

SDM を使用した Cisco IOS でのクライアントレス SSL VPN (WebVPN) の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[設定前の作業](#)

[Cisco IOS での WebVPN の設定](#)

[ステップ 1. WebVPN ゲートウェイの設定](#)

[ステップ 2. ポリシー グループに対して許可されるリソースの設定](#)

[ステップ 3. WebVPN ポリシー グループの設定とリソースの選択](#)

[ステップ 4. WebVPN コンテキストの設定](#)

[ステップ 5. ユーザ データベースと認証方法の設定](#)

[結果](#)

[確認](#)

[手順](#)

[コマンド](#)

[トラブルシューティング](#)

[手順](#)

[コマンド](#)

[関連情報](#)

概要

クライアントレス SSL VPN (WebVPN) では、SSL 対応ブラウザがあれば、ユーザはどんな場所からでも安全に企業 LAN のリソースへアクセスできます。ユーザはまず WebVPN ゲートウェイで認証を受けますが、WebVPN ゲートウェイでは、あらかじめ設定されたネットワーク リソースへのユーザ アクセスが許可されます。WebVPN ゲートウェイは、Cisco IOS® ルータ、Cisco Adaptive Security Appliances (ASA; 適応型セキュリティ アプライアンス)、Cisco VPN 3000 コンセントレータ、Catalyst 6500 および 7600 ルータ対応 Cisco WebVPN サービス モジュールに設定できます。

Secure Socket Layer (SSL) Virtual Private Network (VPN; 仮想プライベート ネットワーク) テクノロジーは、3 つの主要モードで Cisco デバイス上に設定できます。3 つのモードとは、クライアントレス SSL VPN (WebVPN)、シンクライアント SSL VPN (ポート転送)、および SSL VPN クライアント (SVC) モードです。このドキュメントでは、Cisco IOS ルータでの WebVPN の設定方法を紹介します。

注: ルータの IP ドメイン名またホスト名に変更を加えないでください。自己署名証明書が再生成され、設定済みのトラストポイントが無効になります。ルータが WebVPN 用に設定されている場合、自己署名証明書が再生成されると、接続の問題が発生します。WebVPN は、SSL トラストポイント名を WebVPN ゲートウェイ設定に結びつけます。このため、新しい自己署名証明書が発行されると、新しいトラストポイント名が WebVPN の設定と一致せず、ユーザが接続できません。

注: 永続的な自己署名証明書を使用する WebVPN ルータで `ip https-secure server` コマンドを実行すると、新しい RSA キーが生成されて、証明書が無効になります。新しいトラストポイントが作成されて、このトラストポイントが SSL WebVPN を中断します。`ip https-secure server` コマンドを実行した後に、永続的な自己署名証明書を使用するルータが再起動すると、同じ問題が発生します。

シンクライアント SSL VPN についての詳細は、『[SDM によるシンクライアント SSL VPN \(WebVPN \) の IOS 設定例](#)』を参照してください。

SSL VPN Client の詳細は、『[SDM を使用した IOS での SSL VPN Client \(SVC \) の設定例](#)』を参照してください。

SSL VPN は次の Cisco ルータ プラットフォームで動作します。

- Cisco 870、1811、1841、2801、2811、2821 および 2851 シリーズ ルータ
- Cisco 3725、3745、3825、3845、7200、および 7301 シリーズ ルータ

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco IOS ソフトウェア リリース 12.4(6)T 以降の拡張イメージ
- 「[概要](#)」に記載されている Cisco ルータ プラットフォームのいずれか

使用するコンポーネント

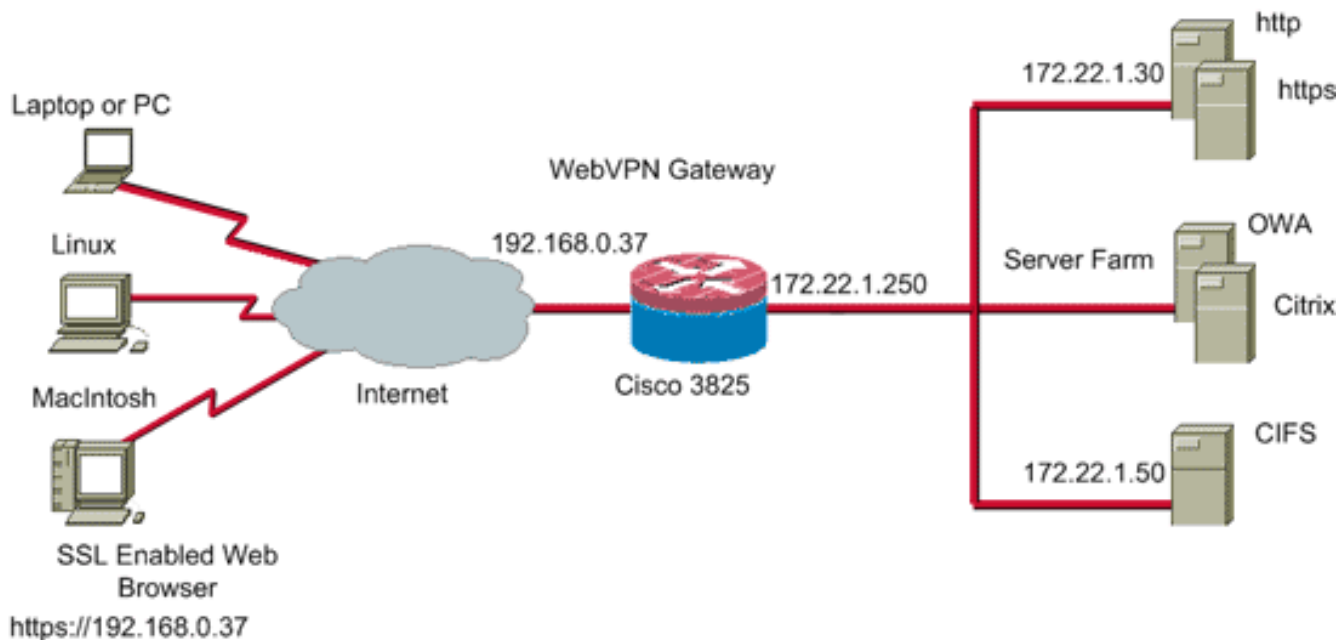
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 3825 ルータ
- 拡張 Enterprise ソフトウェア イメージ : Cisco IOS ソフトウェア リリース 12.4(9)T
- Cisco Router and Security Device Manager (SDM) - バージョン 2.3.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。次の例で使用する IP アドレスは、RFC 1918 から引用したプライベートアドレスで、インターネットでの使用には適格ではありません。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

設定前の作業

開始する前に、次の作業を実行してください。

1. ホスト名とドメイン名を設定します。
2. ルータの SDM 設定を行います。一部のシスコルータには、SDM がプリインストールされています。Cisco SDM がルータにロードされていない場合は、このソフトウェアの無償コピーを [\[Software Download\] ページ](#) (登録ユーザ専用) からダウンロードできます。サービス契約を結んでいる Cisco.com アカウントが必要です。SDM のインストールと設定についての詳細、『[Cisco ルータとセキュリティデバイス マネージャ](#)』を参照してください。
3. ルータで正しい日付、時刻、および時間帯を設定します。

Cisco IOS での WebVPN の設定

1つのデバイスに、複数の WebVPN ゲートウェイを関連付けることができます。各 WebVPN ゲートウェイは、ルータ上の1つの IP アドレスにのみリンクされます。特定の WebVPN ゲートウェイに複数の WebVPN コンテキストを作成できます。各コンテキストを識別するため、コンテキストに一意的な名前を付けます。1つのポリシーグループは、1つの WebVPN コンテキストにのみ関連付けられます。ポリシーグループは、特定の WebVPN コンテキストでどのリソースが利用可能かを説明します。

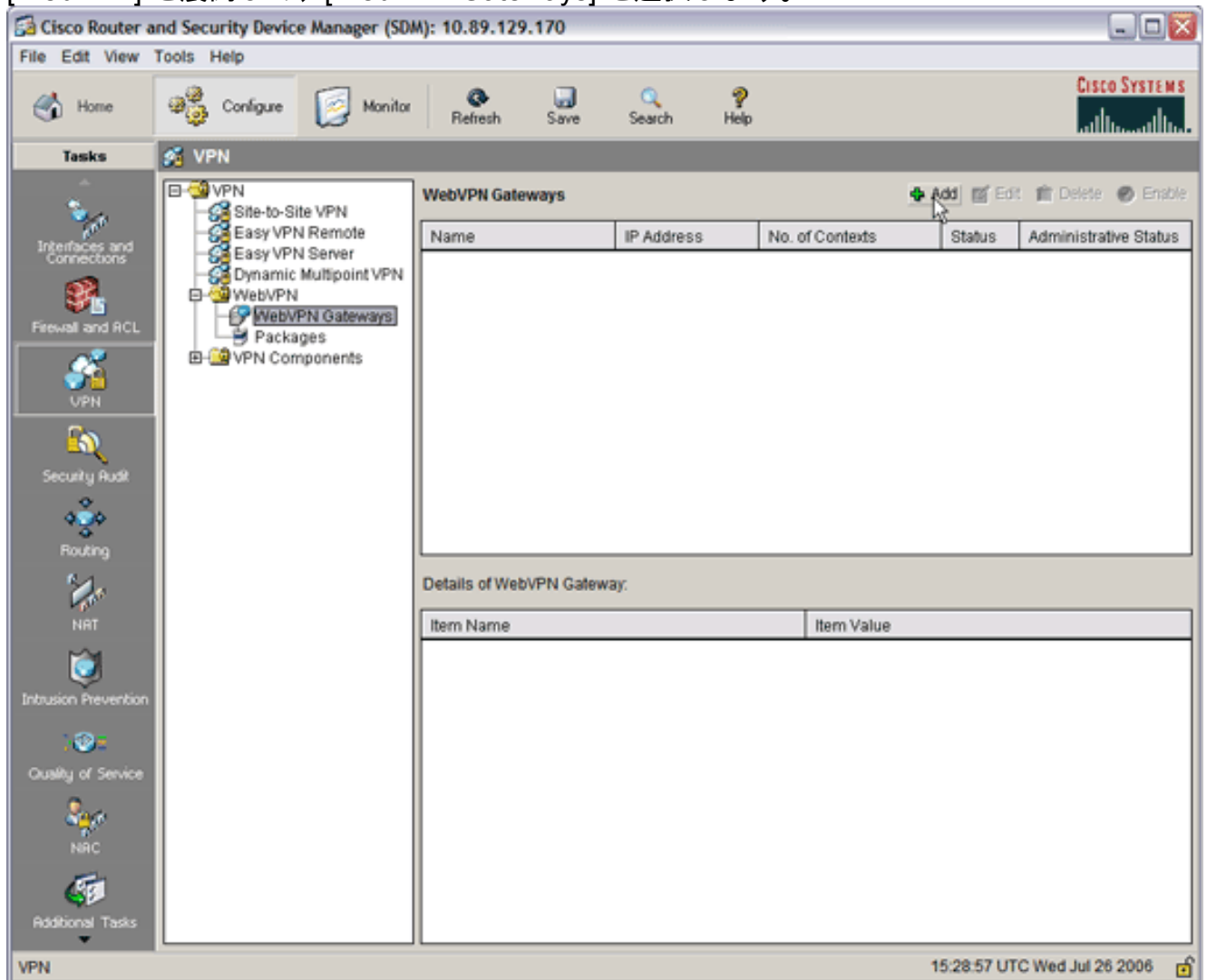
Cisco IOS に WebVPN を設定するには、次の手順を実行します。

1. [WebVPN ゲートウェイの設定](#)
2. [ポリシーグループに対して許可されるリソースを設定する](#)
3. [WebVPN ポリシーグループの設定とリソースの選択](#)
4. [WebVPN コンテキストの設定](#)
5. [ユーザデータベースと認証方法の設定](#)

ステップ 1. WebVPN ゲートウェイの設定

WebVPN ゲートウェイを設定するには、次の手順を実行します。

1. SDM アプリケーションで、[Configure] をクリックし、次に [VPN] をクリックします。
2. [WebVPN] を展開して、[WebVPN Gateways] を選択します。



3. [Add] をクリックします。[Add WebVPN Gateway] ダイアログ ボックスが表示されます。

Add WebVPN Gateway

Gateway Name:

Enable Gateway

IP Address

WebVPN clients will use this IP address and port number to connect to the WebVPN gateway.

IP Address: ▼ Port:

Hostname: (Optional)

Enable secure SDM access through 192.168.0.37

Digital Certificate

Digital Certificate configured under this trustpoint will be sent to the client for SSL authentication.

Trustpoint: ▼

Redirect HTTP Traffic (Optional)

Configure HTTP redirect so that clients accessing the portal page using HTTP will be automatically redirected to the secure HTTPS service that WebVPN uses.

HTTP Port:

OK Cancel Help

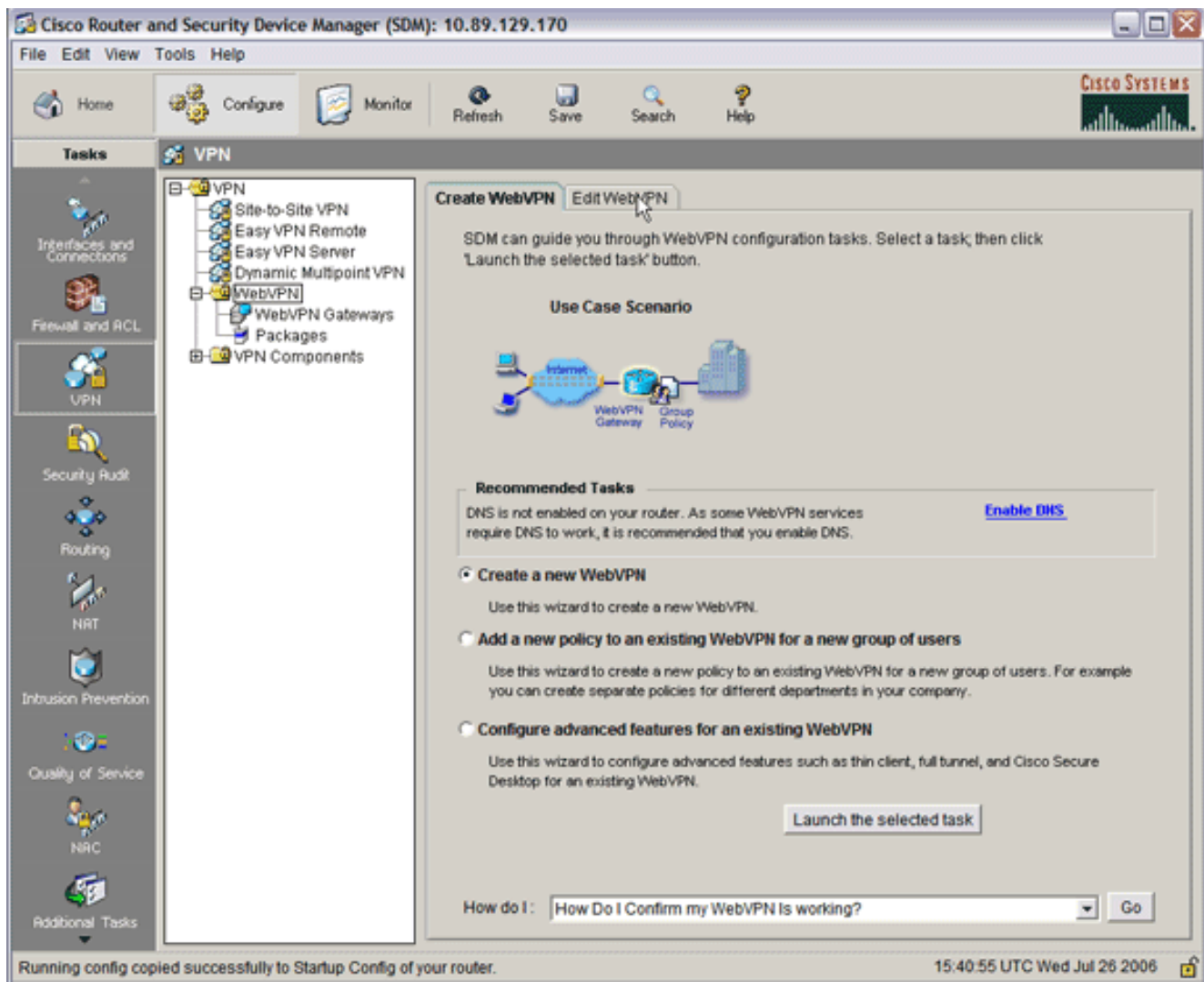
4. [Gateway Name] および [IP Address] フィールドに値を入力し、[Enable Gateway] チェックボックスをオンにします。
5. [Redirect HTTP Traffic] チェックボックスをオンにして、[OK] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

ステップ 2. ポリシーグループに対して許可されるリソースの設定

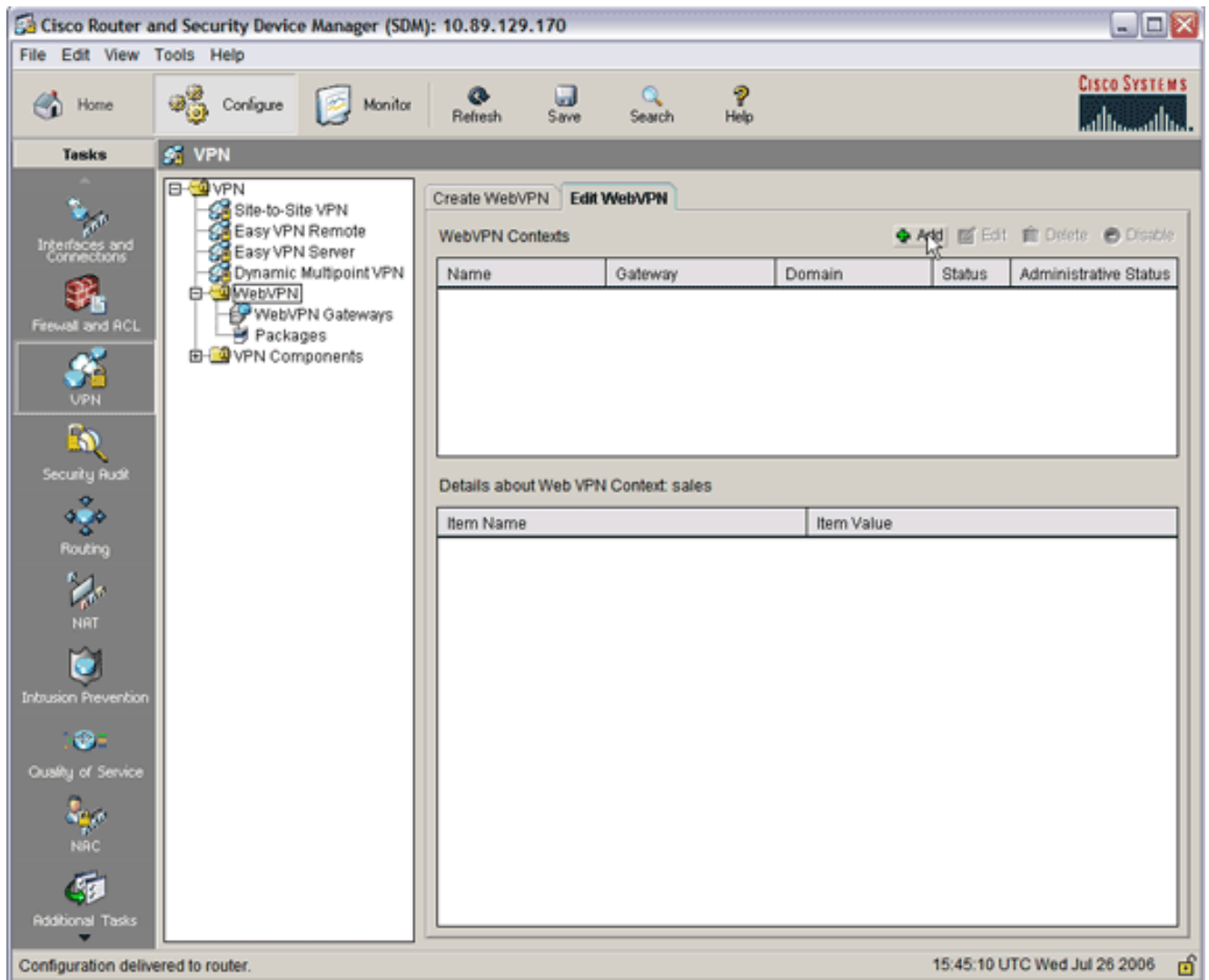
ポリシーグループを作成する前にリソースを設定すれば、ポリシーグループへ簡単にリソースを追加できます。

ポリシーグループに対して許可されるリソースを設定するには、次の手順を実行します。

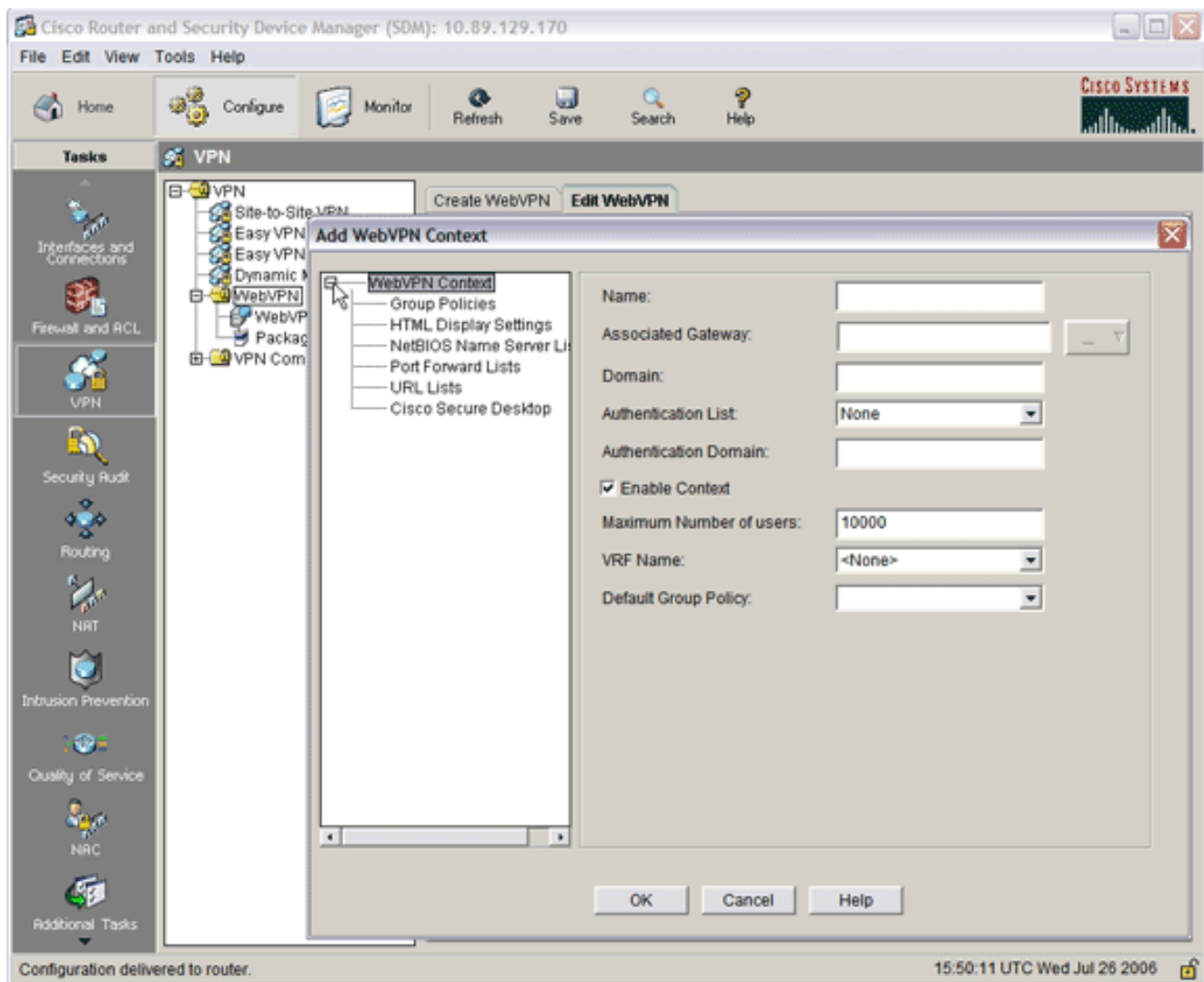
1. [Configure] をクリックし、次に [VPN] をクリックします。



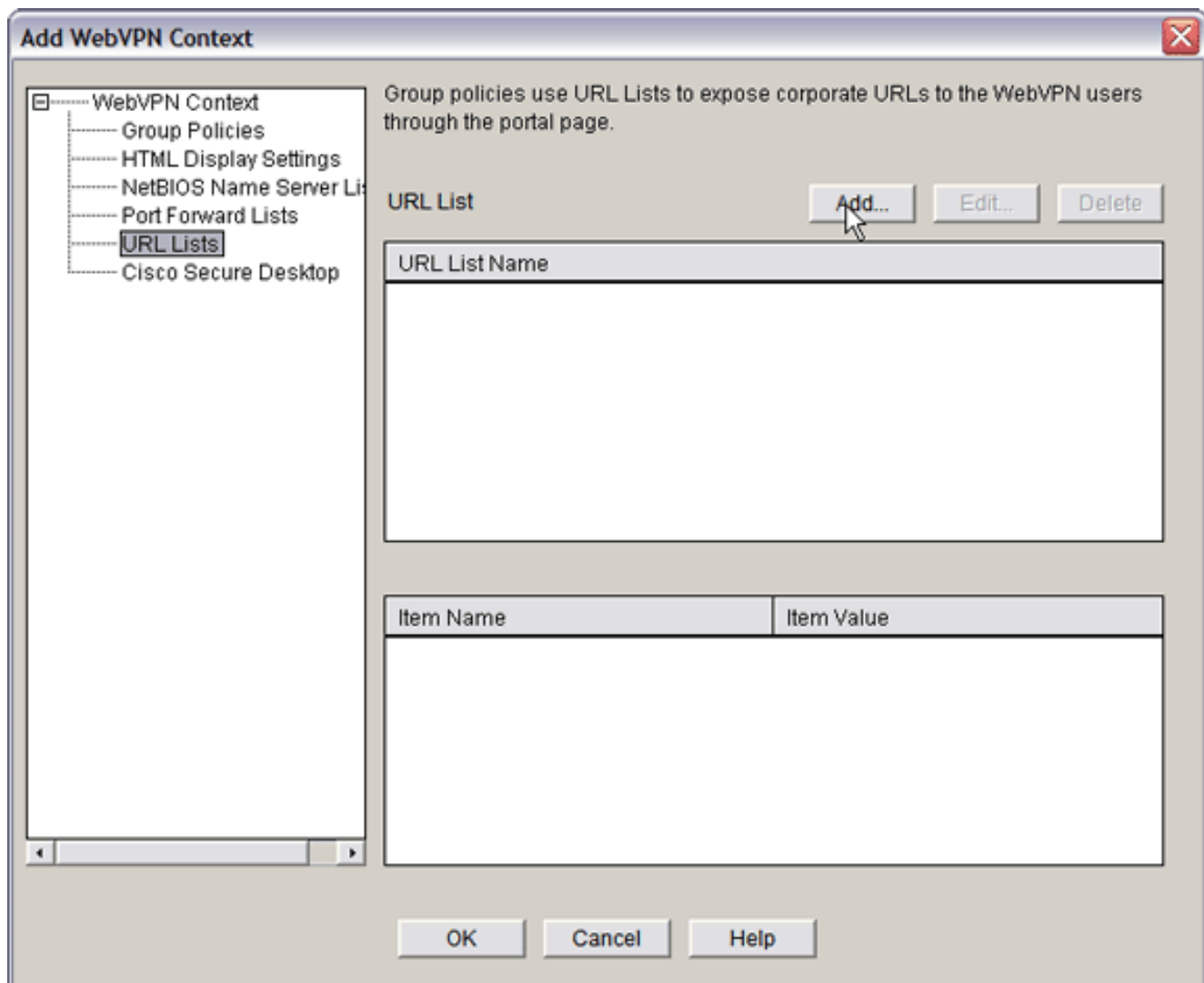
2. WebVPN を選択し、次に編集 WebVPN タブをクリックして下さい。注: WebVPN では、HTTP、HTTPS、Common Internet File System (CIFS) プロトコルによる Windows ファイル ブラウジング、および Citrix のアクセスも設定できます。



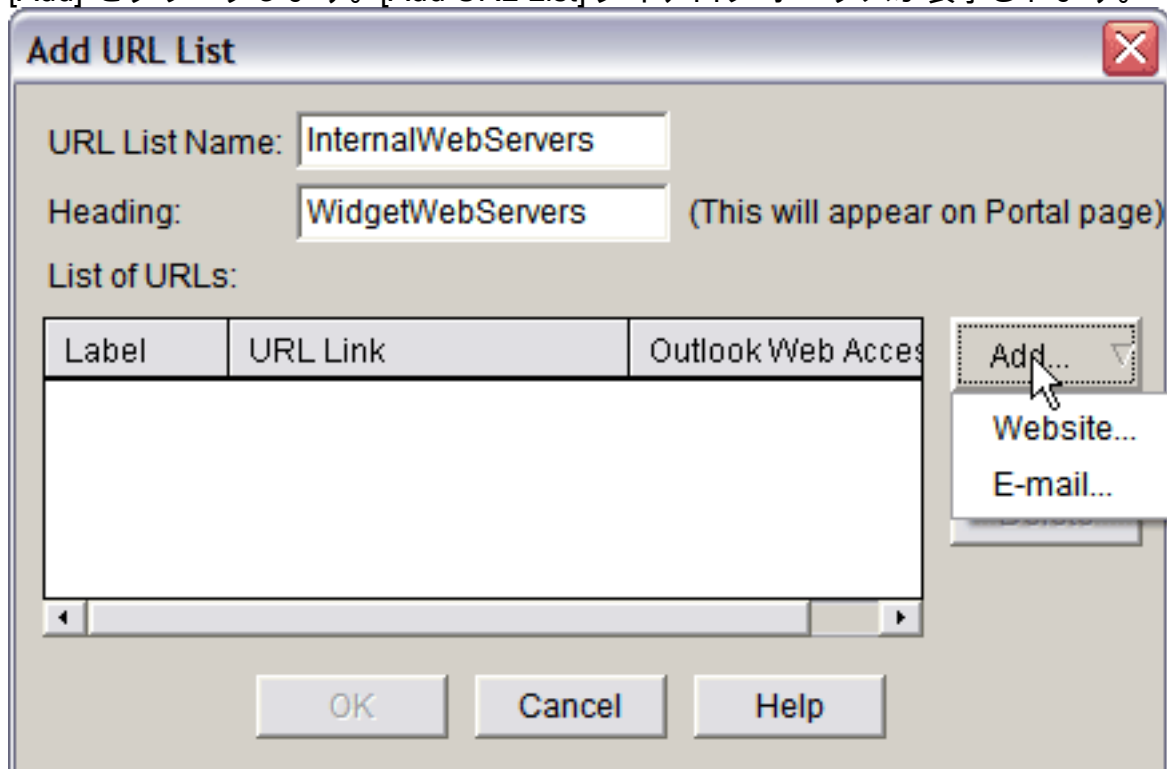
3. [Add] をクリックします。[Add WebVPN Context] ダイアログ ボックスが表示されます。



4. [WebVPN Context] を展開し、[URL Lists] を選択します。



5. [Add] をクリックします。[Add URL List] ダイアログ ボックスが表示されます。



6. [URL List Name] および [Heading] フィールドに値を入力します。

7. [Add] をクリックし、[Website] を選択します。

Add URL List ✖

URL List Name:

Heading: (This will appear on Portal page)

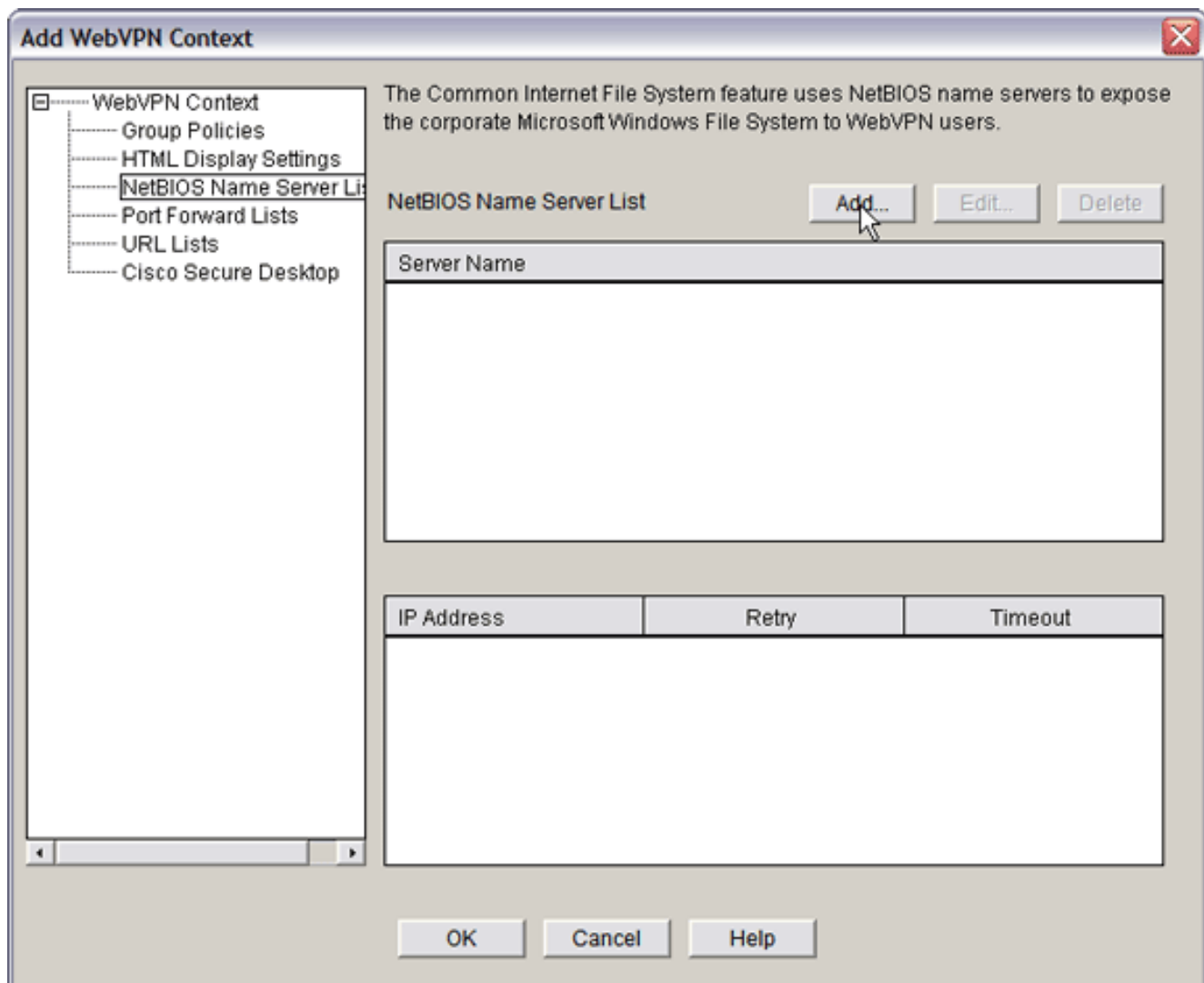
List of URLs:

Label	URL Link	Outlook Web Access
WidgetWeb	http://172.22.1.30	
OWA	http://172.22.1.50/exchang	Enabled

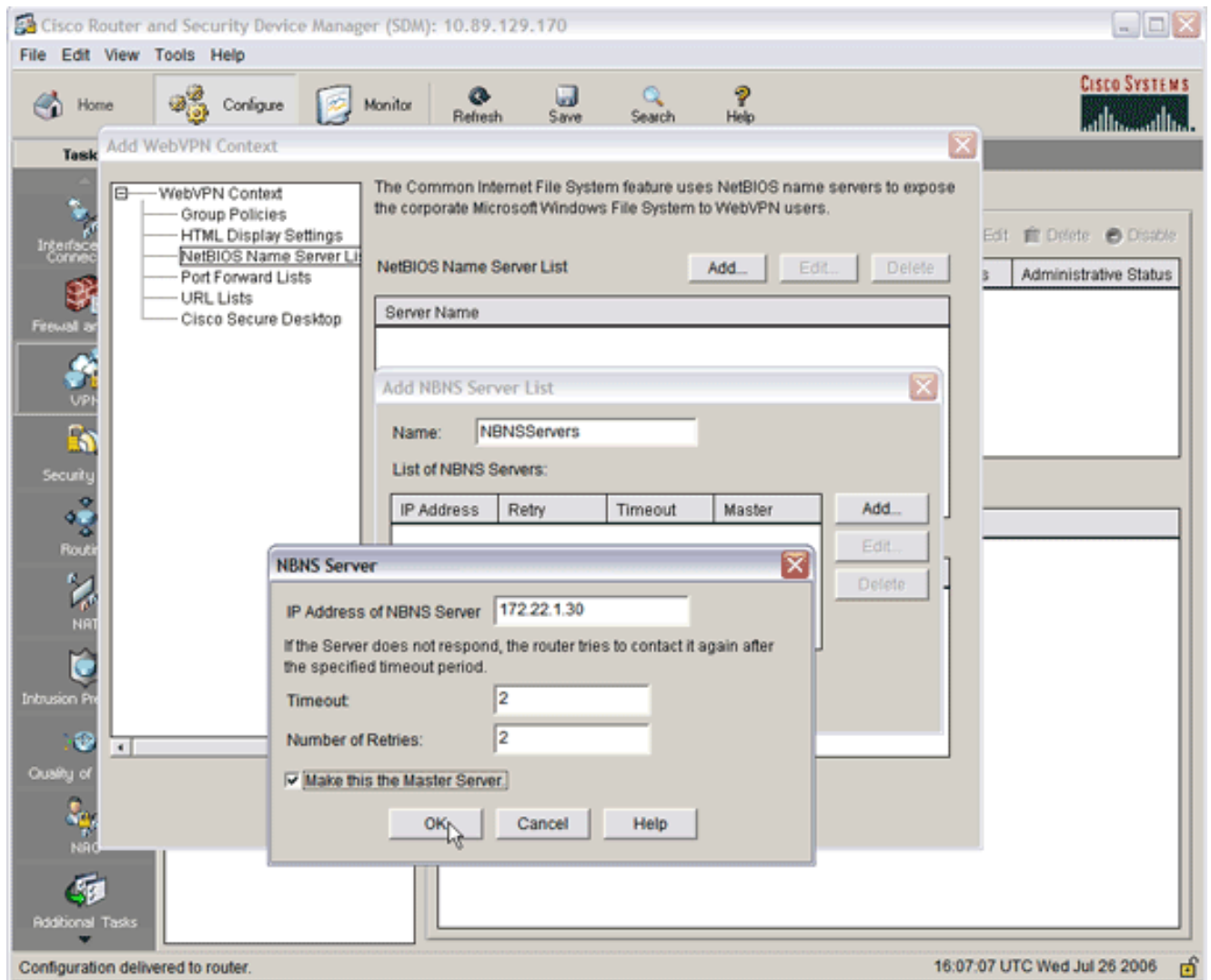
このリス

トには、この WebVPN 接続で利用可能にする、すべての HTTP および HTTPS Web サーバが含まれています。

8. Outlook Web Access (OWA) へのアクセスを追加するには、[Add] をクリックし、[E-mail] を選択して、必要なすべてのフィールドへ入力してから [OK] をクリックします。
9. NetBIOS Name Service (NBNS) サーバを指定し、Windows ドメイン内の共有を順序通りに設定すれば、CIFS による Windows ファイル ブラウジングが可能になります。[WebVPN Context] リストから、[NetBIOS Name Server Lists] を選択します。



[Add] をクリックします。[Add NBNS Server List] ダイアログ ボックスが表示されます。リストの名前を入力し、[Add] をクリックします。[NBNS Server] ダイアログ ボックスが表示されます。

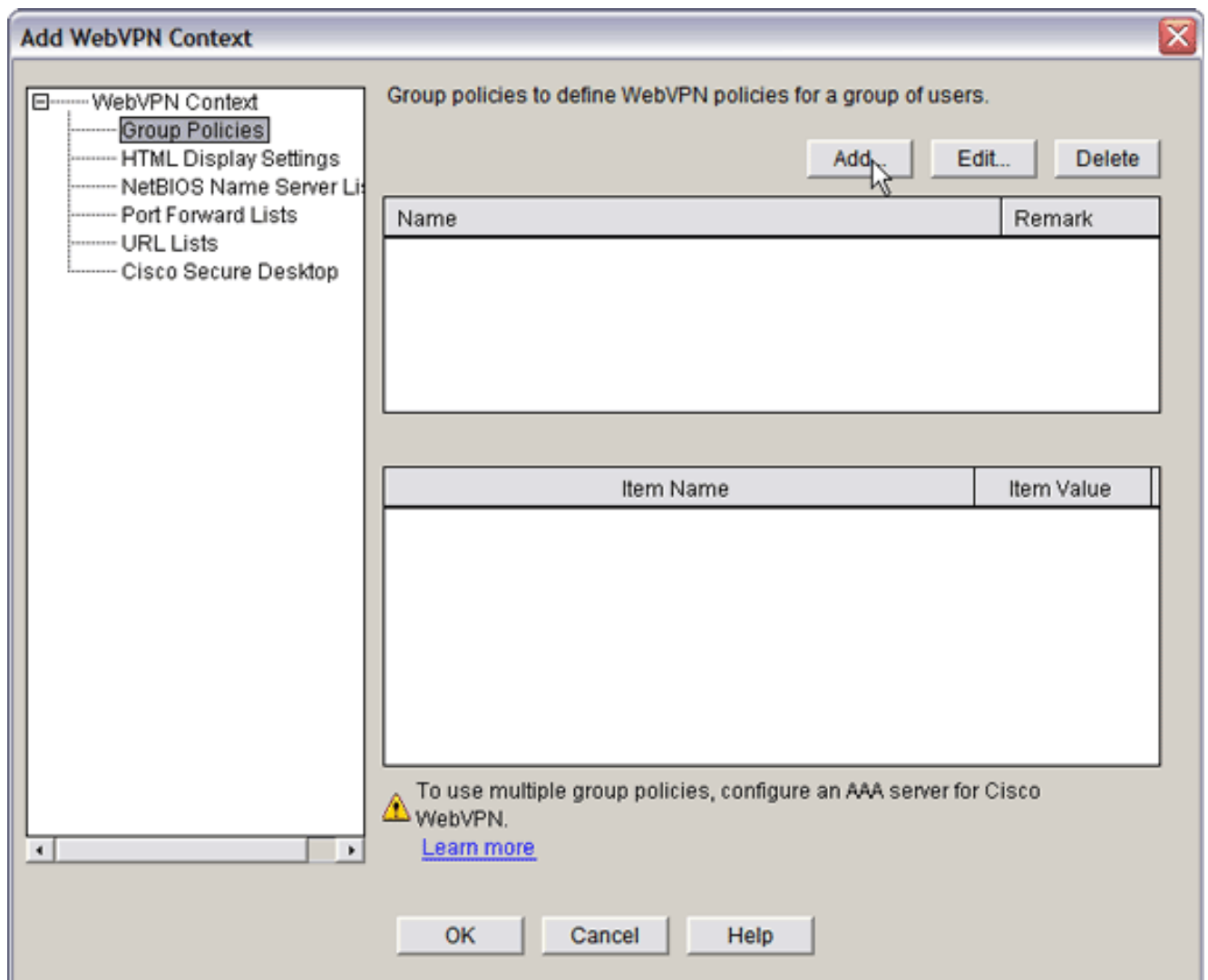


該当する場合、[Make This the Master Server] チェック ボックスをオンにします。[OK] をクリックし、さらに [OK] をクリックします。

[ステップ 3. WebVPN ポリシー グループの設定とリソースの選択](#)

WebVPN ポリシー グループを設定し、リソースを選択するには、次の手順を実行します。

1. [Configure] をクリックし、次に [VPN] をクリックします。
2. [WebVPN] を展開し、[WebVPN Context] を選択します。



3. [Group Policies] を選択し、[Add] をクリックします。[Add Group Policy] ダイアログ ボックスが表示されます。

Add Group Policy

General Clientless Thin Client SSL VPN Client (Full Tunnel)

Name:

Make this the default group policy for context.

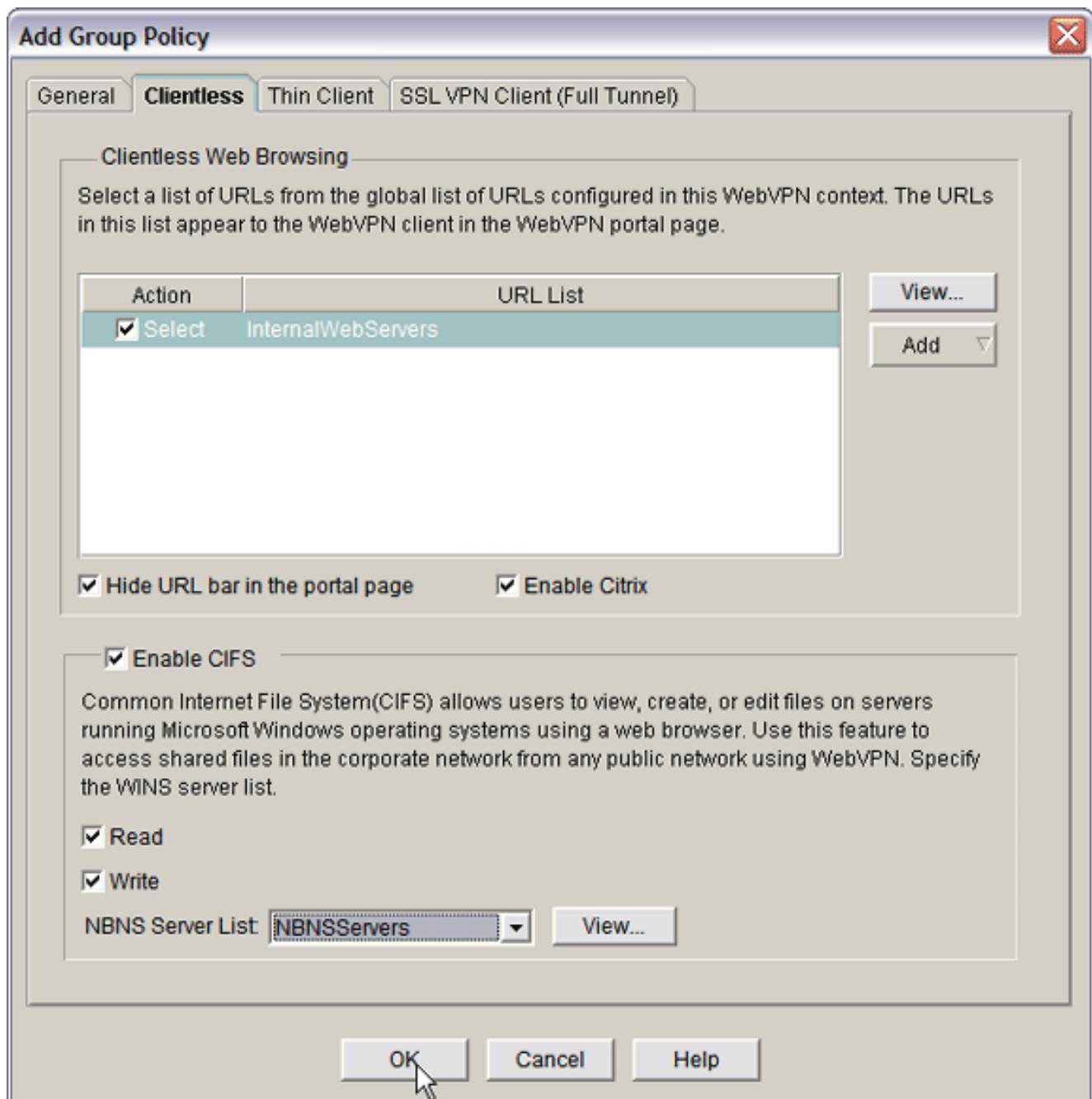
Timeouts

Client's WebVPN session will be disconnected if the client is connected longer than the session timeout or if the client is idle longer than the idle timeout.

Idle Timeout: (sec) Session Timeout: (sec)

OK Cancel Help

4. 新しいポリシーの名前を入力し、**[Make this the default group policy for context]** チェックボックスにチェックマークを入れます。
5. ダイアログボックスの上にある **[Clientless]** タブをクリックします。

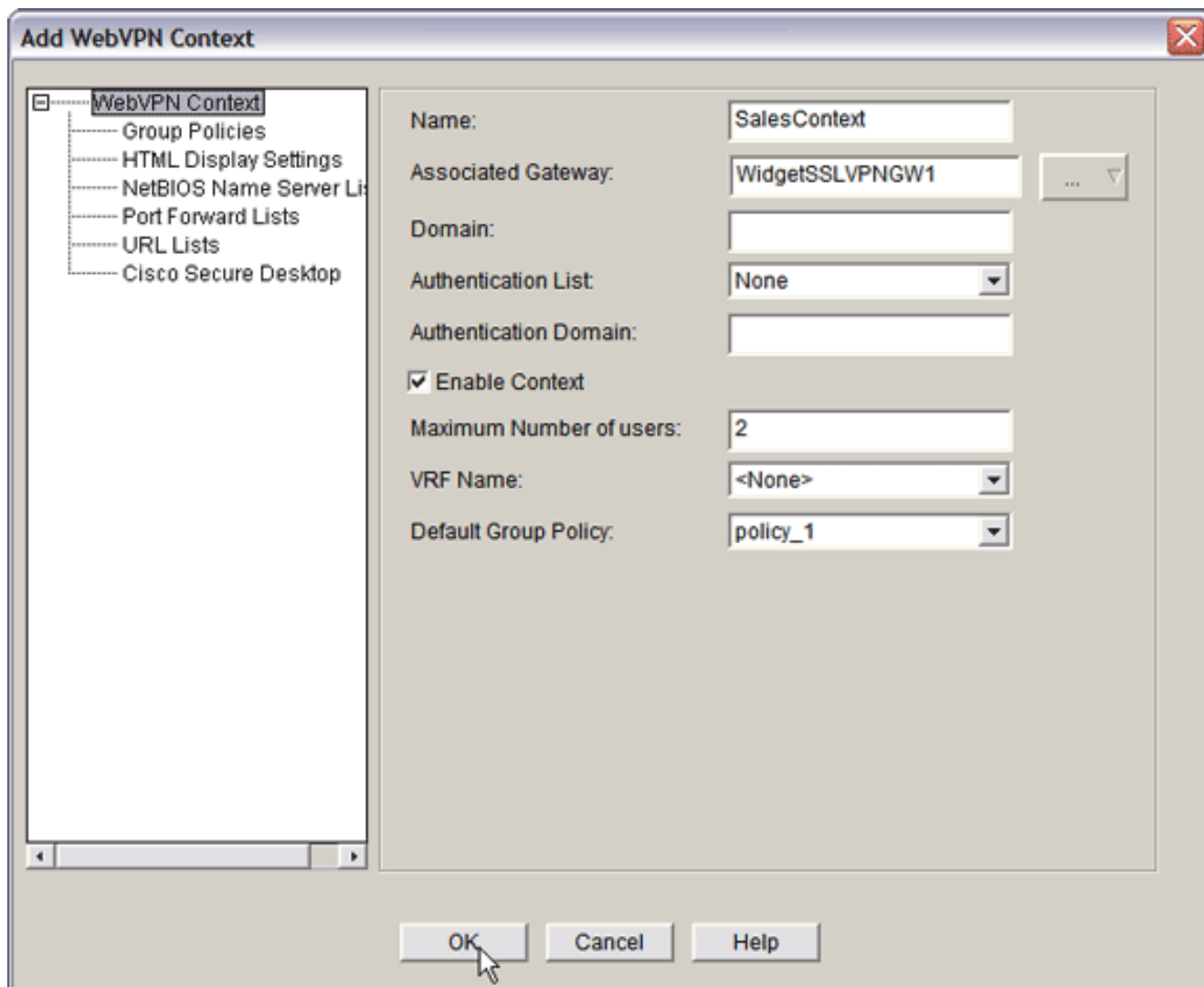


6. 選択する URL リストの [Select] チェック ボックスにチェックマークを付けます。
7. お客様が Citrix クライアントを使用するため、Citrix サーバへのアクセスが必要な場合は、[Enable Citrix] チェック ボックスをオンにします。
8. [Enable CIFS]、[Read]、および [Write] チェック ボックスをオンにします。
9. [NBNS Server List] ドロップダウンの矢印をクリックして、[ステップ 2](#) で Windows ファイル ブラウジング用に作成した NBNS サーバ リストを選択します。
10. [OK] をクリックします。

[ステップ 4. WebVPN コンテキストの設定](#)

WebVPN ゲートウェイ、グループ ポリシー、およびリソースをリンクさせるには、WebVPN コンテキストを設定する必要があります。WebVPN コンテキストを設定するには、次の手順を実行します。

1. [WebVPN Context] を選択し、コンテキストの名前を入力します。



2. [Associated Gateway] ドロップダウンの矢印をクリックして、関連付けられているゲートウェイを選択します。
3. 複数のコンテキストを作成する場合は、このコンテキストを識別する一意の名前を [Domain] フィールドに入力します。 [Domain] フィールドを空欄にすると、ユーザは **https://IPAddress** で WebVPN にアクセスすることになります。ドメイン名 (たとえば、Sales) を入力すると、ユーザは **https://IPAddress/Sales** で接続することになります。
4. [Enable Context] チェック ボックスをオンにします。
5. [Maximum Number of Users] フィールドで、デバイスのライセンスで許可されている最大のユーザ数を入力します。
6. [Default Group policy] ドロップダウンの矢印をクリックし、グループ ポリシーを選択してこのコンテキストに関連付けます。
7. [OK] をクリックし、さらに [OK] をクリックします。

ステップ 5. ユーザ データベースと認証方法の設定

Radius、Cisco AAA サーバ、またはローカル データベースで認証を行うように、クライアントレス SSL VPN (WebVPN) セッションを設定できます。次の例では、ローカル データベースを使用します。

ユーザ データベースと認証方法を設定するには、次の手順を実行します。

1. [Configuration] をクリックし、[Additional Tasks] をクリックします。
2. [Router Access] を展開し、[User Accounts/View] を選択します。

Cisco Router and Security Device Manager (SDM): 10.89.129.170

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks Additional Tasks

Router Properties
Router Access
User Accounts View
VTY
Management Access
SSH
Secure Device Provisioning
DHCP
DNS
Dynamic DNS Methods
ACL Editor
Port to Application Mappings
URL Filtering
AAA
Local Pools
Router Provisioning
Configuration Management

User Accounts View

Username	Password	Privilege Level	View Name
admin	*****	15	<None>
austin	*****	15	<None>
ausnml	*****	15	<None>
fallback	*****	15	<None>

Add... Edit... Delete

Additional Tasks 17:12:15 UTC Wed Jul 26 2006

3. [Add] ボタンをクリックします。[Add an Account] ダイアログ ボックスが表示されます。

Add an Account

Enter the username and password

Username:

Password:

New Password:

Confirm New Password:

Encrypt password using MD5 hash algorithm

Privilege Level:

Associate a View with the user

View Name:

4. ユーザアカウントとパスワードを入力します。
5. [OK] をクリックし、さらに [OK] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

結果

ASDM は次のコマンドライン設定を作成します。

```
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 enrollmnet  
selfsigned serial-number none ip-address none  
revocation-check crl rsaкеypair 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  
2E56CDDF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C  
FOA14383 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$3xFv$W0YUsKDxladDc.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
```

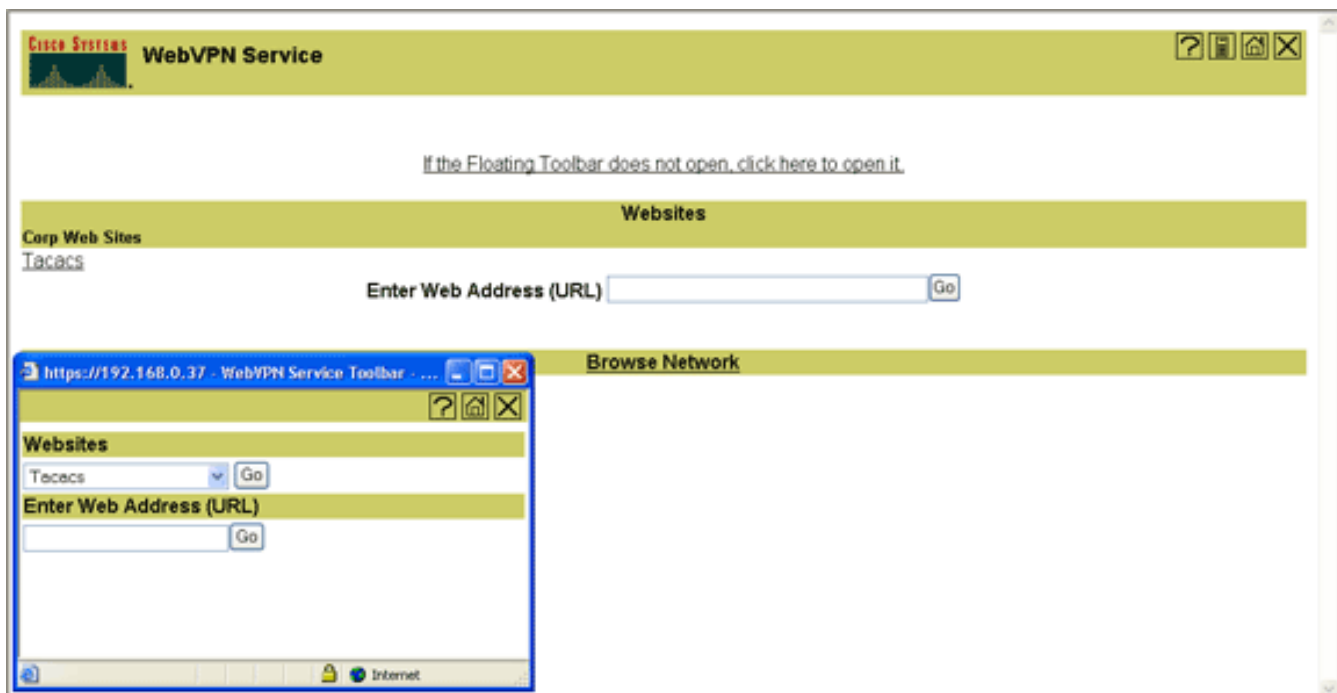
確認

ここでは、設定が正常に動作していることを確認します。

手順

設定が正常に動作していることを確認するには、次の手順を実行します。

- ユーザを使用して設定をテストします。SSL 対応 Web ブラウザに、**https://WebVPN_Gateway_IP_Address** と入力します。この場合、**WebVPN_Gateway_IP_Address** は WebVPN サービスの IP アドレスです。証明書を承認してユーザ名とパスワードを入力すると、次のイメージのようなイメージが表示されます。



- SSL VPN セッションをチェックします。SDM アプリケーションで、[Monitor] ボタンをクリックし、次に [VPN Status] をクリックします。[WebVPN (All Contexts)] を展開し、適切なコンテキストを展開して、[Users] を選択します。
- エラーメッセージを確認します。SDM アプリケーションで、[Monitor] ボタンをクリックし、[Logging] をクリックして、次に [Syslog] タブをクリックします。
- デバイスの実行コンフィギュレーションを表示します。SDM アプリケーションで [Configure] ボタンをクリックし、[Additional Tasks] をクリックします。[Configuration Management] を展開し、[Config Editor] を選択します。

コマンド

いくつかの **show** コマンドは WebVPN に関連しています。これらのコマンドをコマンドライン インターフェイス (CLI) で実行して、統計情報や他の情報を表示できます。show コマンドの詳細は、『[WebVPN 設定の確認](#)』を参照してください。

注: [Output Interpreter Tool](#) (OIT) ([登録](#) ユーザ専用) では、特定の show コマンドがサポートされています。OIT を使用して、show コマンド出力の解析を表示できます。

トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

注: コピー処理が行われている間は、**Copy File to Server** コマンドを中断したり、別のウィンドウに移動しないでください。操作を中断すると、不完全なファイルがサーバに保存される可能性があります。

注: ユーザは WebVPN クライアントを使用して新しいファイルをアップロードしたり、ダウンロードしたりすることができますが、**Copy File to Server** コマンドを使用して、WebVPN の Common Internet File System (CIFS) のファイルを上書きすることはできません。ユーザがサーバ上のファイルを置き換えようとする、次のメッセージが表示されます。

Unable to add the file

手順

設定をトラブルシューティングするには、次の手順を実行します。

1. クライアントでポップアップ ブロッカーが無効になっていることを確認します。
2. クライアントで cookie が有効になっていることを確認します。
3. クライアントで Netscape、Internet Explorer、Firefox、または Mozilla ブラウザが使用されていることを確認します。

コマンド

いくつかの debug コマンドは、WebVPN に関連しています。これらのコマンドの詳細については、『[WebVPN の Debug コマンドの使用](#)』を参照してください。

注: debug コマンドを使用すると、Cisco デバイスに悪影響が及ぶ可能性があります。debug コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

関連情報

- [Cisco IOS SSLVPN](#)
- [Cisco IOS SSLVPN Q&A](#)
- [SDM によるシンクライアント SSL VPN \(WebVPN \) の IOS 設定例](#)
- [SDM を使用した IOS での SSL VPN Client \(SVC \) の設定例](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)