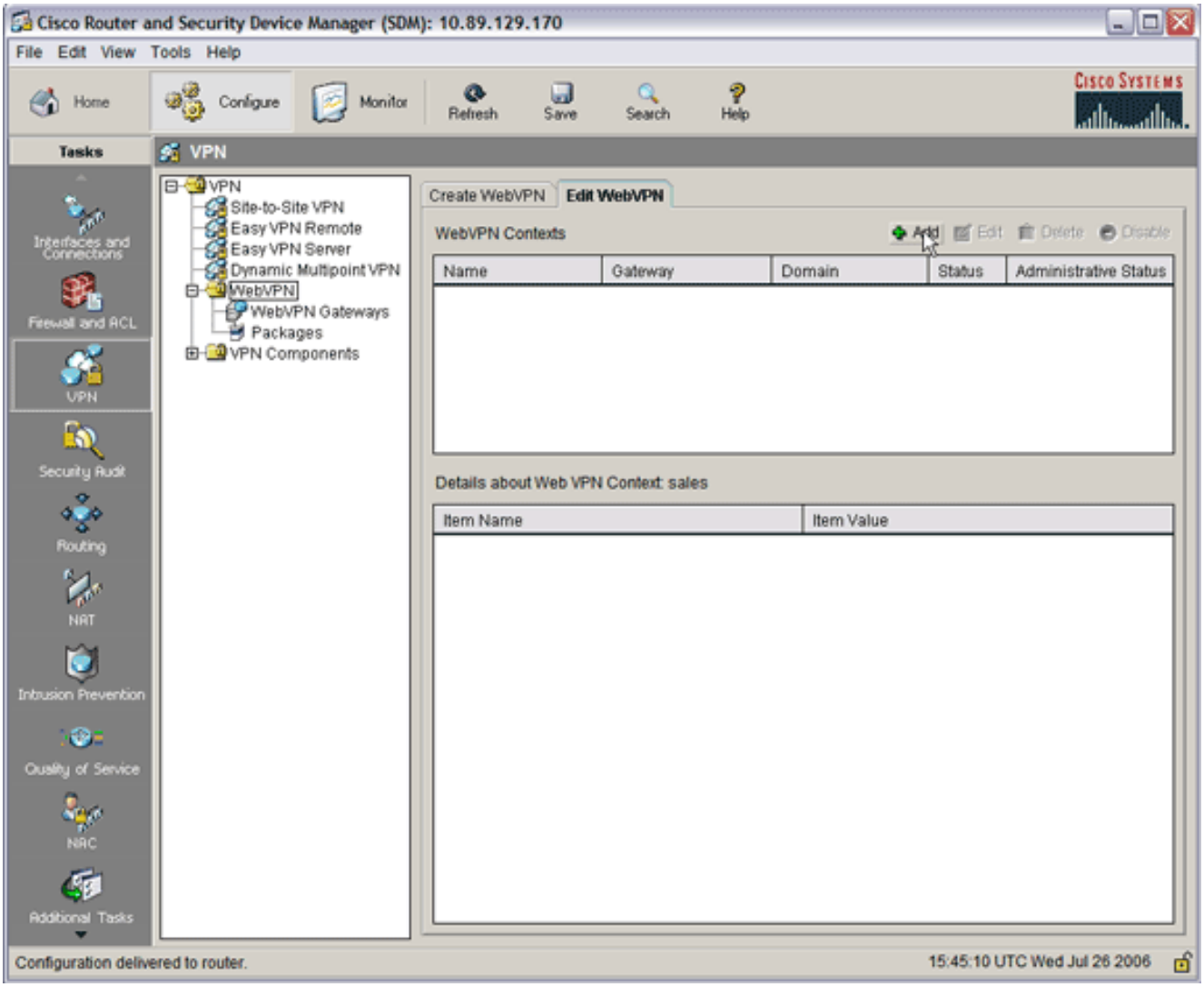
Gehen Sie wie folgt vor, um die für die Richtliniengruppe zulässigen Ressourcen zu konfigurieren:

1. Klicken Sie auf **Konfigurieren** und dann auf

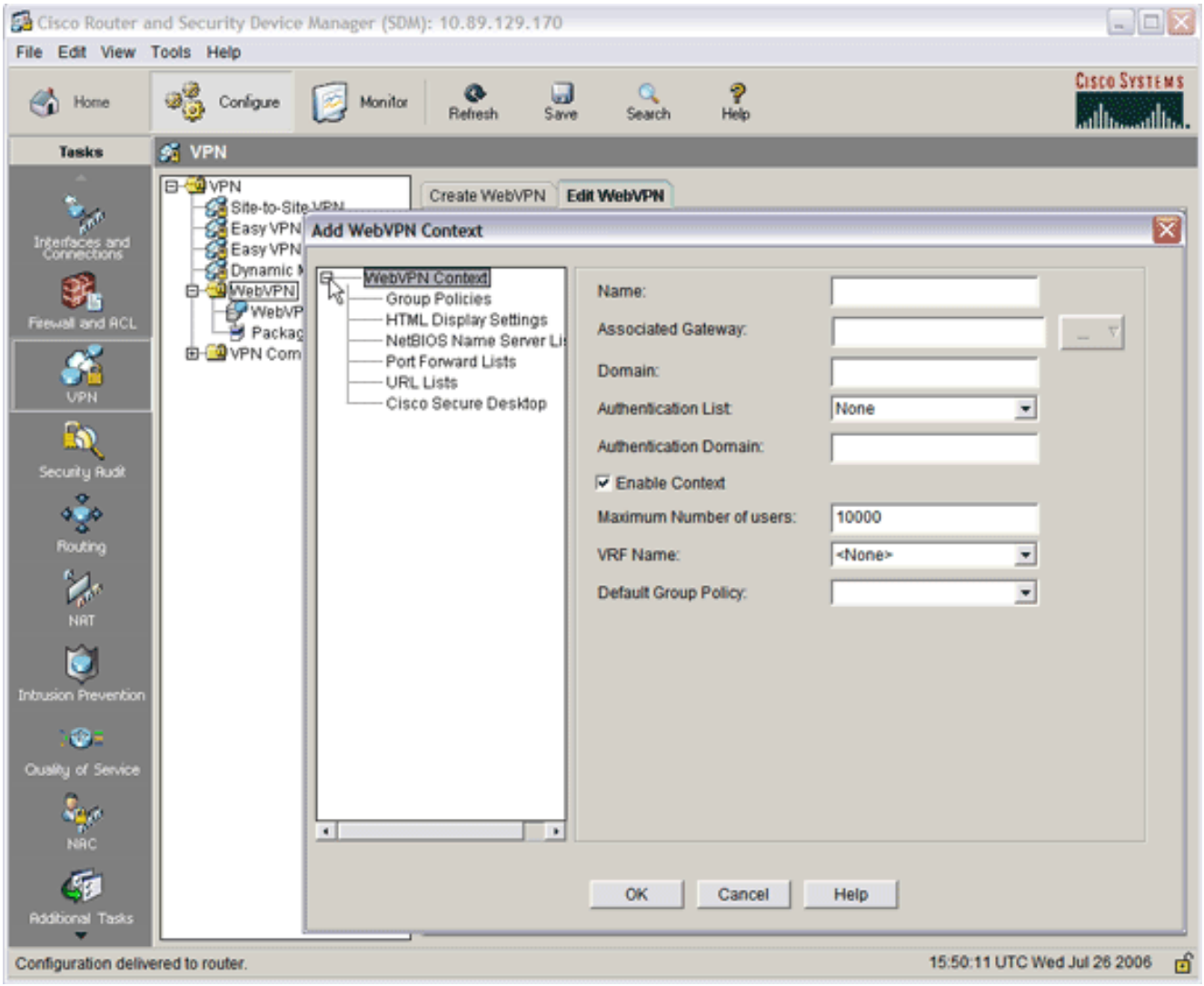
VPN.



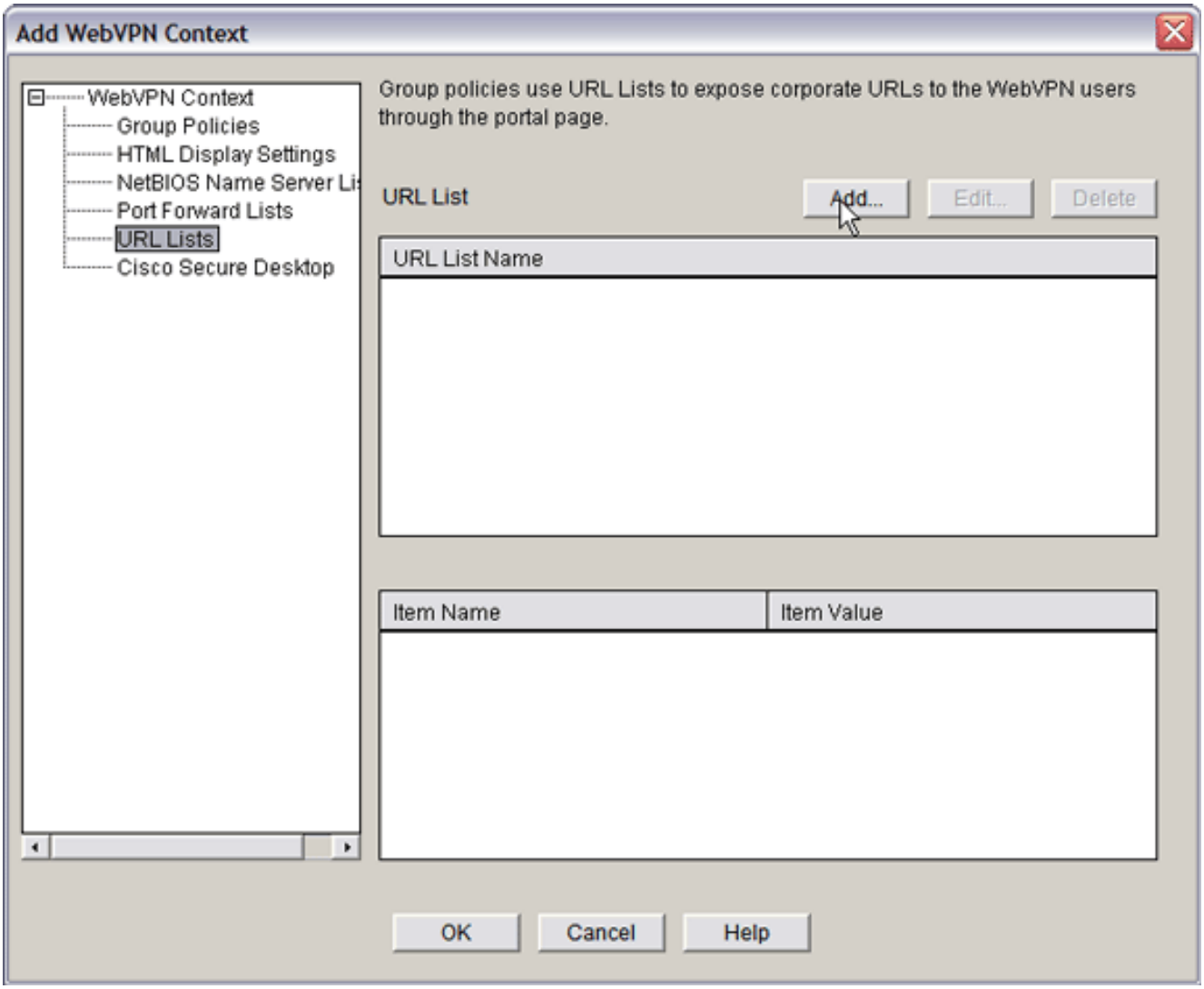
2. Wählen Sie **WebVPN aus**, und klicken Sie dann auf die Registerkarte **WebVPN bearbeiten**.**Hinweis:** Mit WebVPN können Sie den Zugriff für HTTP, HTTPS, das Durchsuchen von Windows-Dateien über das CIFS-Protokoll (Common Internet File System) und Citrix
konfigurieren.



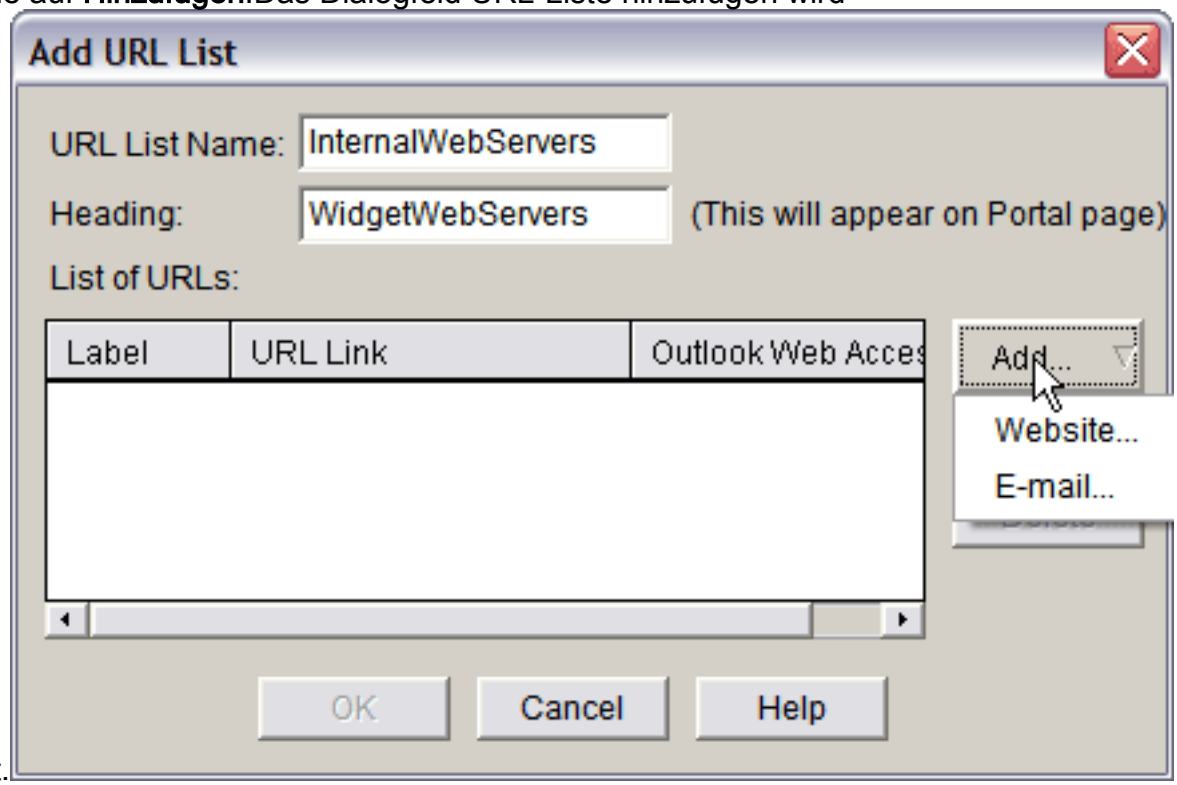
3. Klicken Sie auf **Hinzufügen**.Das Dialogfeld WebVPN-Kontext hinzufügen wird angezeigt.



4. Erweitern Sie **WebVPN-Kontext**, und wählen Sie **URL-Listen aus**.

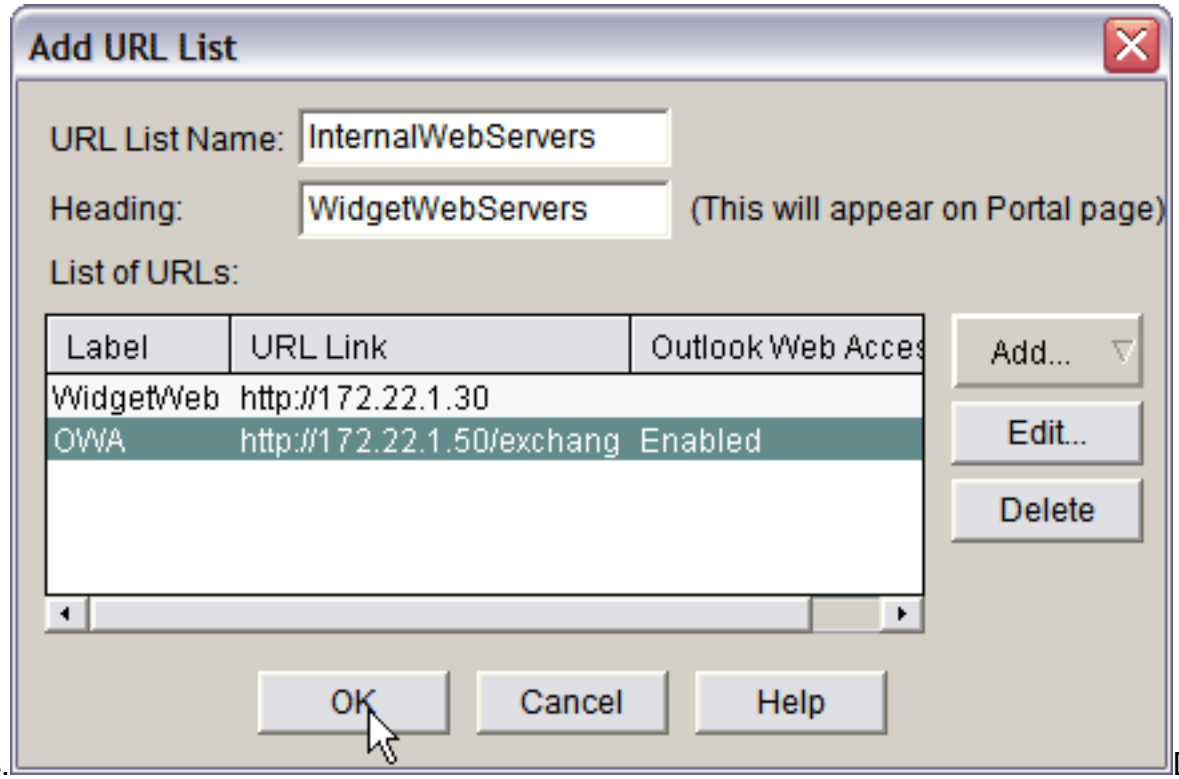


5. Klicken Sie auf **Hinzufügen**.Das Dialogfeld URL-Liste hinzufügen wird



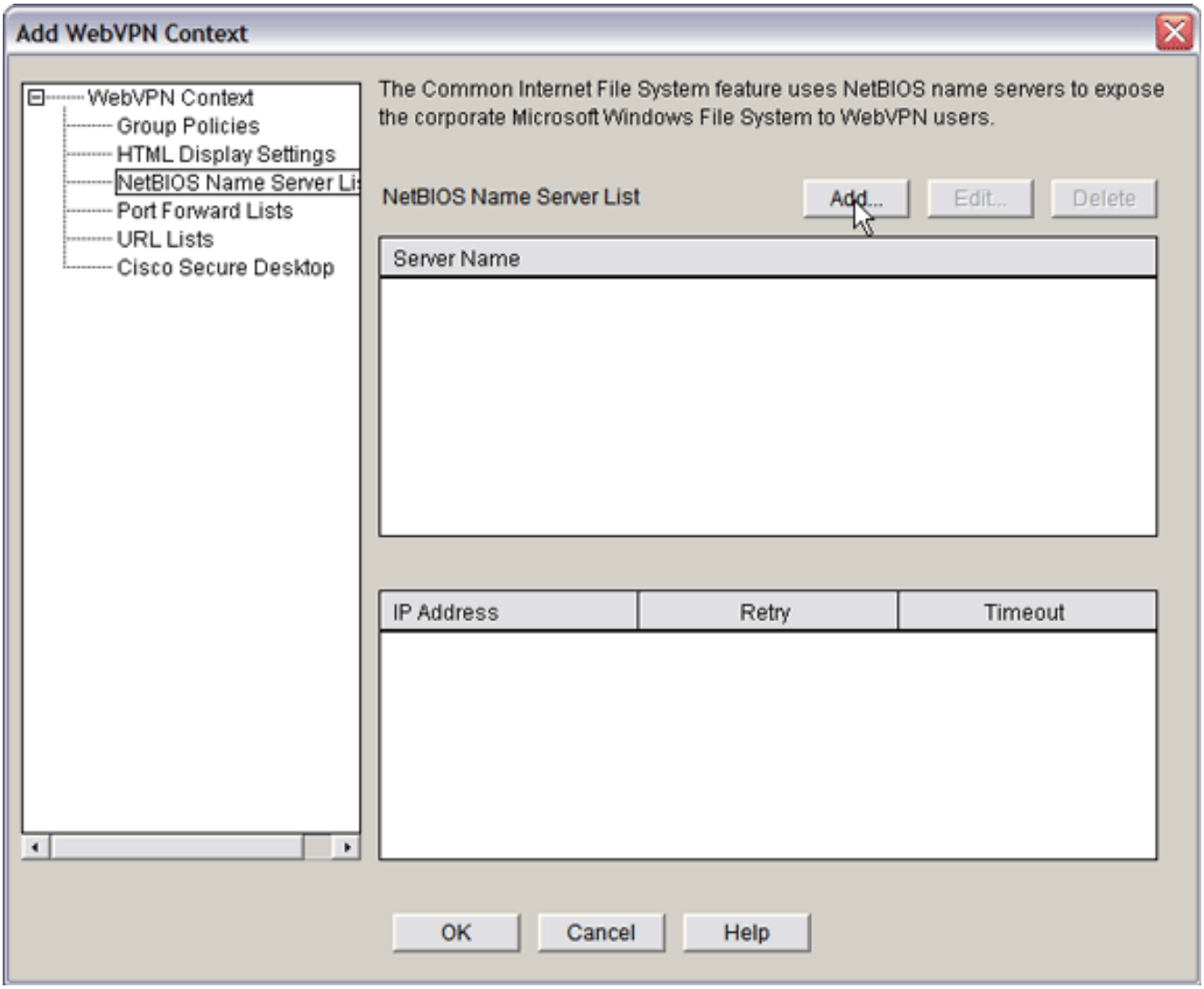
angezeigt.

6. Geben Sie Werte in die Felder URL-Listenname und Überschrift ein.
7. Klicken Sie auf **Hinzufügen**, und wählen Sie **Website**

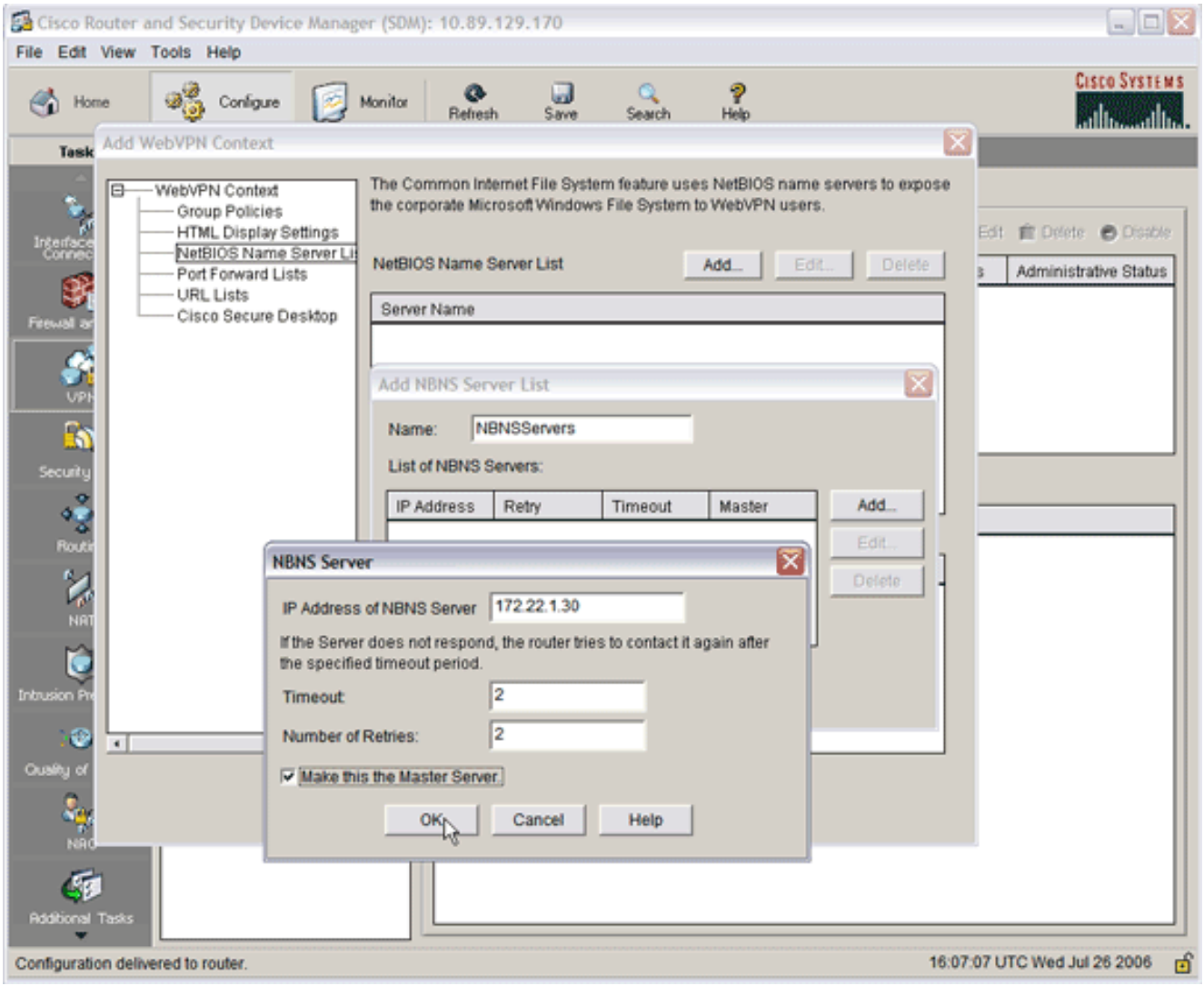


aus.Diese Liste enthält alle HTTP- und HTTPS-Webserver, die für diese WebVPN-Verbindung verfügbar sein sollen.

8. Um den Zugriff für Outlook Web Access (OWA) hinzuzufügen, klicken Sie auf **Hinzufügen**, wählen Sie **E-Mail aus**, und klicken Sie dann nach Eingabe aller gewünschten Felder auf **OK**.
9. Um das Durchsuchen von Windows-Dateien durch CIFS zu ermöglichen, können Sie einen NetBIOS Name Service (NBNS)-Server bestimmen und die entsprechenden Freigaben in der Windows-Domäne in der richtigen Reihenfolge konfigurieren.Wählen Sie aus der Liste WebVPN-Kontext die Option **NetBIOS Name Server Lists (NetBIOS-Namensserver-Listen)**.



Klicken Sie auf **Hinzufügen**.Das Dialogfeld "NBNS-Serverliste hinzufügen" wird angezeigt.Geben Sie einen Namen für die Liste ein, und klicken Sie auf **Hinzufügen**.Das Dialogfeld "NBNS Server" wird
angezeigt.

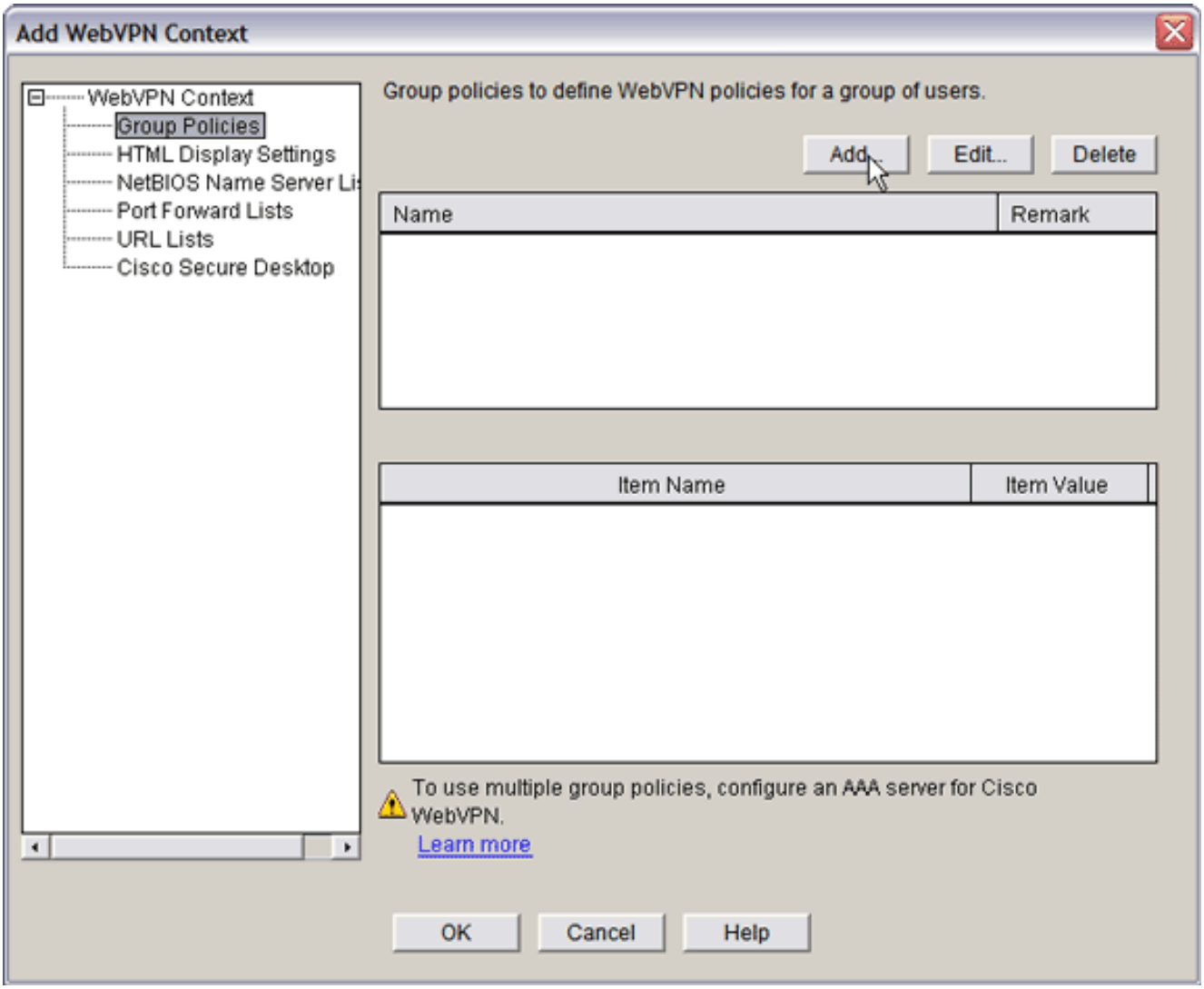


Aktivieren Sie ggf. das Kontrollkästchen **Make This the Master Server (Dies zum Master-Server machen).**Klicken Sie auf **OK** und dann auf **OK**.

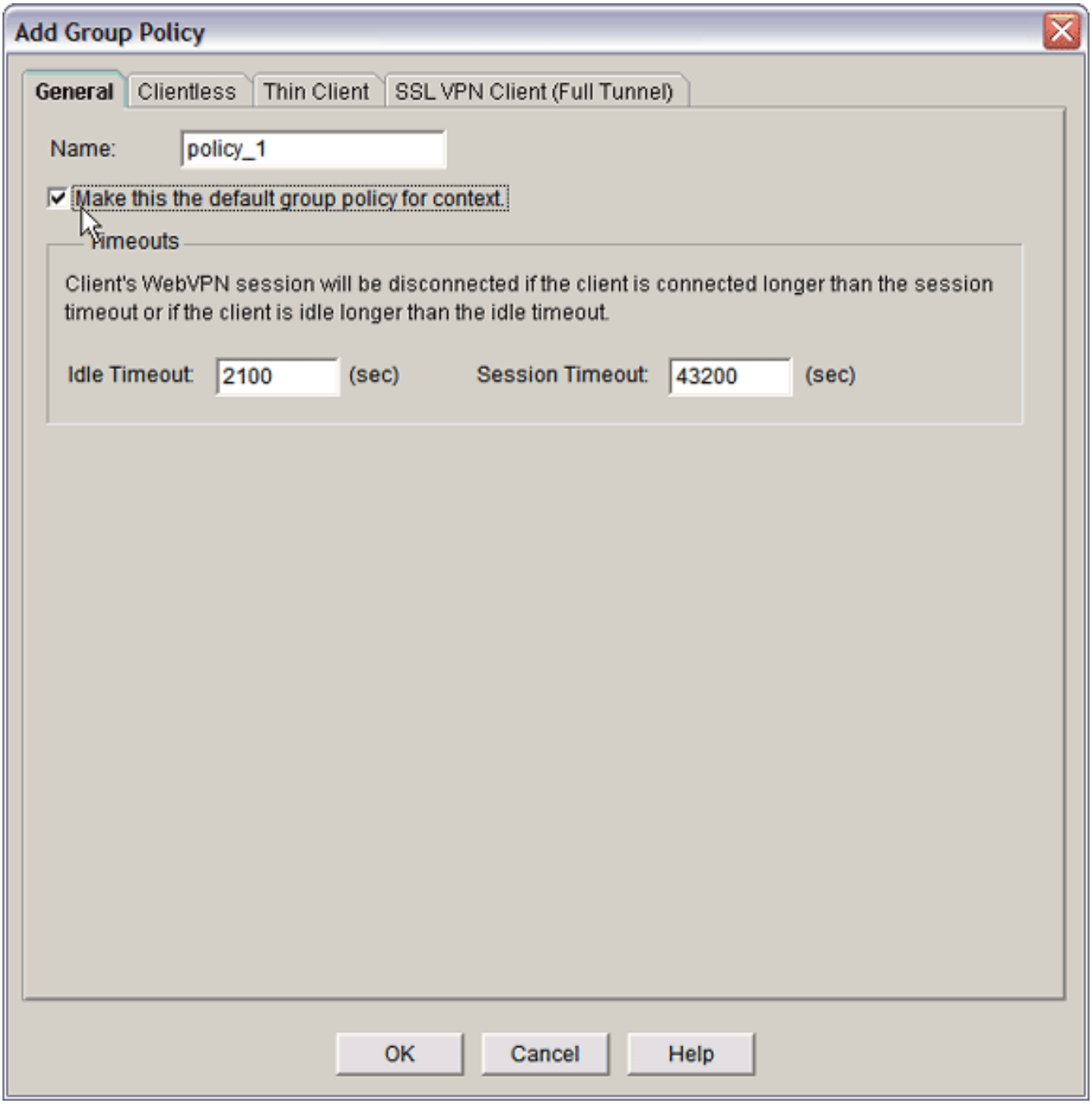
Schritt 3: Konfigurieren der WebVPN-Richtliniengruppe und Auswählen der Ressourcen

Gehen Sie wie folgt vor, um die WebVPN-Richtliniengruppe zu konfigurieren und die Ressourcen auszuwählen:

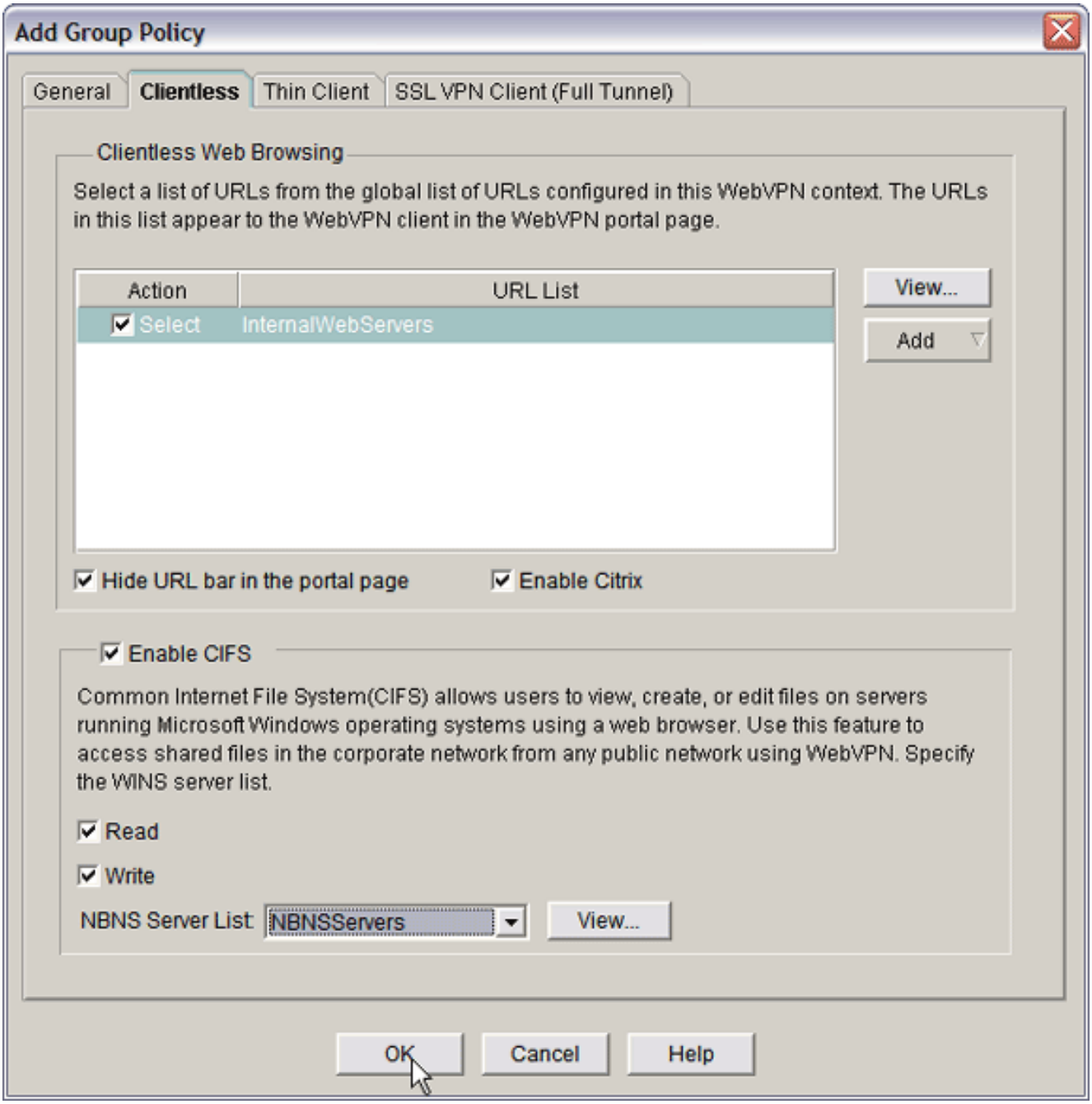
1. Klicken Sie auf **Konfigurieren** und dann auf **VPN**.
2. Erweitern Sie **WebVPN**, und wählen Sie **WebVPN Context aus**.



3. Wählen Sie **Gruppenrichtlinien aus**, und klicken Sie auf **Hinzufügen**.Das Dialogfeld Gruppenrichtlinie hinzufügen wird angezeigt.



4. Geben Sie einen Namen für die neue Richtlinie ein, und aktivieren Sie das Kontrollkästchen **Make this the default group policy for context (Standardgruppenrichtlinie für Kontext** festlegen).
5. Klicken Sie auf die Registerkarte **Clientless** oben im Dialogfeld.

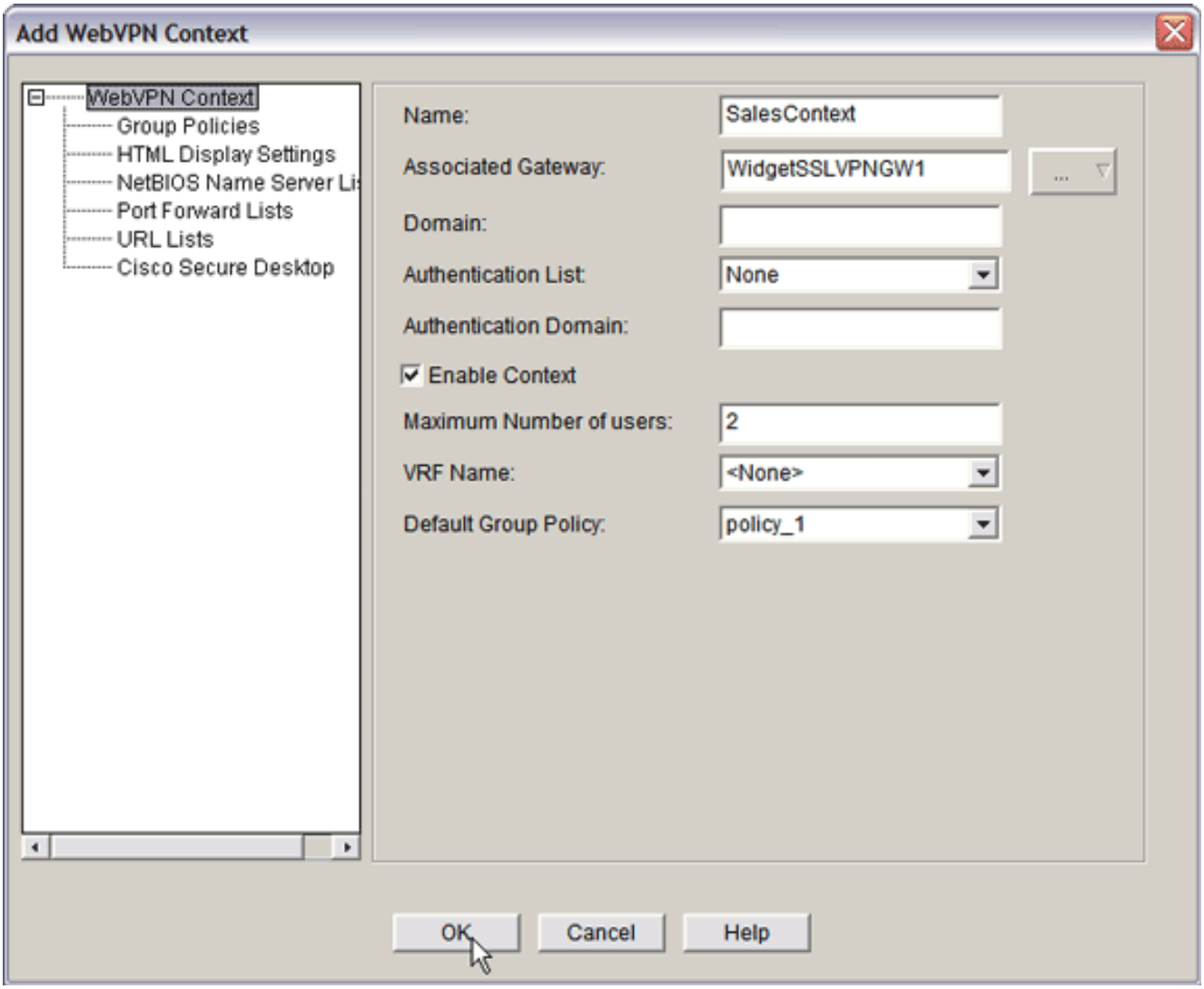


6. Aktivieren Sie das Kontrollkästchen **Wählen** für die gewünschte URL-Liste.
7. Wenn Ihre Kunden Citrix Clients verwenden, die Zugriff auf Citrix-Server benötigen, aktivieren Sie das Kontrollkästchen **Enable Citrix**.
8. Aktivieren Sie die Kontrollkästchen **Enable CIFS**, **Read** und **Write**.
9. Klicken Sie auf den Pfeil des Dropdown-Menüs **NBNS Server List** (Serverliste für NBNS-Server), und wählen Sie die NBNS-Serverliste aus, die Sie in Schritt 2 für das Durchsuchen von Windows-Dateien erstellt haben.
10. Klicken Sie auf **OK**.

Schritt 4: Konfigurieren des WebVPN-Kontexts

Um das WebVPN-Gateway, die Gruppenrichtlinie und die Ressourcen miteinander zu verknüpfen, müssen Sie den WebVPN-Kontext konfigurieren. Gehen Sie wie folgt vor, um den WebVPN-Kontext zu konfigurieren:

1. Wählen Sie **WebVPN Context**, und geben Sie einen Namen für den Kontext ein.



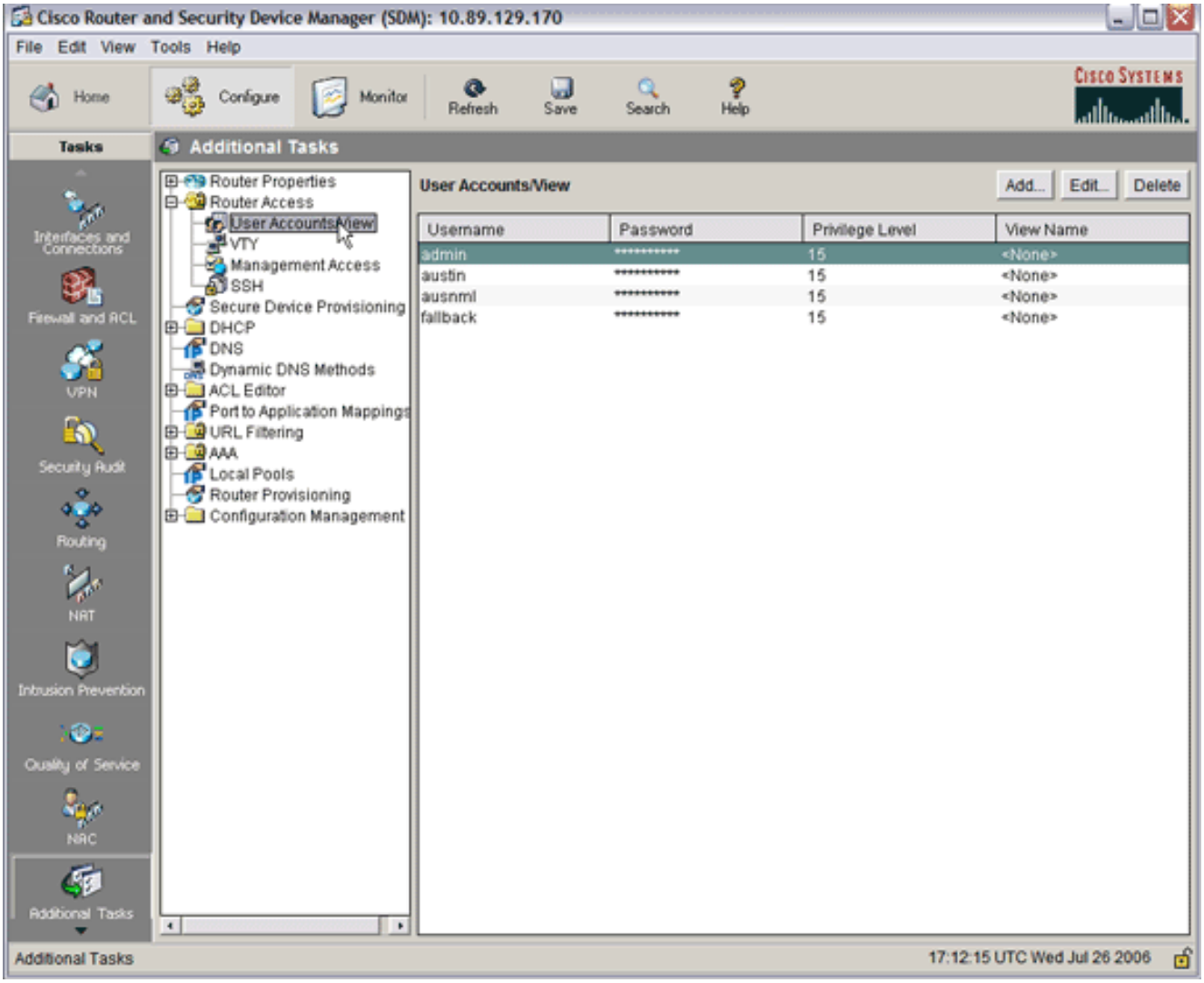
2. Klicken Sie auf den Pfeil des Dropdown-Menüs Zugeordnetes Gateway, und wählen Sie ein zugehöriges Gateway aus.
3. Wenn Sie mehr als einen Kontext erstellen möchten, geben Sie im Feld Domäne einen eindeutigen Namen ein, um diesen Kontext zu identifizieren. Wenn Sie das Feld Domäne leer lassen, müssen Benutzer mit der **https://*IPAddress*** auf das WebVPN zugreifen. Wenn Sie einen Domänennamen eingeben (z. B. *Sales*), müssen sich die Benutzer mit **https://*IPAddress*/Sales** verbinden.
4. Aktivieren Sie das Kontrollkästchen **Kontext aktivieren**.
5. Geben Sie im Feld Maximum Number of Users (Maximale Anzahl von Benutzern) die maximal zulässige Anzahl von Benutzern für die Gerätelizenz ein.
6. Klicken Sie auf den Pfeil des Dropdown-Menüs **Richtlinie für Standardgruppe**, und wählen Sie die Gruppenrichtlinie aus, die diesem Kontext zugeordnet werden soll.
7. Klicken Sie auf **OK** und dann auf **OK**.

Schritt 5: Konfigurieren der Benutzerdatenbank und der Authentifizierungsmethode

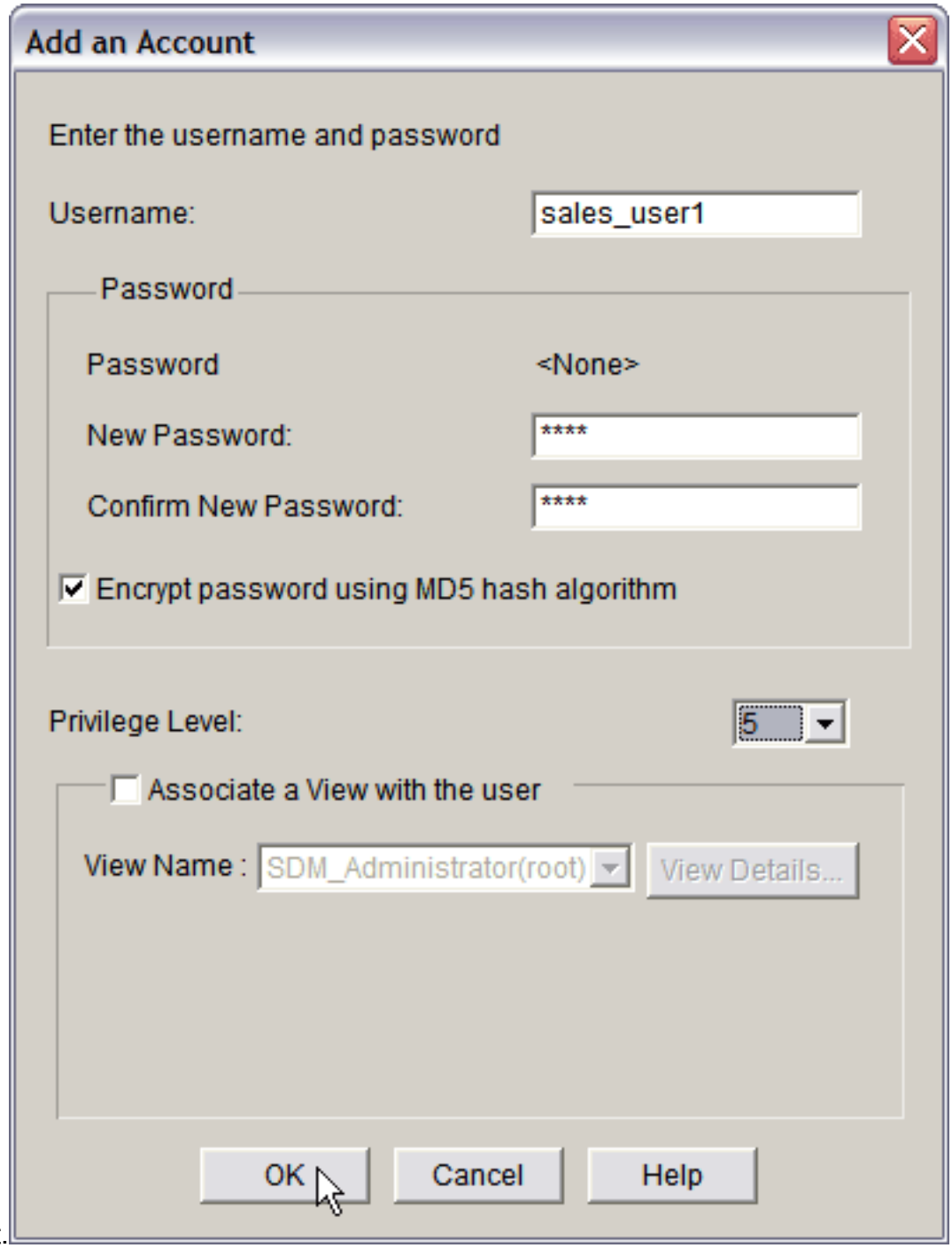
Sie können Clientless SSL VPN (WebVPN)-Sitzungen für die Authentifizierung mit Radius, dem Cisco AAA-Server oder einer lokalen Datenbank konfigurieren. In diesem Beispiel wird eine lokale Datenbank verwendet.

Gehen Sie wie folgt vor, um die Benutzerdatenbank und die Authentifizierungsmethode zu konfigurieren:

1. Klicken Sie auf **Konfiguration** und dann auf **Weitere Aufgaben**.
2. Erweitern Sie **den Router-Zugriff**, und wählen Sie **Benutzerkonten/Ansicht aus**.



3. Klicken Sie auf die Schaltfläche **Hinzufügen**.Das Dialogfeld Konto hinzufügen wird



angezeigt.

4. Geben Sie ein Benutzerkonto und ein Kennwort ein.
5. Klicken Sie auf **OK** und dann auf **OK**.
6. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

Ergebnisse

Der ASDM erstellt folgende Befehlszeilenkonfigurationen:

ausml-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
```

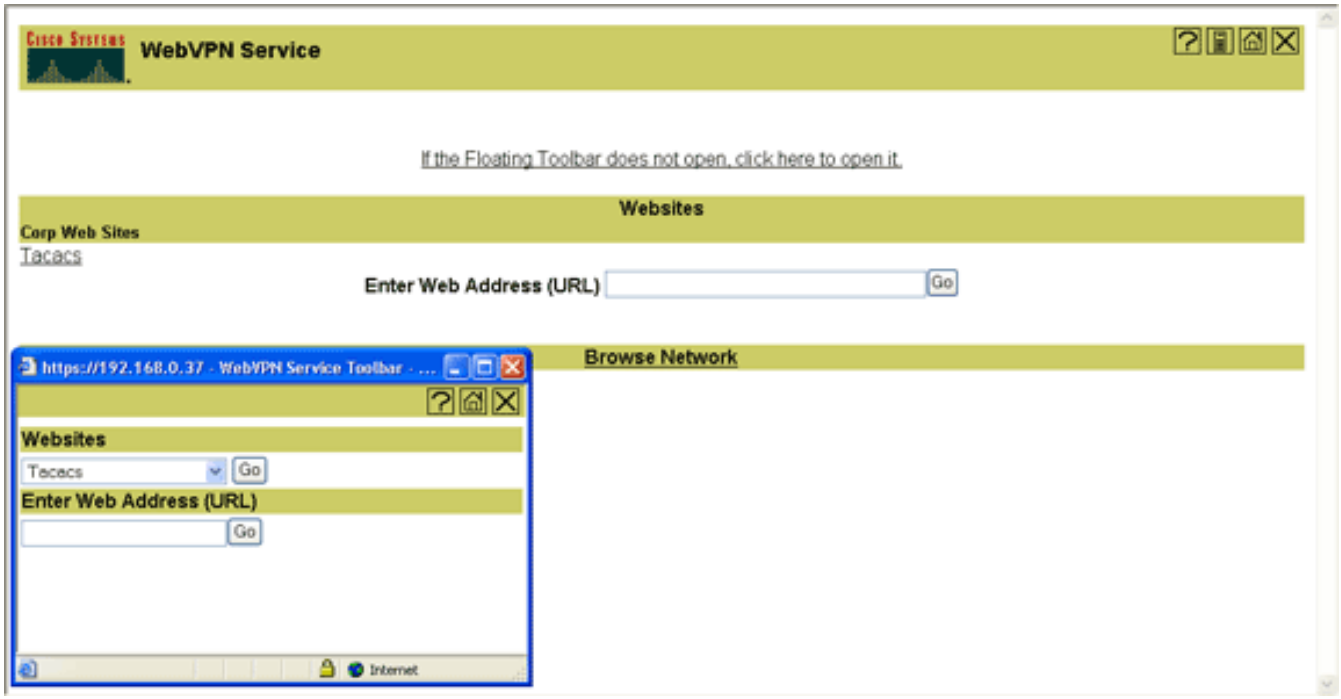
Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Vorgehensweise

Gehen Sie wie folgt vor, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert:

- Testen Sie Ihre Konfiguration mit einem Benutzer. Geben Sie **https://*WebVPN_Gateway_IP_Address* in einen** SSL-fähigen Webbrowser ein. wobei *WebVPN_Gateway_IP_Address* die IP-Adresse des WebVPN-Dienstes ist. Nachdem Sie das Zertifikat akzeptiert und einen Benutzernamen und ein Kennwort eingegeben haben, sollte ein Bildschirm ähnlich dem Bild angezeigt
  werden.



- Überprüfen Sie die SSL VPN-Sitzung. Klicken Sie in der SDM-Anwendung auf die Schaltfläche **Überwachen** und anschließend auf **VPN-Status**. Erweitern Sie **WebVPN (All Contexts)**, erweitern Sie den entsprechenden Kontext, und wählen Sie **Benutzer** aus.
- Überprüfen Sie Fehlermeldungen. Klicken Sie in der SDM-Anwendung auf die Schaltfläche **Monitor**, klicken Sie auf **Protokollierung** und anschließend auf die Registerkarte **Syslog**.
- Zeigen Sie die aktuelle Konfiguration für das Gerät an. Klicken Sie in der SDM-Anwendung auf die Schaltfläche **Konfigurieren** und anschließend auf **Zusätzliche Aufgaben**. Erweitern Sie **Konfigurationsmanagement**, und wählen Sie **Config Editor aus**.

Befehle

Mehrere **show**-Befehle sind WebVPN zugeordnet. Sie können diese Befehle in der Befehlszeilenschnittstelle (CLI) ausführen, um Statistiken und andere Informationen anzuzeigen. Detaillierte Informationen zu **show**-Befehlen finden Sie unter Verifying WebVPN Configuration.

Hinweis: Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Hinweis: Unterbrechen Sie nicht den Befehl **Datei auf Server kopieren,** oder navigieren Sie während des Kopiervorgangs zu einem anderen Fenster. Eine Unterbrechung des Vorgangs kann dazu führen, dass eine unvollständige Datei auf dem Server gespeichert wird.

Hinweis: Benutzer können die neuen Dateien mit dem WebVPN-Client hochladen und herunterladen, der Benutzer ist jedoch nicht berechtigt, die Dateien im Common Internet File System (CIFS) in WebVPN mit dem Befehl **Copy File to Server (Datei in Server kopieren**) zu überschreiben. Der Benutzer erhält diese Meldung, wenn der Benutzer versucht, eine Datei auf dem Server zu ersetzen:

Unable to add the file

Vorgehensweise

Gehen Sie wie folgt vor, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen:

1. Stellen Sie sicher, dass die Clients Popup-Blocker deaktivieren.
2. Stellen Sie sicher, dass für Clients Cookies aktiviert sind.
3. Stellen Sie sicher, dass die Clients die Webbrowser Netscape, Internet Explorer, Firefox oder Mozilla verwenden.

Befehle

Dem WebVPN sind mehrere **Debugbefehle** zugeordnet. Detaillierte Informationen zu diesen Befehlen finden Sie unter Verwenden von WebVPN-Debug-Befehlen.

Hinweis: Die Verwendung von **Debug-**Befehlen kann sich negativ auf Ihr Cisco Gerät auswirken. Bevor Sie **Debug-**Befehle verwenden, lesen Sie die Informationen unter Wichtige Informationen über Debug-Befehle.

Zugehörige Informationen

- Cisco IOS SSL VPN
- Fragen und Antworten zu Cisco IOS SSLVPN
- Beispiel einer IOS-Konfiguration mit Thin-Client SSL VPN (WebVPN) mit SDM
- SSL VPN Client (SVC) auf IOS mit SDM-Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems