Configurazione di una VPN SSL senza client (WebVPN) su Cisco IOS con SDM

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Esempio di rete
Convenzioni
Task di preconfigurazione
Configurazione di WebVPN su Cisco IOS
Passaggio 1. Configurare il gateway WebVPN
Passaggio 2. Configurare le risorse consentite per il gruppo di criteri
Passaggio 3. Configurare il gruppo di criteri WebVPN e selezionare le risorse
Passaggio 4. Configurare il contesto WebVPN
Passaggio 5. Configurazione del database utenti e del metodo di autenticazione
Risultati
Verifica
Procedura
Comandi
Risoluzione dei problemi
Procedura
Comandi
Informazioni correlate

Introduzione

La VPN SSL senza client (WebVPN) consente a un utente di accedere in modo sicuro alle risorse sulla LAN aziendale da qualsiasi luogo con un browser Web abilitato per SSL. L'utente esegue innanzitutto l'autenticazione con un gateway WebVPN che consente all'utente di accedere a risorse di rete preconfigurate. I gateway WebVPN possono essere configurati sui router Cisco IOS®, Cisco Adaptive Security Appliance (ASA), Cisco VPN 3000 concentrator e Cisco WebVPN Services Module per i router Catalyst 6500 e 7600.

La tecnologia SSL (Secure Sockets Layer) e VPN (Virtual Private Network) può essere configurata sui dispositivi Cisco in tre modalità principali: VPN SSL senza client (WebVPN), VPN SSL thin client (inoltro porte) e modalità client VPN SSL (SVC). Questo documento mostra la configurazione di WebVPN sui router Cisco IOS.

Nota: non modificare il nome di dominio IP o il nome host del router in quanto ciò attiverà la

rigenerazione del certificato autofirmato e sostituirà il trust point configurato. La rigenerazione del certificato autofirmato causa problemi di connessione se il router è stato configurato per WebVPN. WebVPN associa il nome del trust point SSL alla configurazione del gateway WebVPN. Pertanto, se viene rilasciato un nuovo certificato autofirmato, il nome del nuovo trust point non corrisponde alla configurazione WebVPN e gli utenti non sono in grado di connettersi.

Nota: se si esegue il comando **ip https-secure server** su un router WebVPN che utilizza un certificato autofirmato permanente, viene generata una nuova chiave RSA e il certificato non è più valido. Viene creato un nuovo trust point che interrompe SSL WebVPN. Se il router che usa il certificato autofirmato persistente viene riavviato dopo aver eseguito il comando **ip https-secure server**, si verifica lo stesso problema.

Per ulteriori informazioni sulla VPN SSL thin-client, consultare l'esempio di configurazione di IOS per la VPN SSL thin-client (WebVPN) con SDM.

Per ulteriori informazioni sul client VPN SSL, fare riferimento a SVC (SSL VPN Client) su IOS con configurazione SDM.

La VPN SSL viene eseguita sulle seguenti piattaforme di router Cisco:

- Cisco serie 870, 1811, 1841, 2801, 2811, 2821 e 2851 router
- Router Cisco serie 3725, 3745, 3825, 3845, 7200 e 7301

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Immagine avanzata del software Cisco IOS versione 12.4(6)T o successive
- Una delle piattaforme router Cisco elencate nell'introduzione

Componenti usati

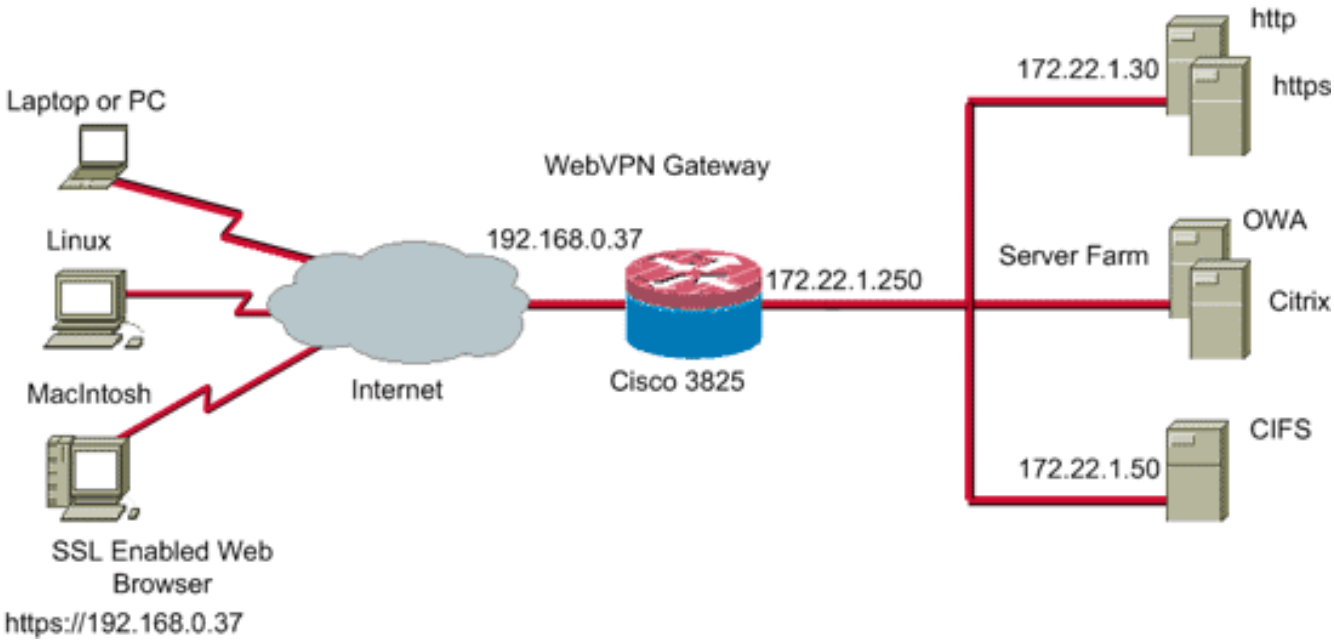
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 3825 router
- Immagine software aziendale avanzata - Software Cisco IOS versione 12.4(9)T
- Cisco Router and Security Device Manager (SDM) - versione 2.3.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi. Gli indirizzi IP utilizzati in questo esempio sono tratti da indirizzi RFC 1918 privati e non legali da utilizzare su Internet.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Task di preconfigurazione

Prima di iniziare, eseguire le attività seguenti:

1. Configurare un nome host e un nome di dominio.
2. Configurare il router per SDM. Cisco invia ad alcuni router una copia preinstallata dell'SDM.Se il software Cisco SDM non è già caricato sul router, è possibile ottenerne una copia gratuita dal sito Download software (solo utenti registrati). Devi avere un account CCO con un contratto di assistenza. Per informazioni dettagliate sull'installazione e la configurazione dell'SDM, consultare il documento Cisco Router and Security Device Manager.
3. Configurare la data, l'ora e il fuso orario corretti per il router.

Configurazione di WebVPN su Cisco IOS

Èpossibile associare più gateway WebVPN a un dispositivo. Ogni gateway WebVPN è collegato a un solo indirizzo IP del router. È possibile creare più contesti WebVPN per un particolare gateway WebVPN. Per identificare singoli contesti, assegnare a ogni contesto un nome univoco. È possibile associare un gruppo di criteri a un solo contesto WebVPN. Il gruppo di criteri descrive le risorse disponibili in un particolare contesto WebVPN.

Completare questi passaggi per configurare WebVPN su Cisco IOS:

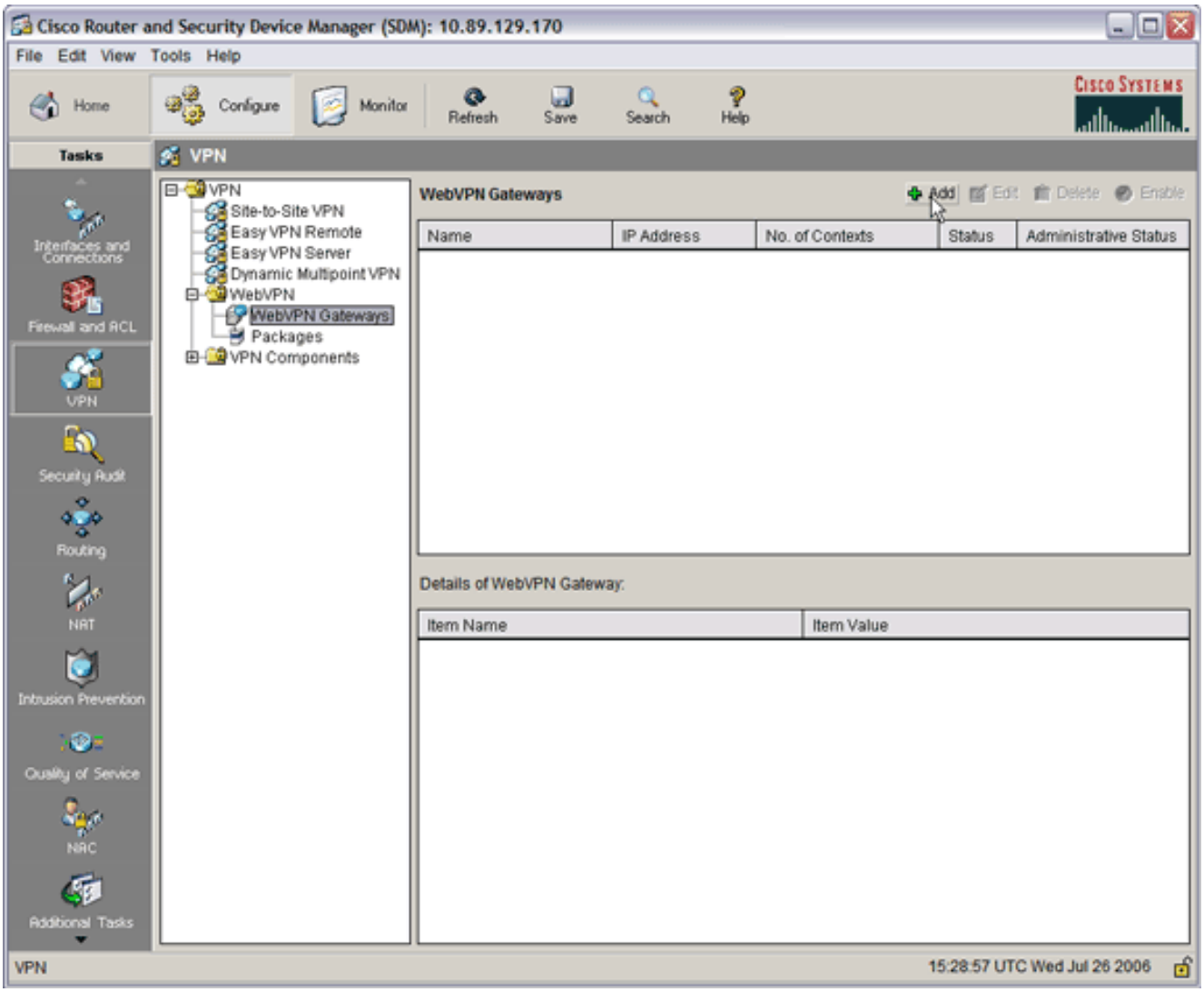
1. Configurare il gateway WebVPN
2. Configurare le risorse consentite per il gruppo di criteri
3. Configurare il gruppo di criteri WebVPN e selezionare le risorse
4. Configurare il contesto WebVPN

5. Configurare il database utente e il metodo di autenticazione

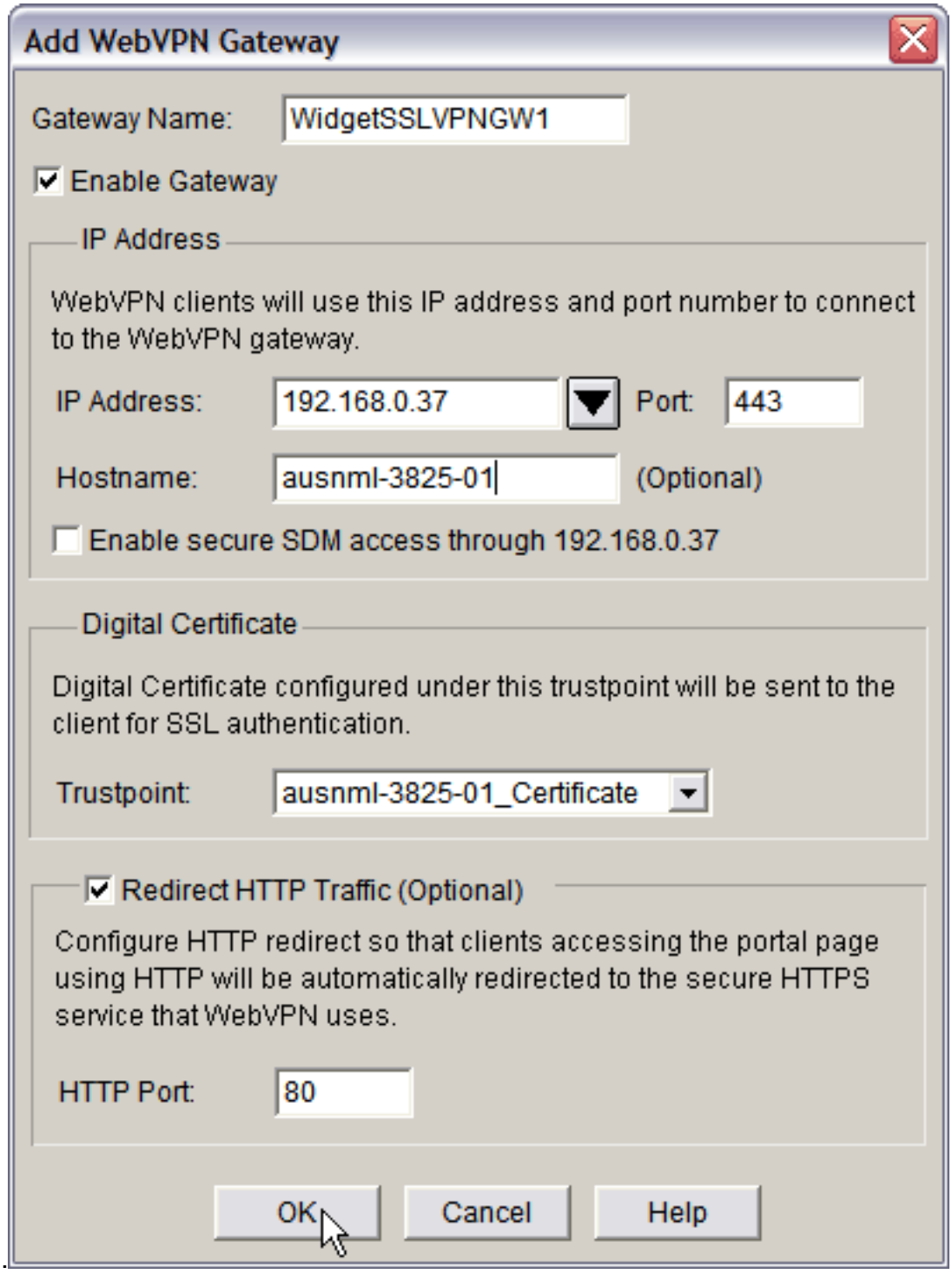
Passaggio 1. Configurare il gateway WebVPN

Per configurare il gateway WebVPN, completare i seguenti passaggi:

1. Nell'applicazione SDM, fare clic su **Configure** (Configura), quindi su **VPN**.
2. Espandere **WebVPN** e scegliere **Gateway WebVPN**.



3. Fare clic su **Add**.Verrà visualizzata la finestra di dialogo Aggiungi gateway



WebVPN.

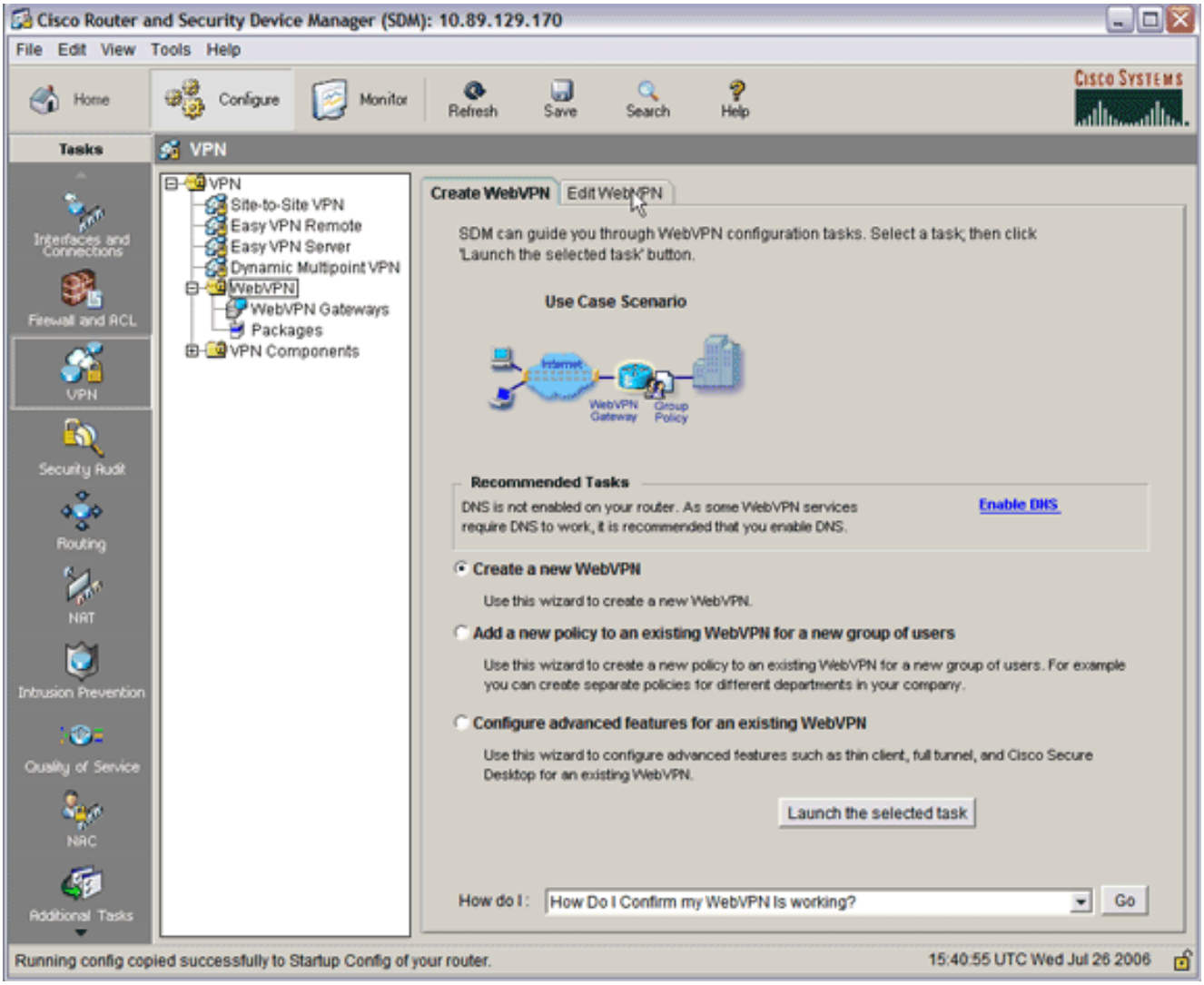
4. Immettere i valori nei campi Nome gateway e Indirizzo IP, quindi selezionare la casella di controllo **Abilita gateway**.
5. Selezionare la casella di controllo **Reindirizza traffico HTTP** e quindi fare clic su **OK**.
6. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

Passaggio 2. Configurare le risorse consentite per il gruppo di criteri

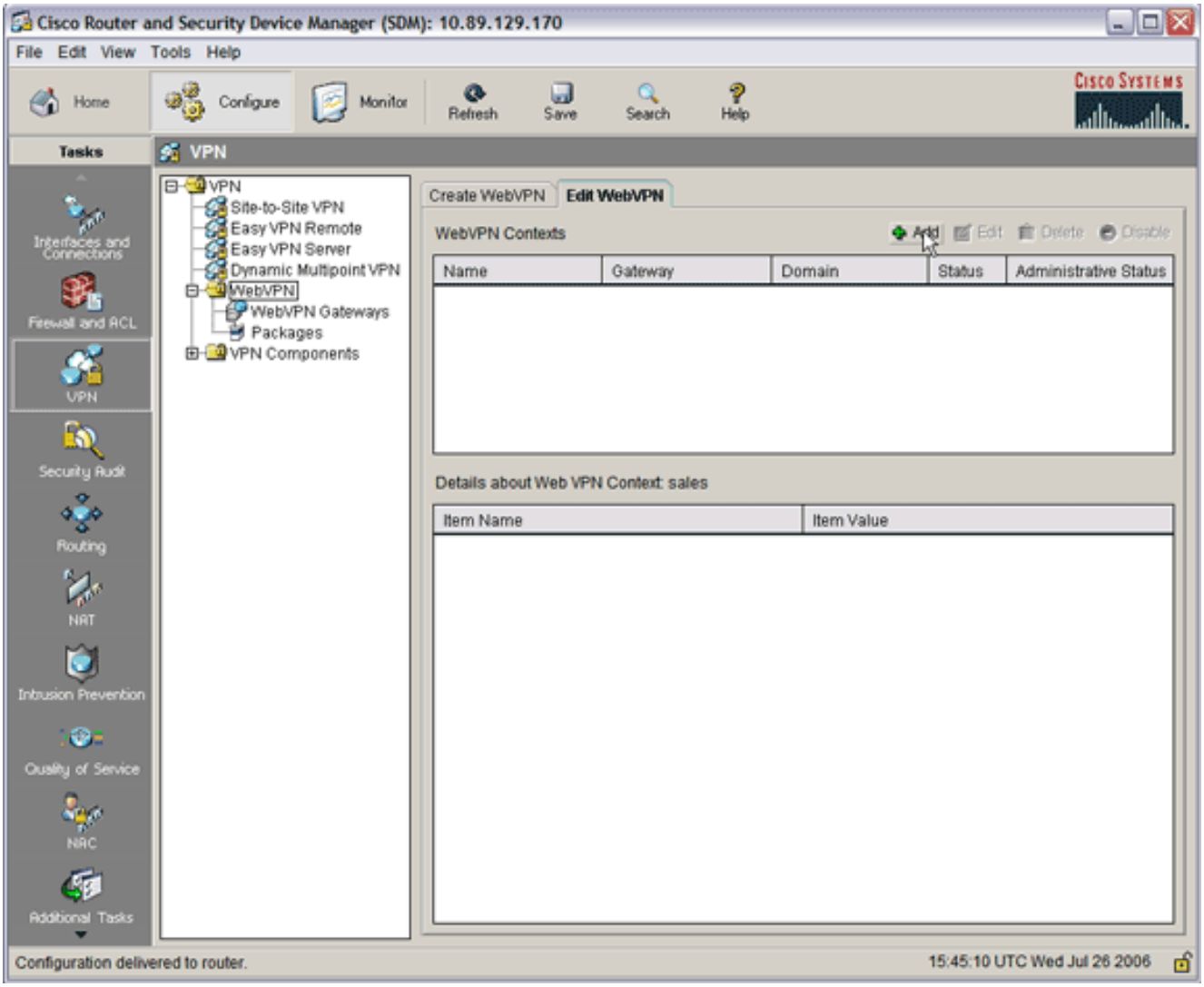
Per semplificare l'aggiunta di risorse a un gruppo di criteri, è possibile configurare le risorse prima di creare il gruppo di criteri.

Completare questa procedura per configurare le risorse consentite per il gruppo di criteri:

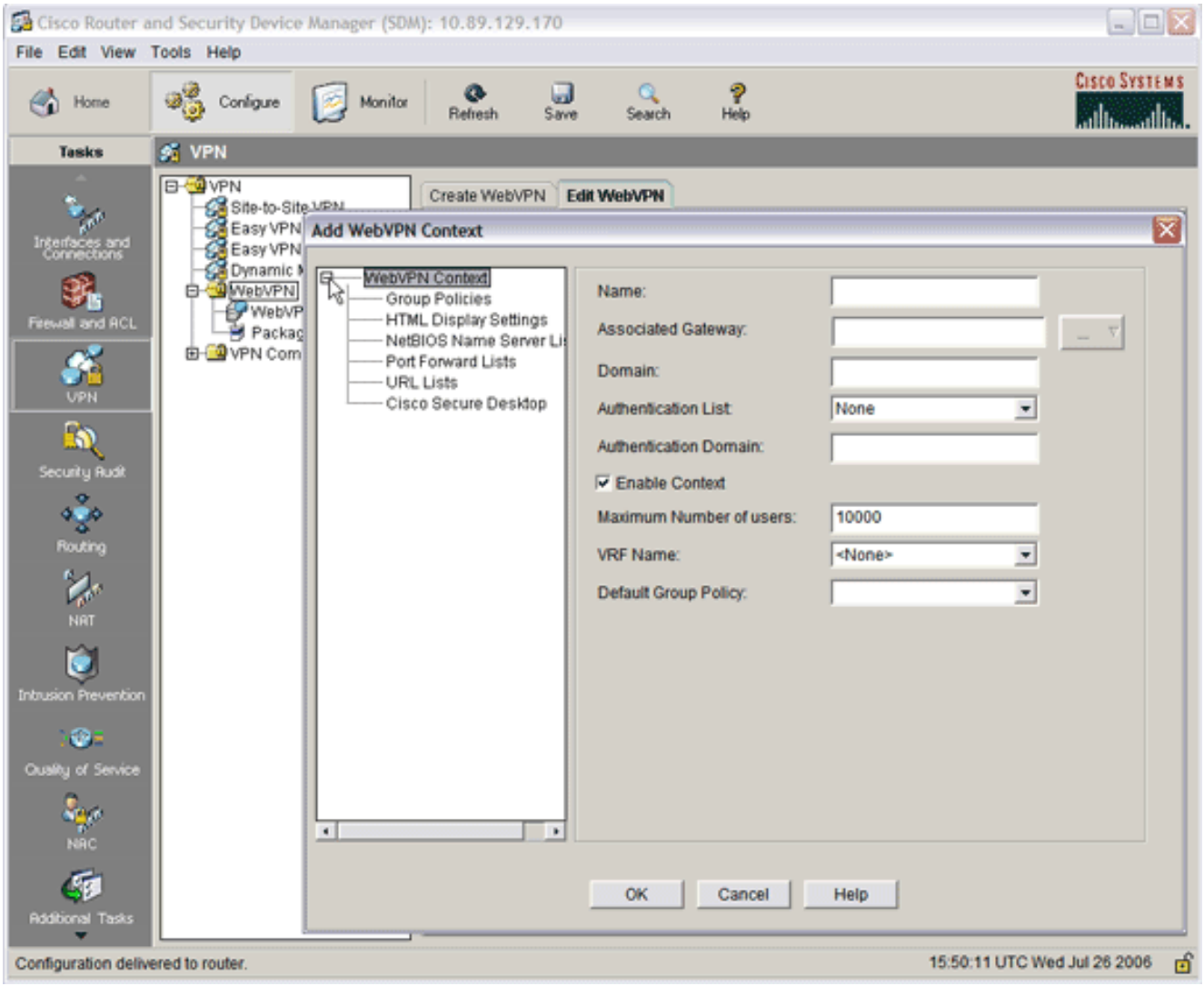
1. Fare clic su **Configura** e quindi su **VPN**.



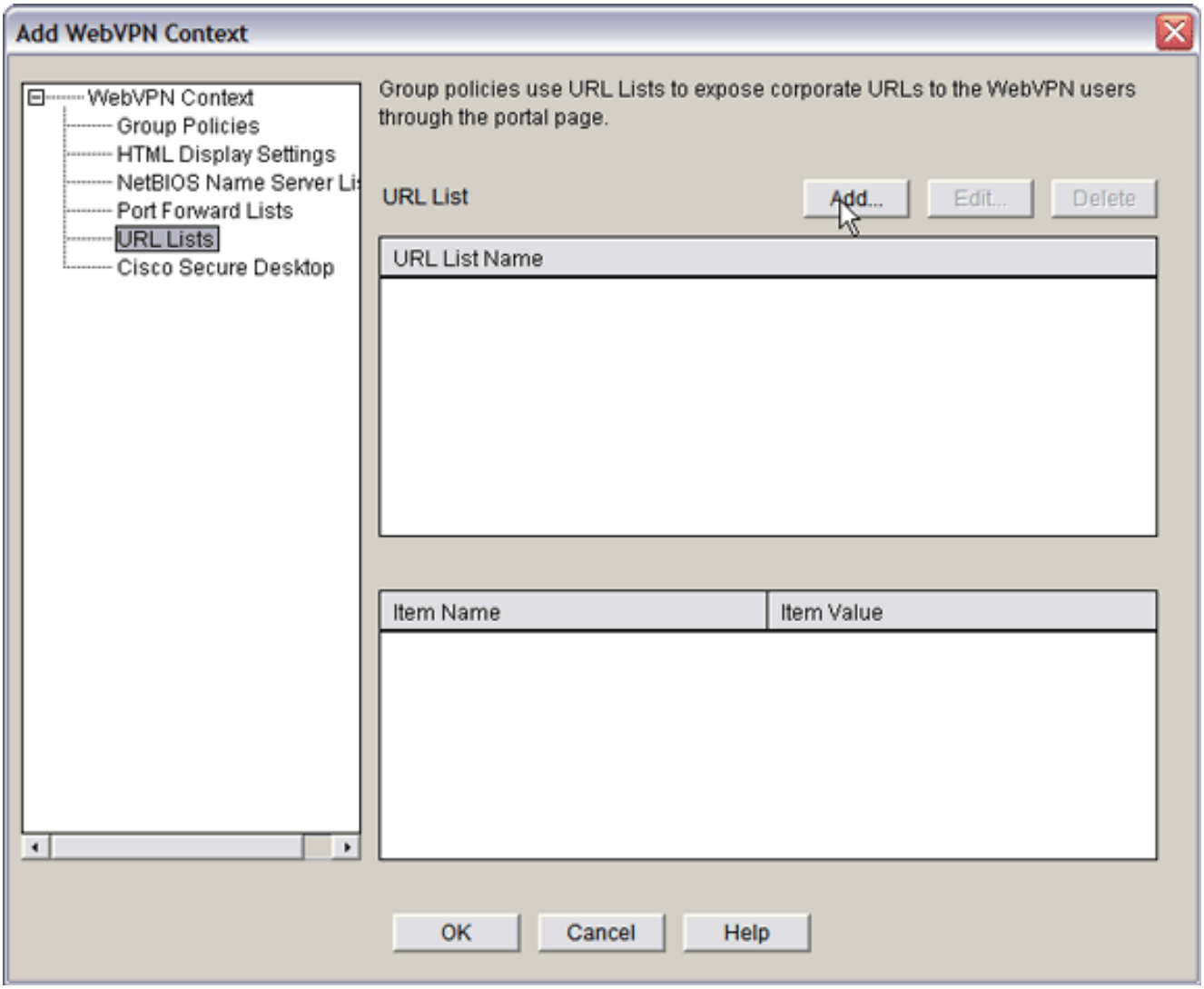
2. Scegliere **WebVPN**, quindi fare clic sulla scheda **Modifica WebVPN**.**Nota:** WebVPN consente di configurare l'accesso per HTTP, HTTPS, l'esplorazione dei file di Windows tramite il protocollo CIFS (Common Internet File System) e
Citrix.



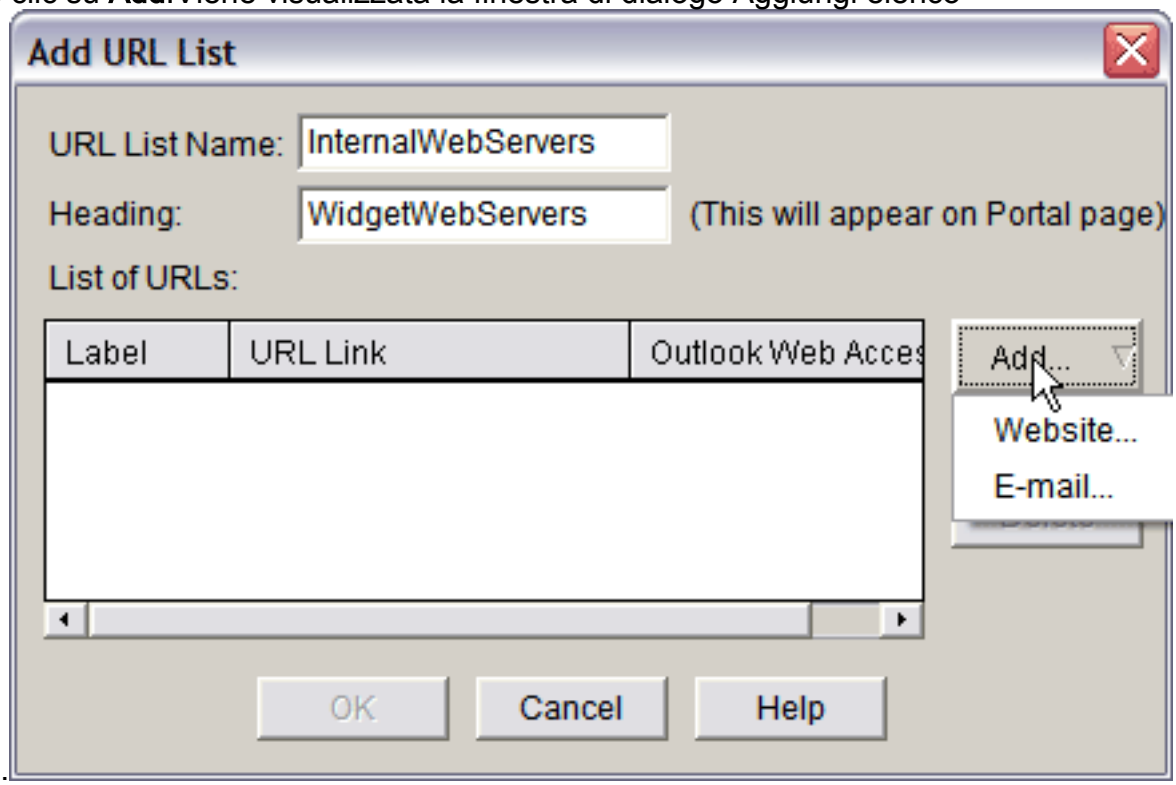
3. Fare clic su **Add**.Verrà visualizzata la finestra di dialogo Aggiungi contesto WebVPN.



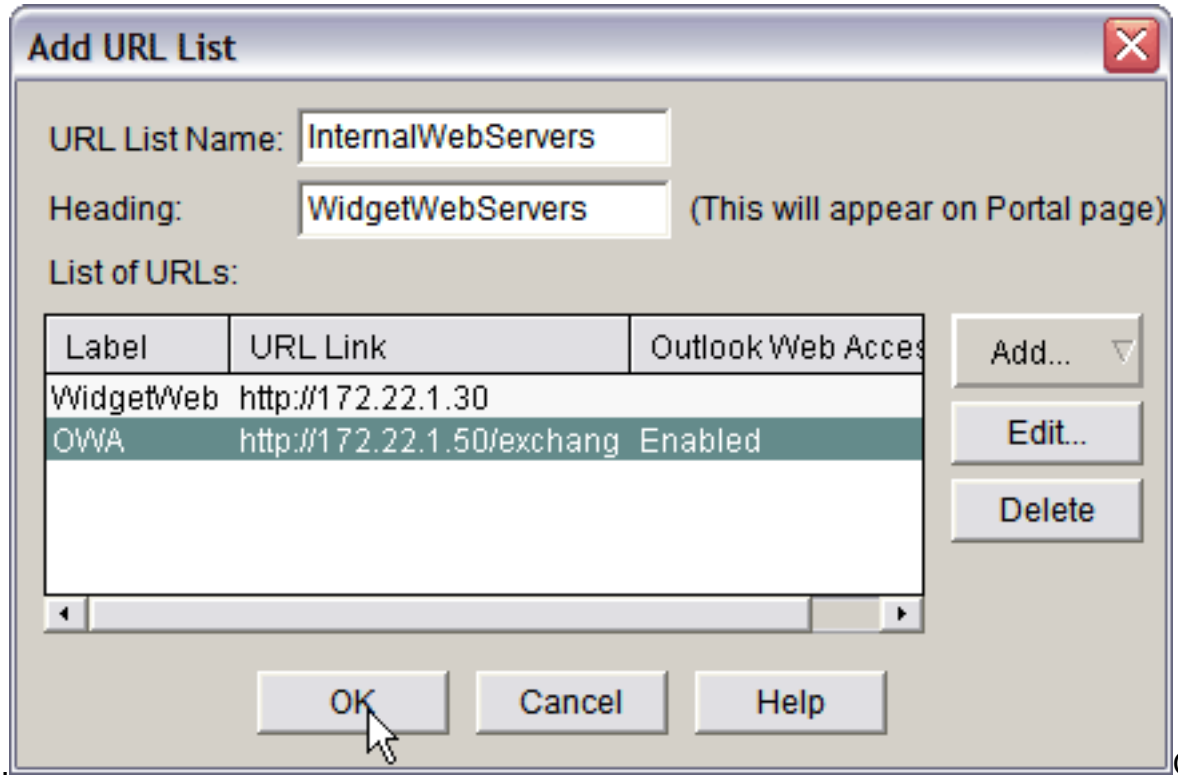
4. Espandere **Contesto WebVPN** e scegliere **Elenchi URL**.



5. Fare clic su **Add**.Viene visualizzata la finestra di dialogo Aggiungi elenco URL.

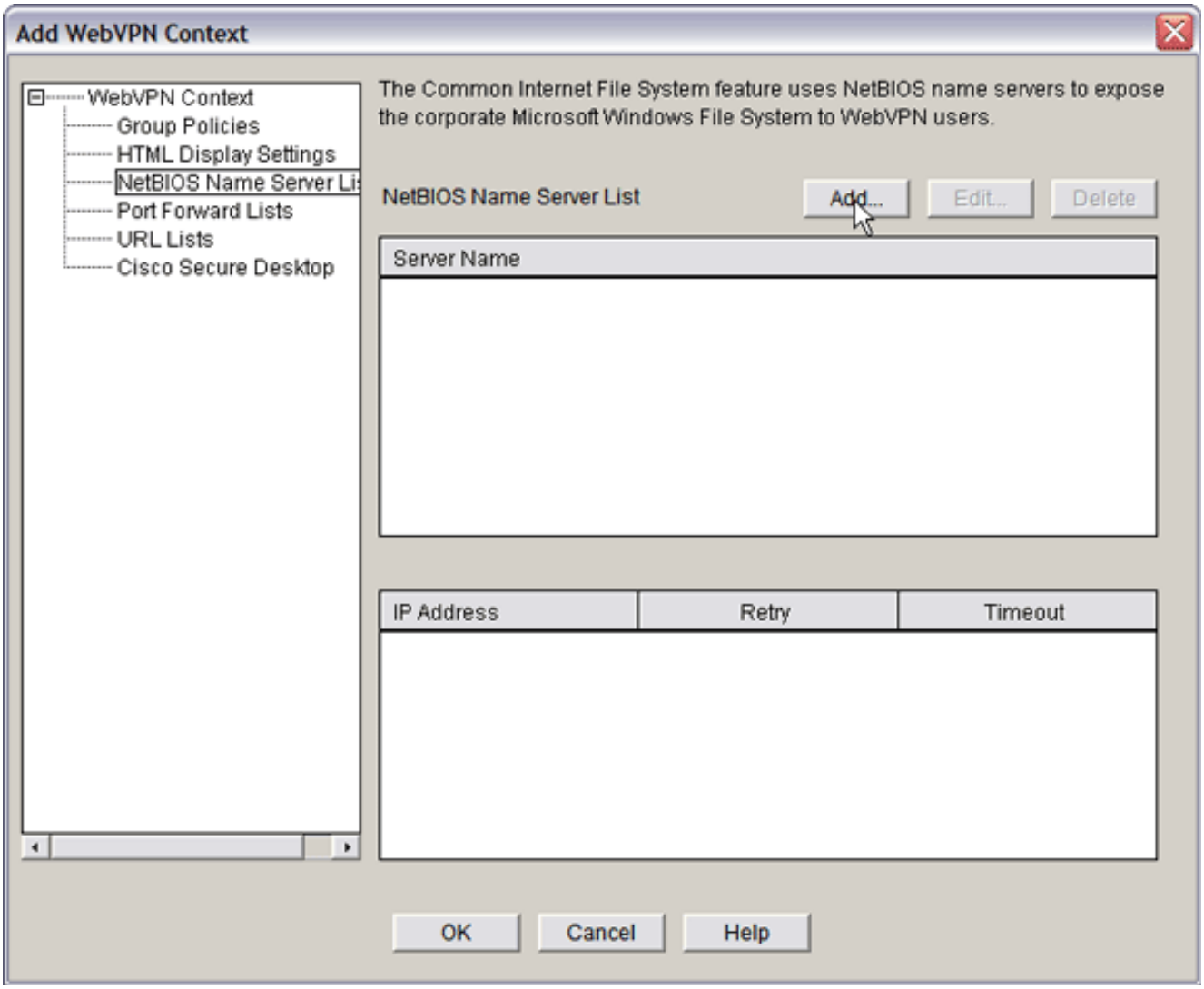


6. Immettere i valori nei campi Nome elenco URL e Intestazione.
7. Fare clic su **Add** (Aggiungi), quindi selezionare **Website** (Sito

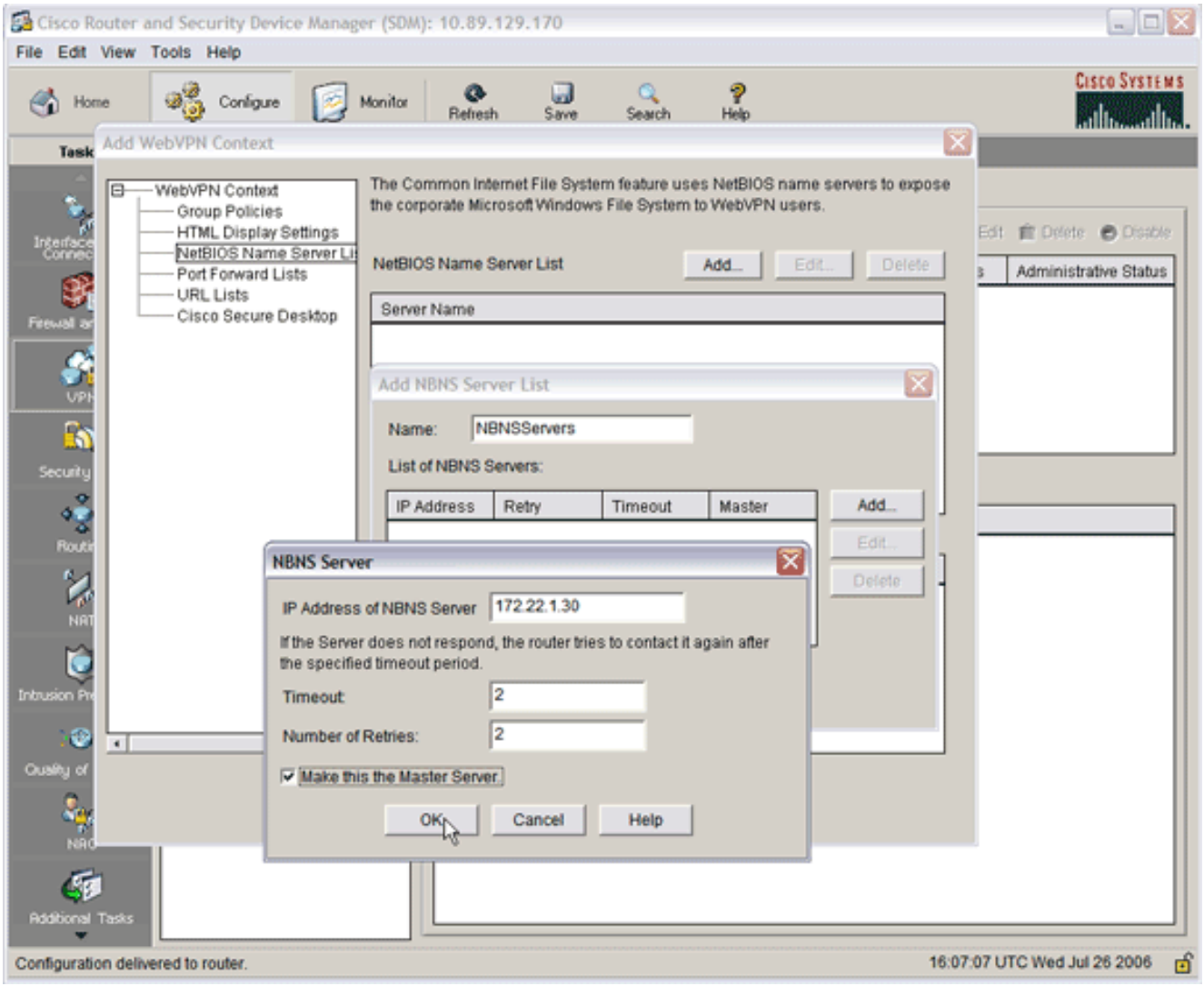


Web).Questo elenco contiene tutti i server Web HTTP e HTTPS che si desidera rendere disponibili per questa connessione WebVPN.

8. Per aggiungere l'accesso per Outlook Web Access (OWA), fare clic su **Aggiungi**, scegliere **Posta elettronica** e quindi fare clic su **OK** dopo aver compilato tutti i campi desiderati.
9. Per consentire l'esplorazione dei file di Windows tramite CIFS, è possibile designare un server NBNS (NetBIOS Name Service) e configurare in modo appropriato le condivisioni appropriate nel dominio Windows.Dall'elenco Contesto WebVPN, scegliere **Elenchi server dei nomi NetBIOS**.



Fare clic su **Add**.Verrà visualizzata la finestra di dialogo Aggiungi elenco server NBNS.Immettere un nome per l'elenco e fare clic su **Aggiungi**.Verrà visualizzata la finestra di dialogo Server
NBNS.

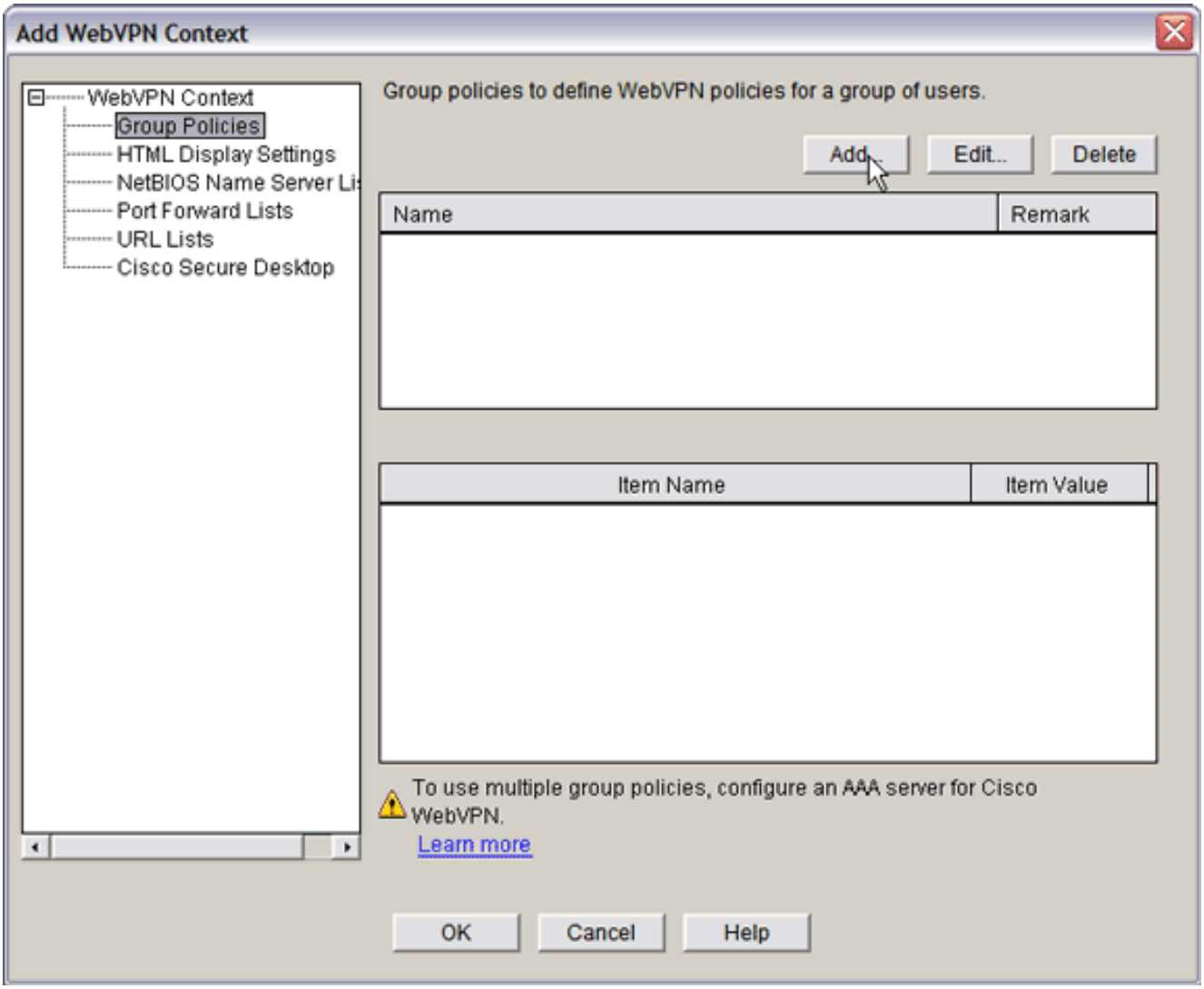


Se applicabile, selezionare la casella di controllo **Imposta come server master**.Fare clic su **OK**, quindi su **OK**.

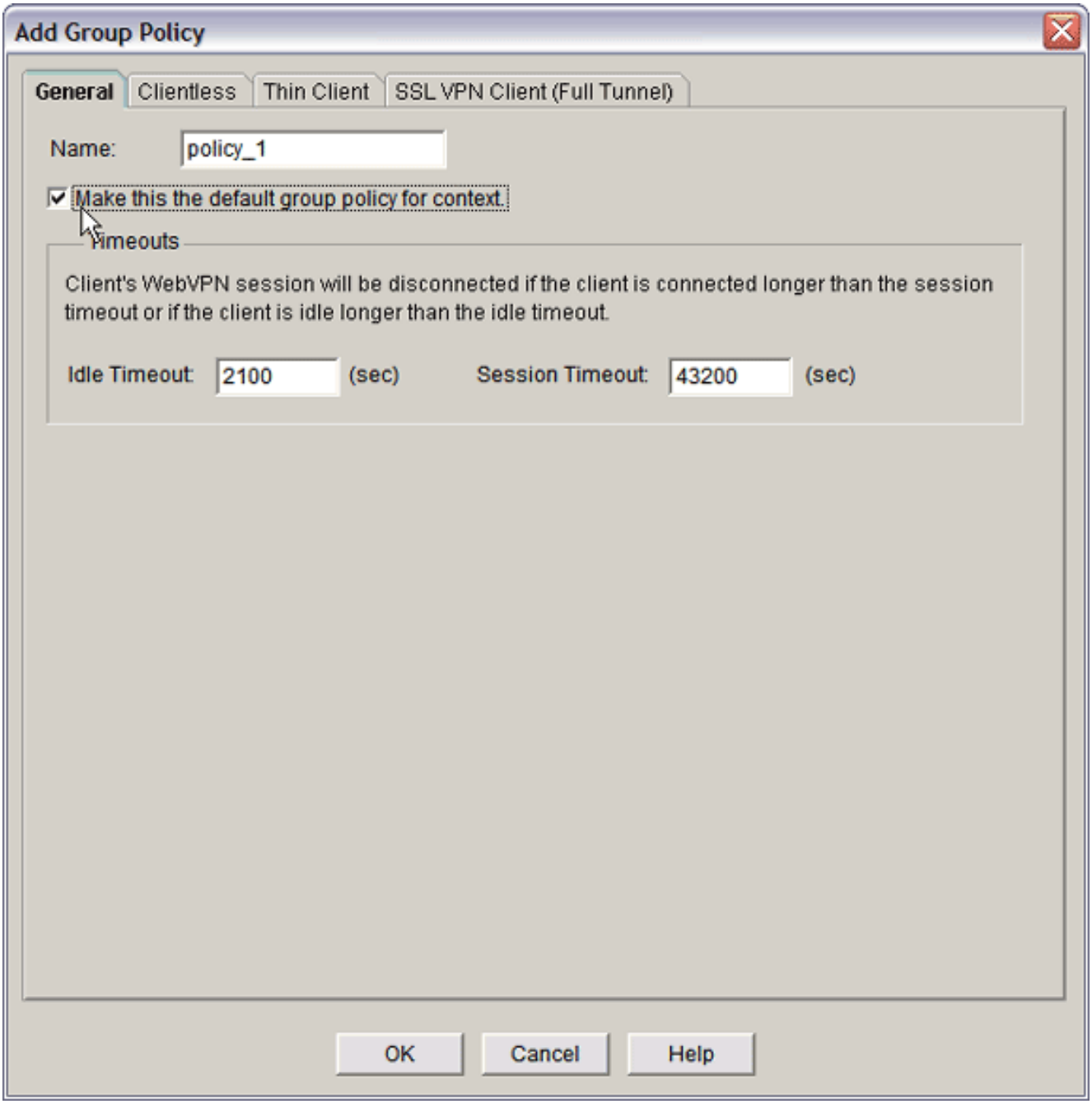
Passaggio 3. Configurare il gruppo di criteri WebVPN e selezionare le risorse

Completare questa procedura per configurare il gruppo di criteri WebVPN e selezionare le risorse:

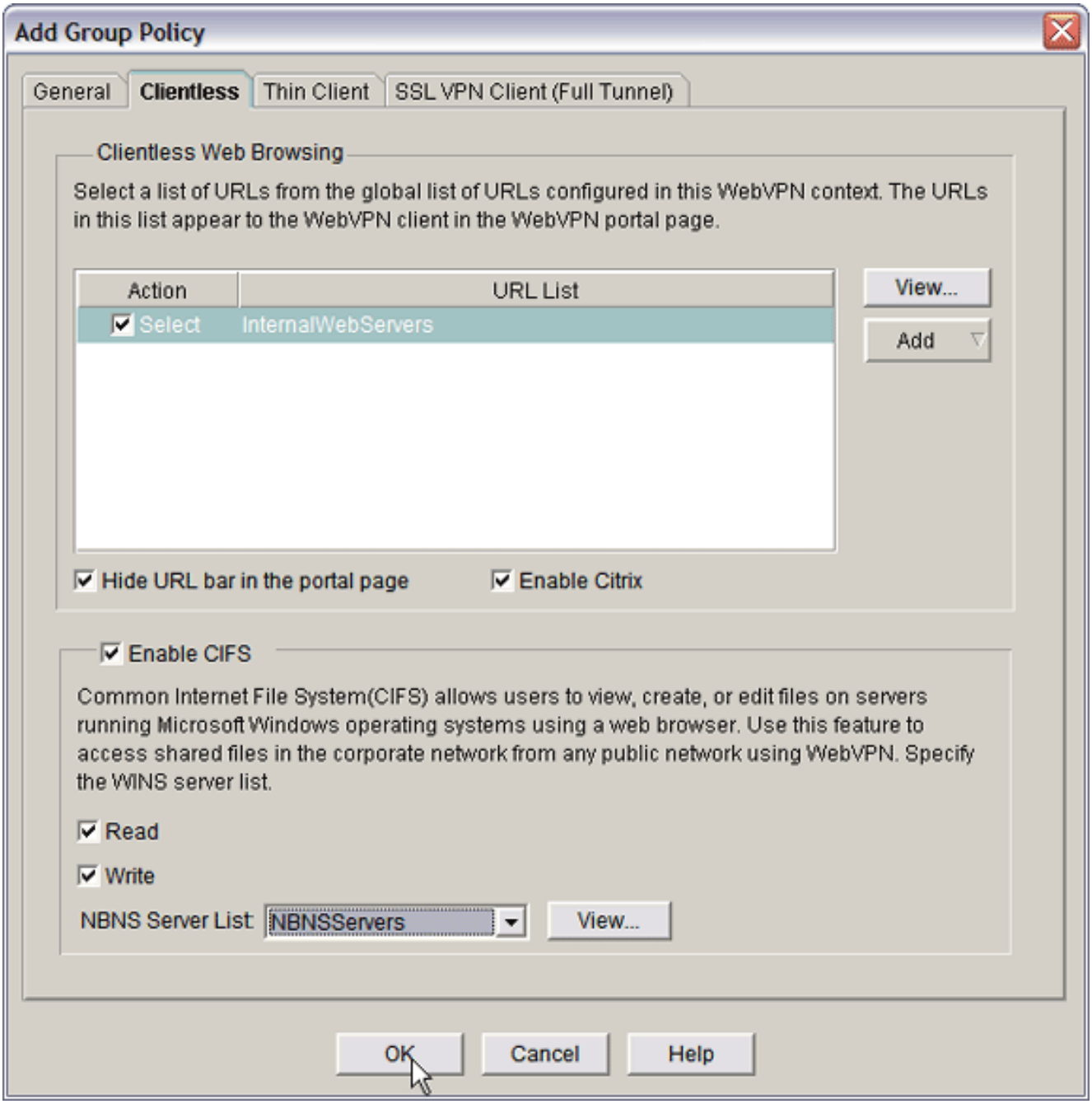
1. Fare clic su **Configura** e quindi su **VPN**.
2. Espandere **WebVPN** e scegliere **Contesto WebVPN**.



3. Scegliere **Criteri di gruppo** e fare clic su **Aggiungi**.Verrà visualizzata la finestra di dialogo Aggiungi Criteri di
gruppo.



4. Immettere un nome per il nuovo criterio e selezionare la casella di controllo **Imposta come criterio di gruppo predefinito per il contesto**.
5. Fare clic sulla scheda **Senza client** nella parte superiore della finestra di dialogo.

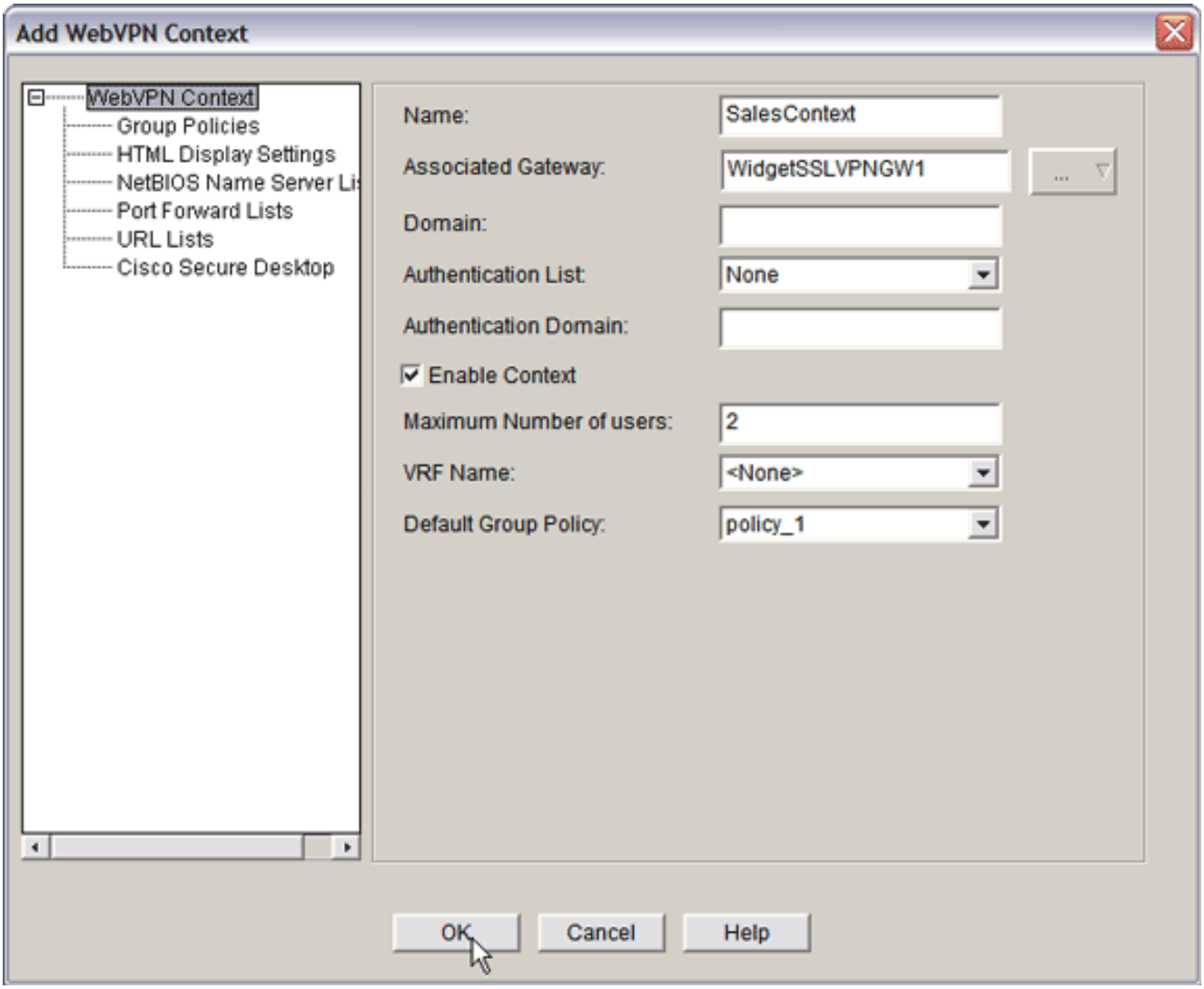


6. Selezionare la casella di controllo **Select** (Seleziona) per l'elenco di URL desiderato.
7. Se i clienti utilizzano client Citrix che richiedono l'accesso ai server Citrix, selezionare la casella di controllo **Abilita Citrix**.
8. Selezionare le caselle di controllo **Attiva CIFS**, **Lettura** e **Scrittura**.
9. Fare clic sulla freccia a discesa **Elenco server NBNS** e scegliere l'elenco dei server NBNS creato per l'esplorazione dei file di Windows nel passaggio 2.
10. Fare clic su **OK**.

Passaggio 4. Configurare il contesto WebVPN

Per collegare il gateway WebVPN, i Criteri di gruppo e le risorse, è necessario configurare il contesto WebVPN. Per configurare il contesto WebVPN, attenersi alla seguente procedura:

1. Scegliere **Contesto WebVPN** e immettere un nome per il contesto.



2. Fare clic sulla freccia a discesa Gateway associato e scegliere un gateway associato.
3. Se si desidera creare più contesti, immettere un nome univoco nel campo Dominio per identificare il contesto. Se si lascia vuoto il campo Dominio, gli utenti devono accedere alla WebVPN con **https://*IndirizzoIP***. Se si immette un nome di dominio, ad esempio *Vendite*, gli utenti devono connettersi con **https://*IndirizzoIP*/Vendite**.
4. Selezionare la casella di controllo **Attiva contesto**.
5. Nel campo Numero massimo di utenti, immettere il numero massimo di utenti consentito dalla licenza del dispositivo.
6. Fare clic sulla freccia a discesa **Criteri di gruppo predefiniti** e selezionare i criteri di gruppo da associare al contesto.
7. Fare clic su **OK**, quindi su **OK**.

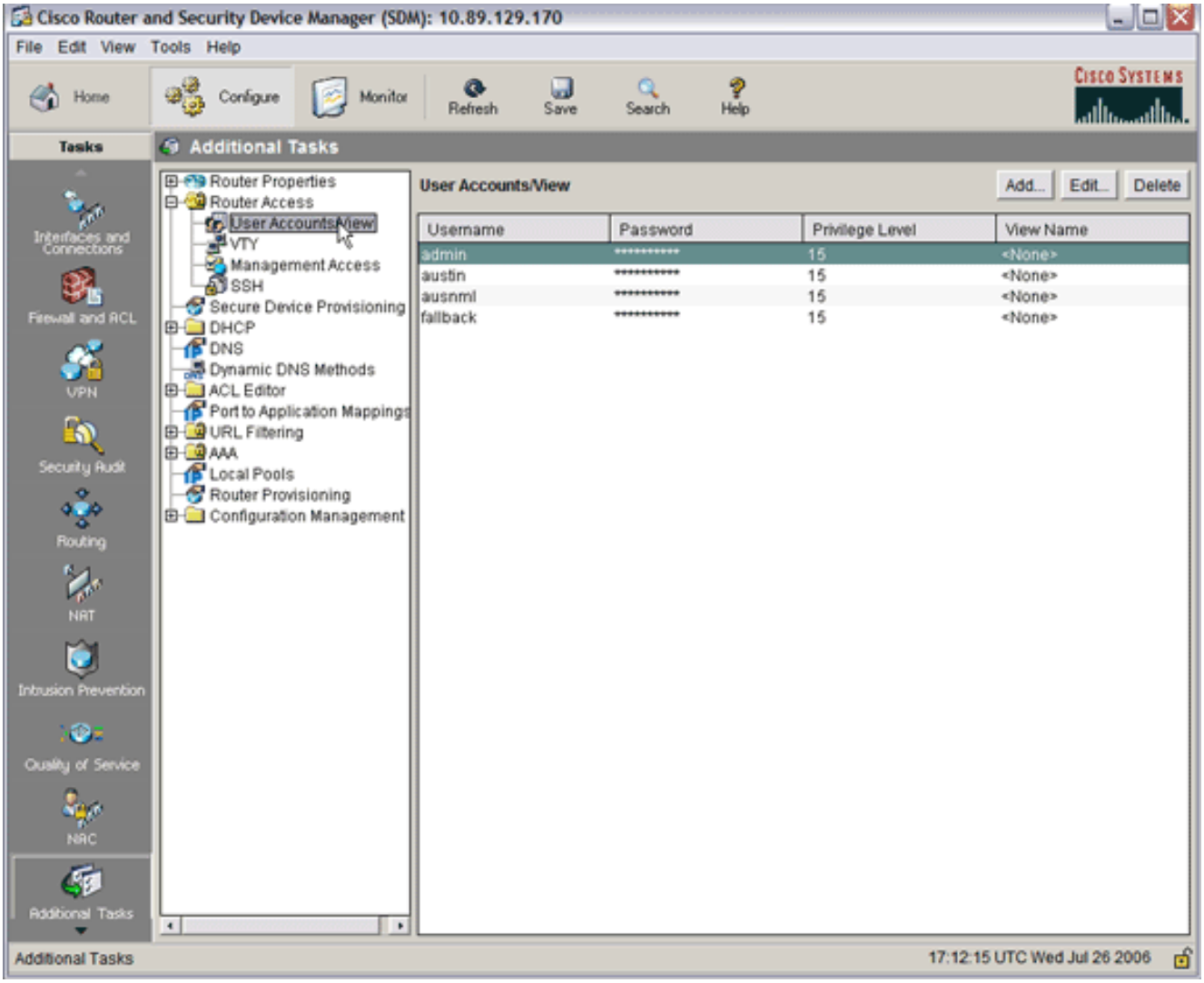
Passaggio 5. Configurazione del database utenti e del metodo di autenticazione

Èpossibile configurare le sessioni SSL VPN (WebVPN) senza client per l'autenticazione con Radius, il server Cisco AAA o un database locale. In questo esempio viene utilizzato un database locale.

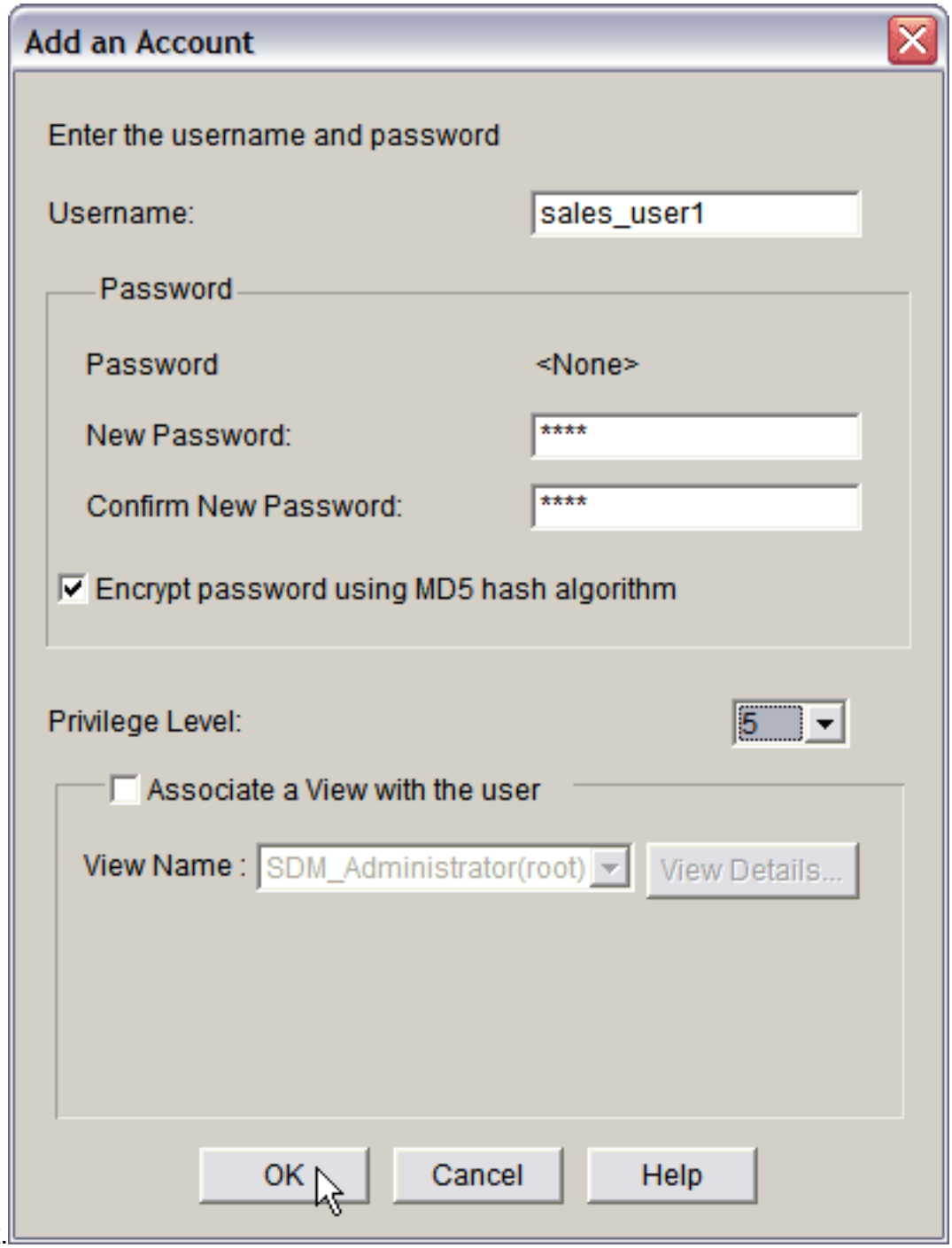
Per configurare il database utenti e il metodo di autenticazione, completare la procedura seguente:

1. Fare clic su **Configurazione** e quindi su **Attività aggiuntive**.
2. Espandere **Accesso router** e scegliere **Account**

utente/Visualizza.



3. Fare clic sul pulsante **Aggiungi**.Verrà visualizzata la finestra di dialogo Aggiungi



account.

4. Immettere un account utente e una password.
5. Fare clic su **OK**, quindi su **OK**.
6. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

Risultati

ASDM crea le seguenti configurazioni della riga di comando:

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
```

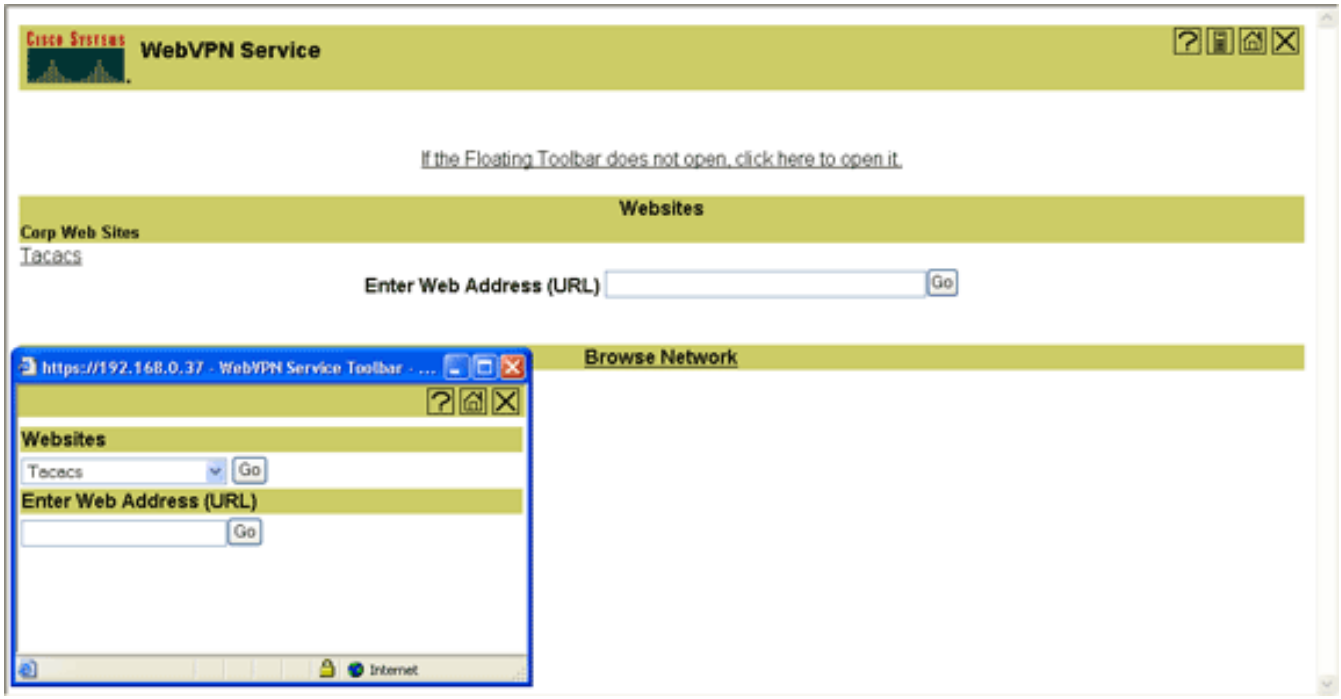
Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Procedura

Per verificare che la configurazione funzioni correttamente, completare le seguenti procedure:

- Verificare la configurazione con un utente. Immettere **https://*WebVPN_Gateway_IP_Address*** in un browser abilitato per SSL; dove *WebVPN_Gateway_IP_Address* è l'indirizzo IP del servizio WebVPN. Dopo aver accettato il certificato e aver immesso un nome utente e una password, verrà visualizzata una schermata simile a questa immagine.



- Controllare la sessione VPN SSL. Nell'applicazione SDM, fare clic sul pulsante **Monitor**, quindi su **VPN Status** (Stato VPN). Espandere **WebVPN (tutti i contesti)**, espandere il contesto appropriato e scegliere **Utenti**.
- Controllare i messaggi di errore. Nell'applicazione SDM, fare clic sul pulsante **Monitor**, selezionare **Logging**, quindi fare clic sulla scheda **Syslog**.
- Visualizzare la configurazione corrente del dispositivo. Nell'applicazione SDM, fare clic sul pulsante **Configure** (Configura), quindi su **Additional Tasks** (Attività aggiuntive). Espandere **Gestione configurazione** e scegliere **Editor configurazione**.

Comandi

Diversi comandi **show** sono associati a WebVPN. È possibile eseguire questi comandi dall'interfaccia della riga di comando (CLI) per visualizzare le statistiche e altre informazioni. Per informazioni dettagliate sui comandi **show**, consultare il documento sulla verifica della configurazione di WebVPN.

Nota: lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Nota: non interrompere il comando **Copia file sul server** né passare a un'altra finestra durante la copia. L'interruzione dell'operazione può causare il salvataggio di un file incompleto sul server.

Nota: gli utenti possono caricare e scaricare i nuovi file utilizzando il client WebVPN, ma non possono sovrascrivere i file nel CIFS (Common Internet File System) su WebVPN utilizzando il comando **Copia file sul server**. L'utente riceve questo messaggio quando tenta di sostituire un file sul server:

```
Unable to add the file
```

Procedura

Per risolvere i problemi relativi alla configurazione, completare la procedura seguente:

1. Assicurarsi che i client disabilitino i blocchi popup.
2. Verificare che i client abbiano i cookie abilitati.
3. Assicurarsi che i client utilizzino i browser Netscape, Internet Explorer, Firefox o Mozilla.

Comandi

Diversi comandi **debug** sono associati a WebVPN. Per informazioni dettagliate su questi comandi, fare riferimento a Uso dei comandi di debug WebVPN.

Nota: l'uso dei comandi di **debug** può avere un impatto negativo sul dispositivo Cisco. Prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Informazioni correlate

- Cisco IOS SSLVPN
- Domande e risposte su Cisco IOS SSLVPN
- Esempio di configurazione di IOS per una VPN SSL thin-client (WebVPN) con SDM
- Esempio di configurazione di SSL VPN Client (SVC) su IOS con SDM
- Documentazione e supporto tecnico – Cisco Systems