ASDM および NTLMv1 を使用した WebVPN およびシングル サインオン機能付き ASA の設定例

目次

概要

このドキュメントでは、NT LAN Manager バージョン 1（NTLMv1）を稼働している Windows Active Directory に対する追加のログイン検証を必要とするサーバの場合に、WebVPN ユーザ ログイン クレデンシャルおよび第 2 の認証を自動的に渡すように、Cisco 適応型セキュリティ アプライアンス（ASA）を設定する方法を説明します。 この機能はシングル サインオン（SSO）と呼ばれています。 この機能により、特定の WebVPN グループに対して設定されたリンクでは、このユーザ認証情報を渡せるようになります。その結果、認証のプロンプトを複数回出さないで済みます。 この機能は、グローバル設定レベルおよびユーザ設定レベルでも使用できます。

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。

- NTLMv1 およびターゲット VPN ユーザの Windows 権限が設定されていることを確認します。 Windows ドメインのアクセス権限の詳細については、Microsoft のドキュメントを参照してください。

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 ASA 7.1(1)
- Cisco Adaptive Security Device Manager（ASDM）5.1(2)
- Microsoft Internet Information Services（IIS）

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。

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

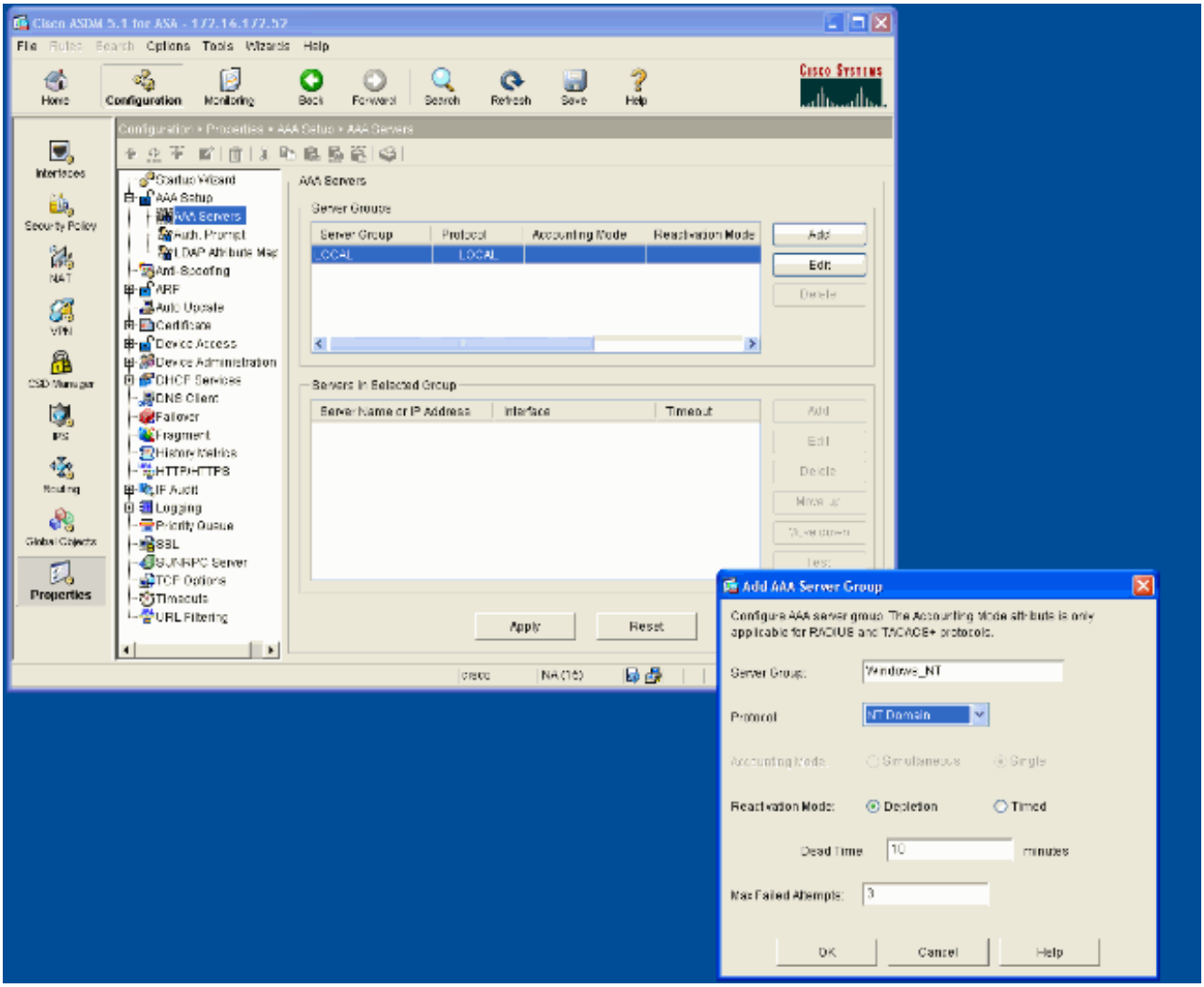
このセクションでは、SSO を利用する WebVPN サーバとしての ASA の設定について説明しています。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

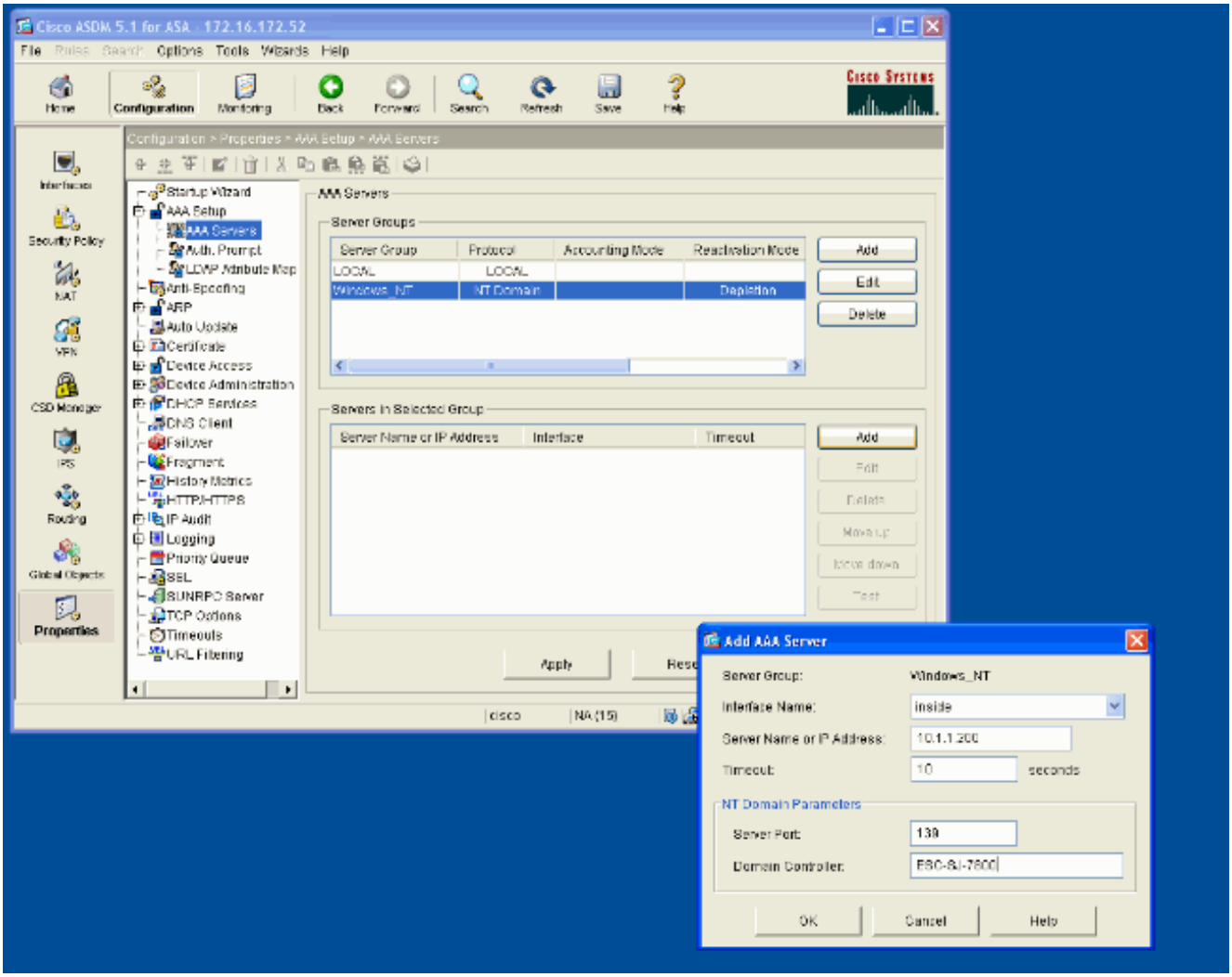
Windows ドメイン認証用 AAA サーバの追加

ドメイン コントローラを使用して認証するように ASA を設定するには、次の手順を実行します。

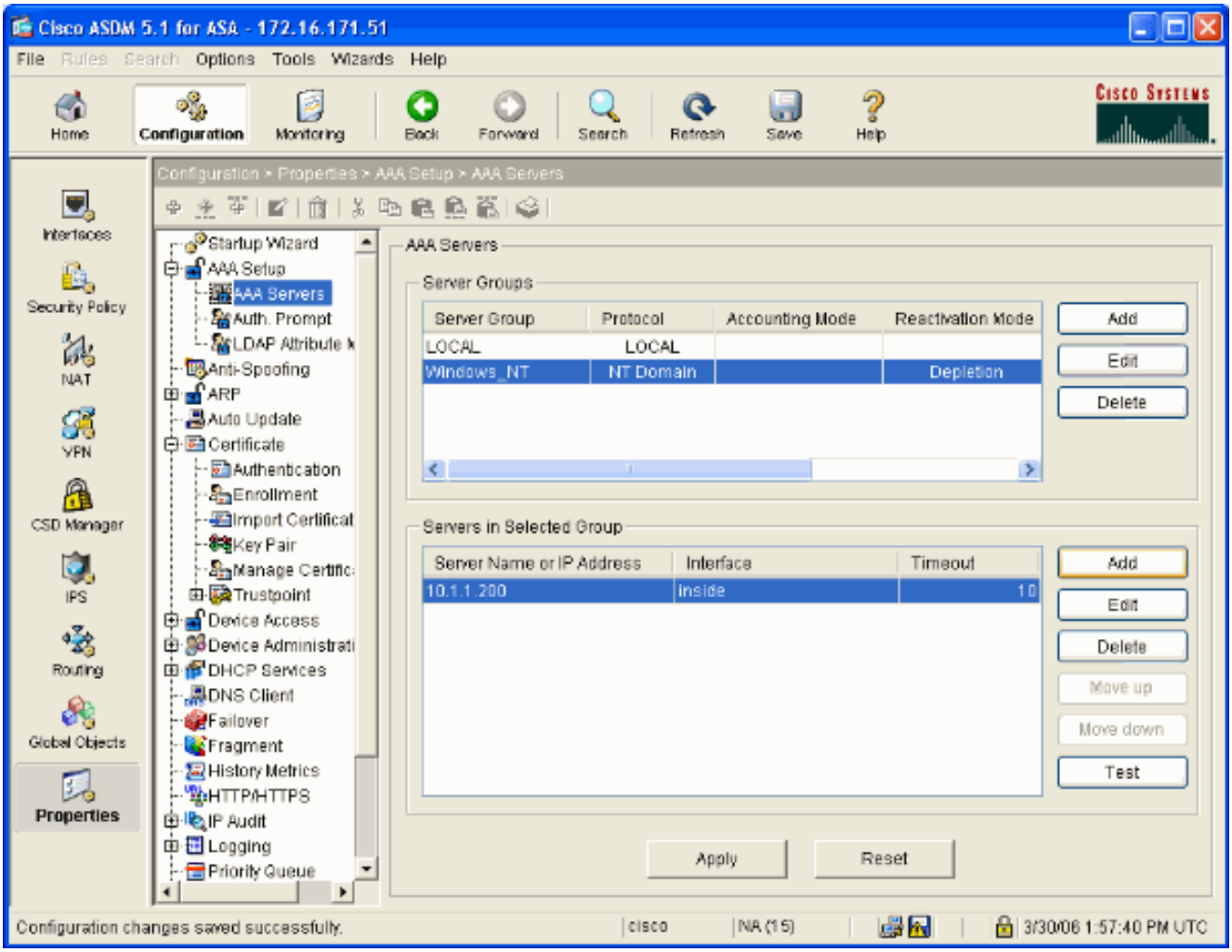
1. [Configuration] > [Properties] > [AAA Setup] > [AAA Servers] を選択し、[Add] をクリックします。 Windows_NT など、サーバ グループの名前を指定し、プロトコルとして [NT Domain] を選択します。



2. Windows サーバを追加します。新しく作成したグループを選択し、[Add] をクリックします。 サーバが配置されているインターフェイスを選択し、IP アドレスおよびドメイン コントローラ名を入力します。 ドメイン コントローラ名は、必ずすべて大文字で入力してください。 完了したら、[OK] をクリックします。



次のウィンドウは、完成した AAA の設定を示します。

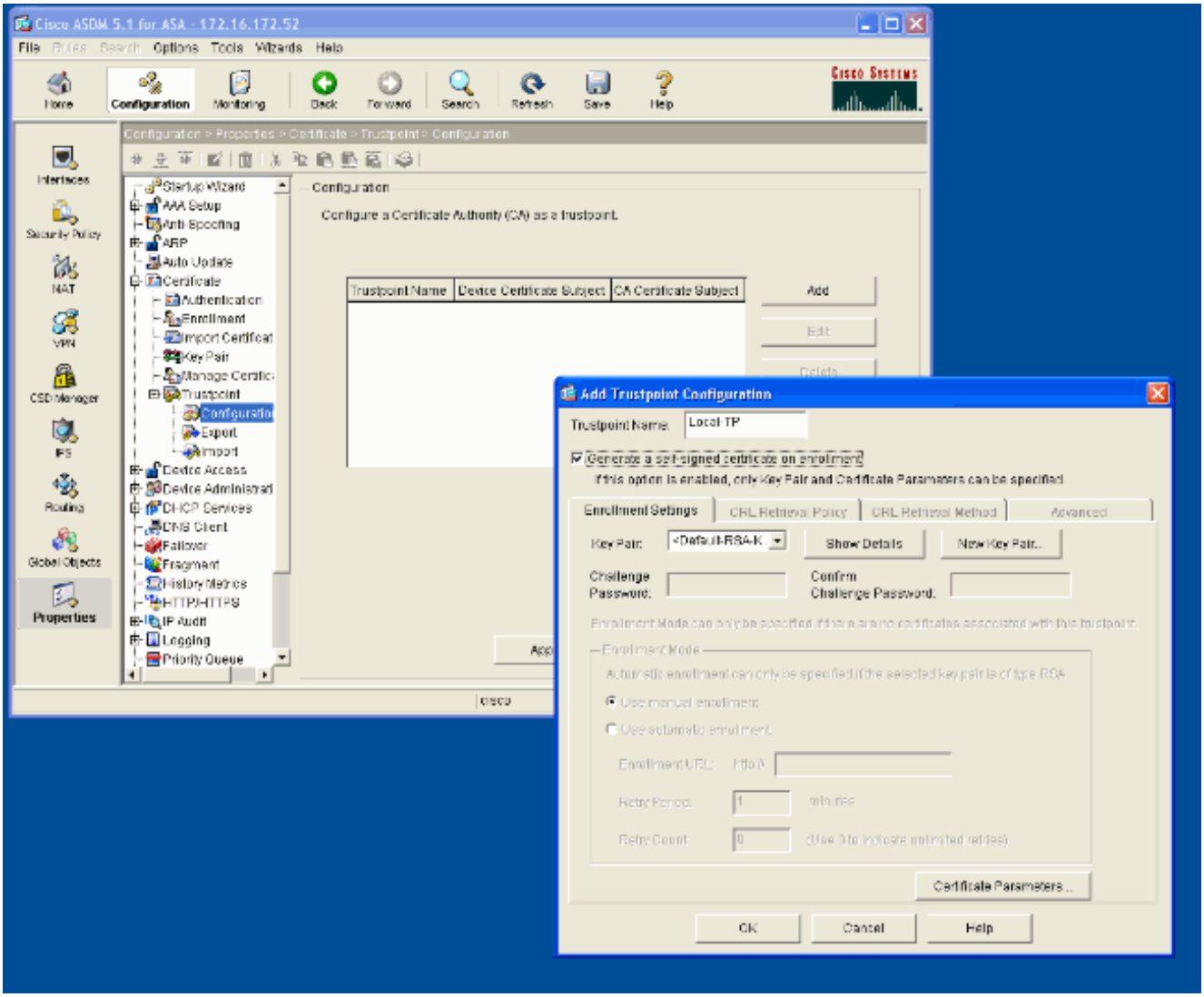


自己署名証明書の作成

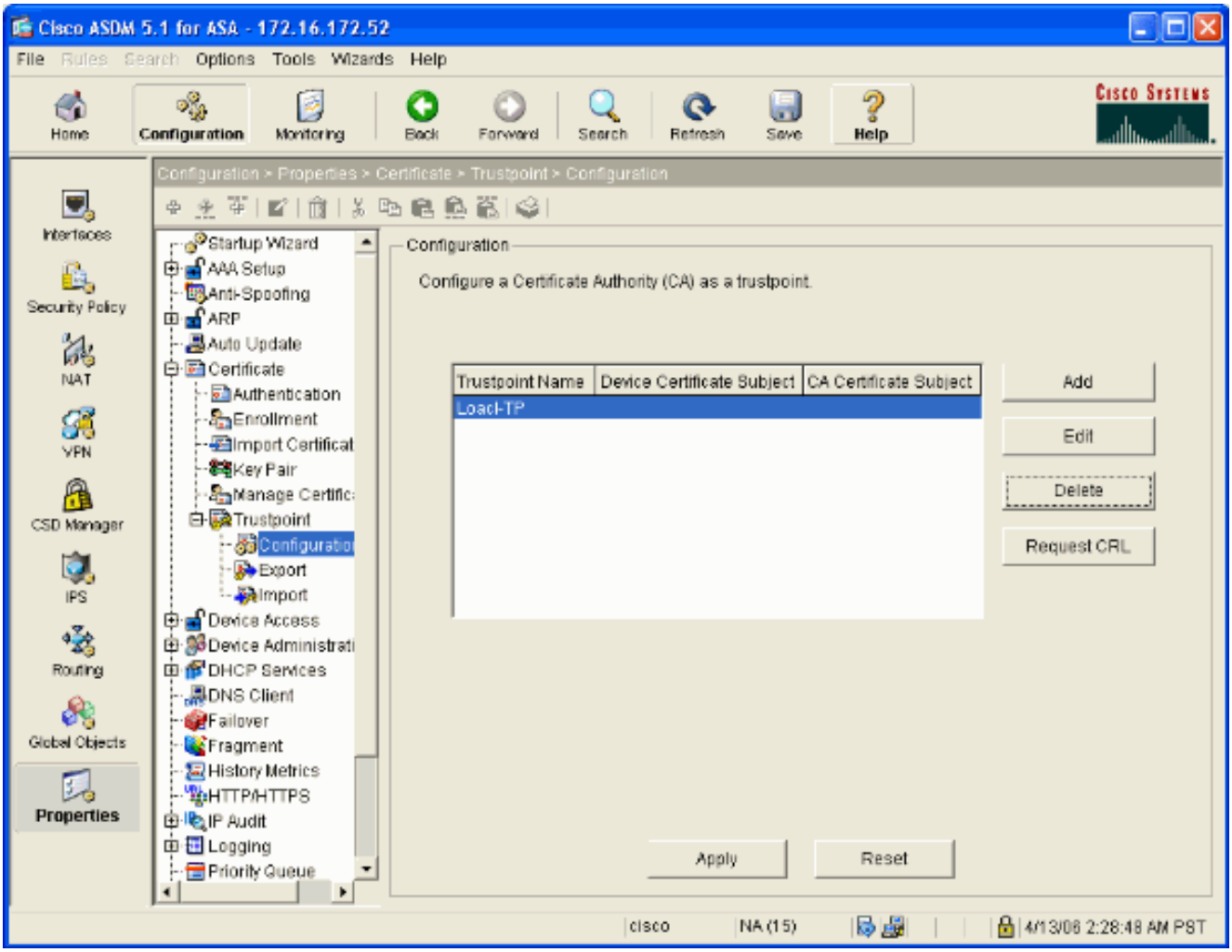
自己署名証明書を使用するように ASA を設定するために、次の手順を実行します。

注: この例では、単純化するために自己署名証明書を使用しています。 外部認証局への登録など、他の証明書登録オプションについては、『証明書の設定』を参照してください。

1. [Configuration] > [Properties] > [Certificate] > [Trustpoint] > [Configuration] を選択し、[Add] をクリックします。
2. 表示されるウィンドウで、トラストポイント名（Local-TP など）を入力し、[Generate a self-signed certificate on enrollment] をオンにします。 他のオプションは、デフォルト設定のままでかまいません。 完了したら、[OK] をクリックします。



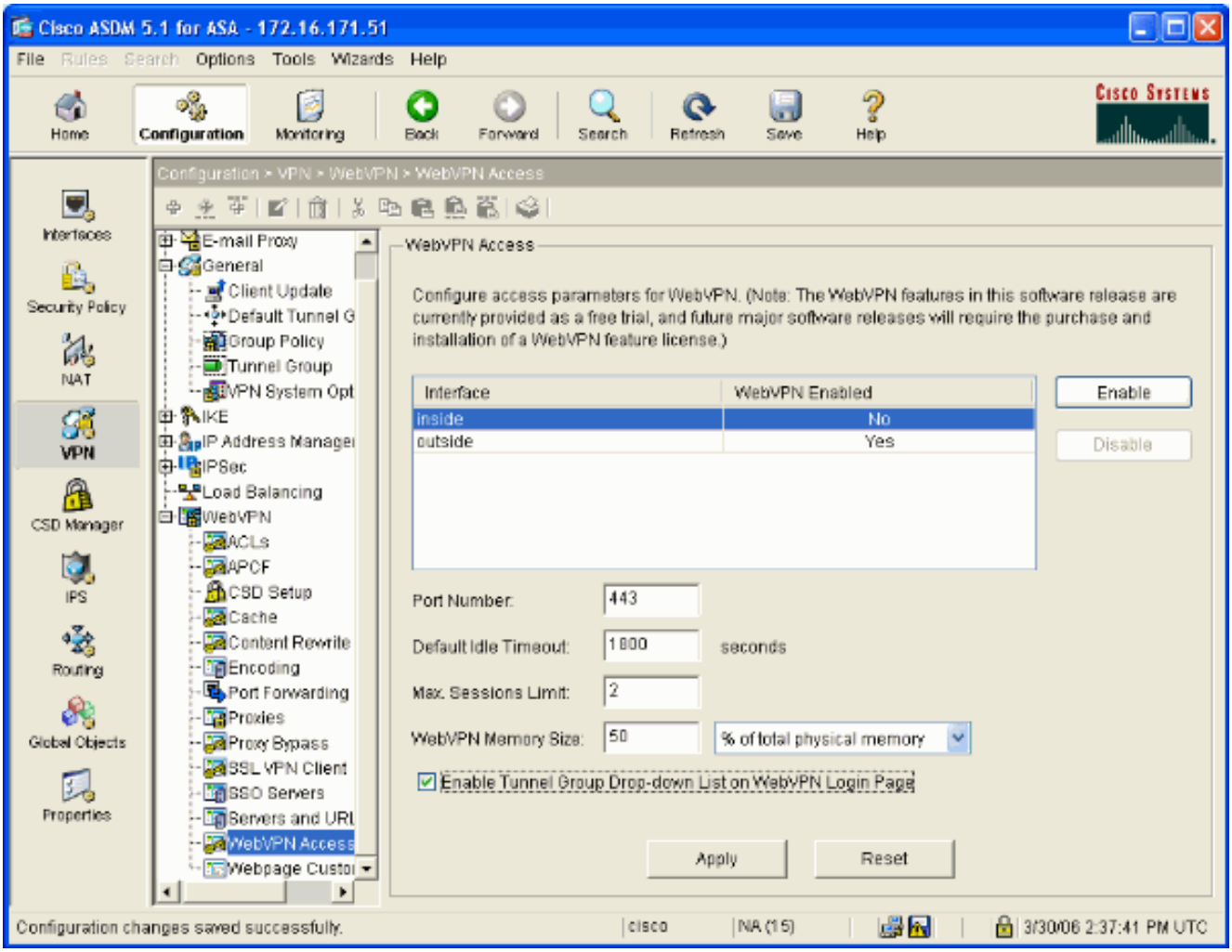
次のウィンドウは、完成したトラストポイント設定を示します。



外部インターフェイスで WebVPN をイネーブルにする。

ネットワークの外部のユーザに、WebVPN を使用した接続を許可するには、次の手順を実行します。

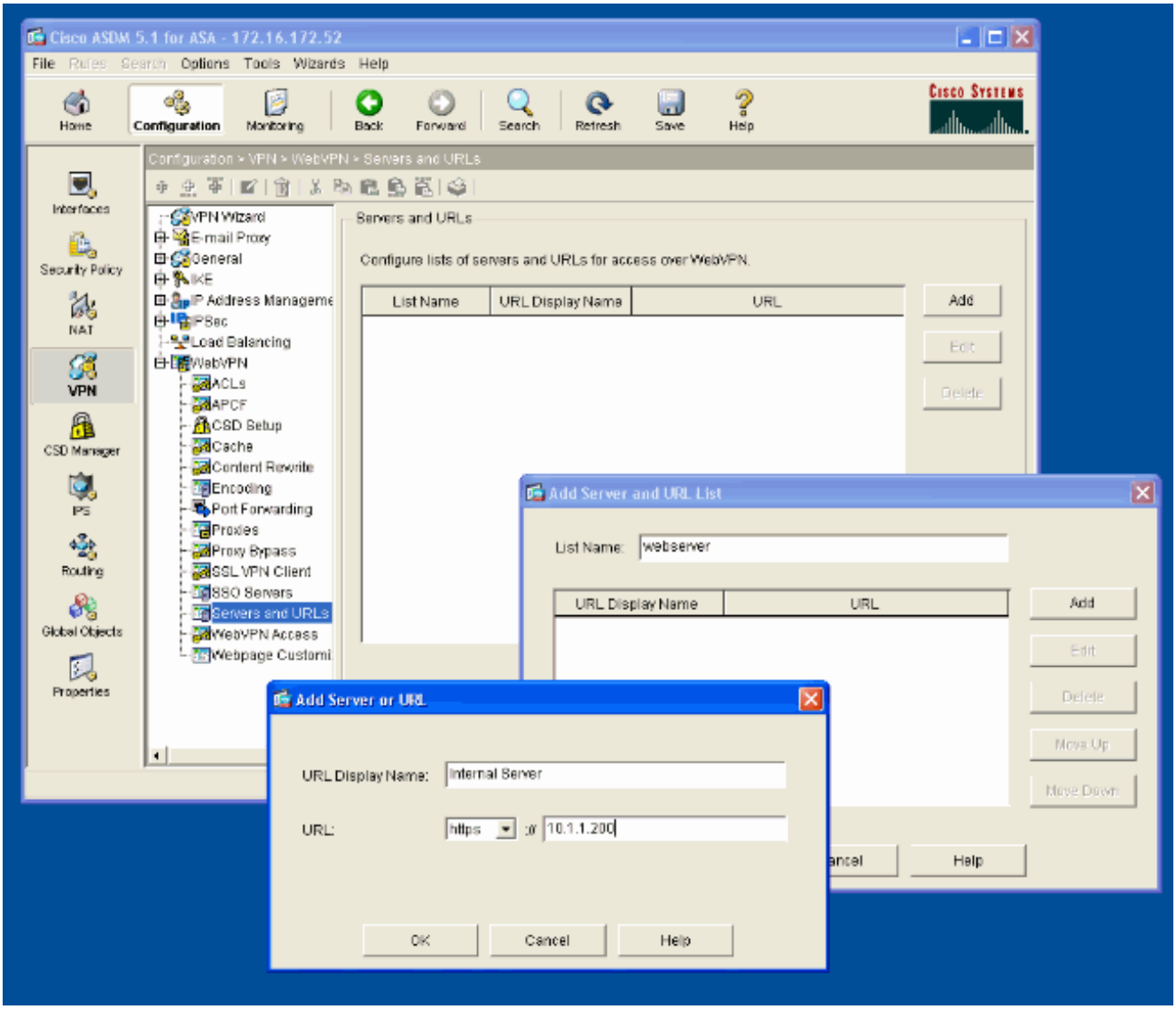
1. [Configuration] > [VPN] > [WebVPN] > [WebVPN Access] を選択します。
2. 必要なインターフェイスを選択してから、[Enable] をクリックし、[Enable Tunnel Group Drop-down List on WebVPN Login Page] をオンにします。**注:** WebVPN と ASDM アクセスに同じインターフェイスを使用するには、ASDM アクセスのデフォルト ポートを、ポート 80 から 8080 などの新しいポートに変更する必要があります。 この操作は、[Configuration] > [Properties] > [Device Access] > [HTTPS/ASDM] で実行します。**注:** ユーザが **https://<ip_address>** ではなく **http://<ip_address>** に移動した場合は、ユーザをポート 443 に自動的にリダイレクトできます。 [Configuration] > [Properties] > [HTTP/HTTPS] を選択し、必要なインターフェイスを選択してから、[Edit] をクリックし、[Redirect HTTP to HTTPS] を選択します。



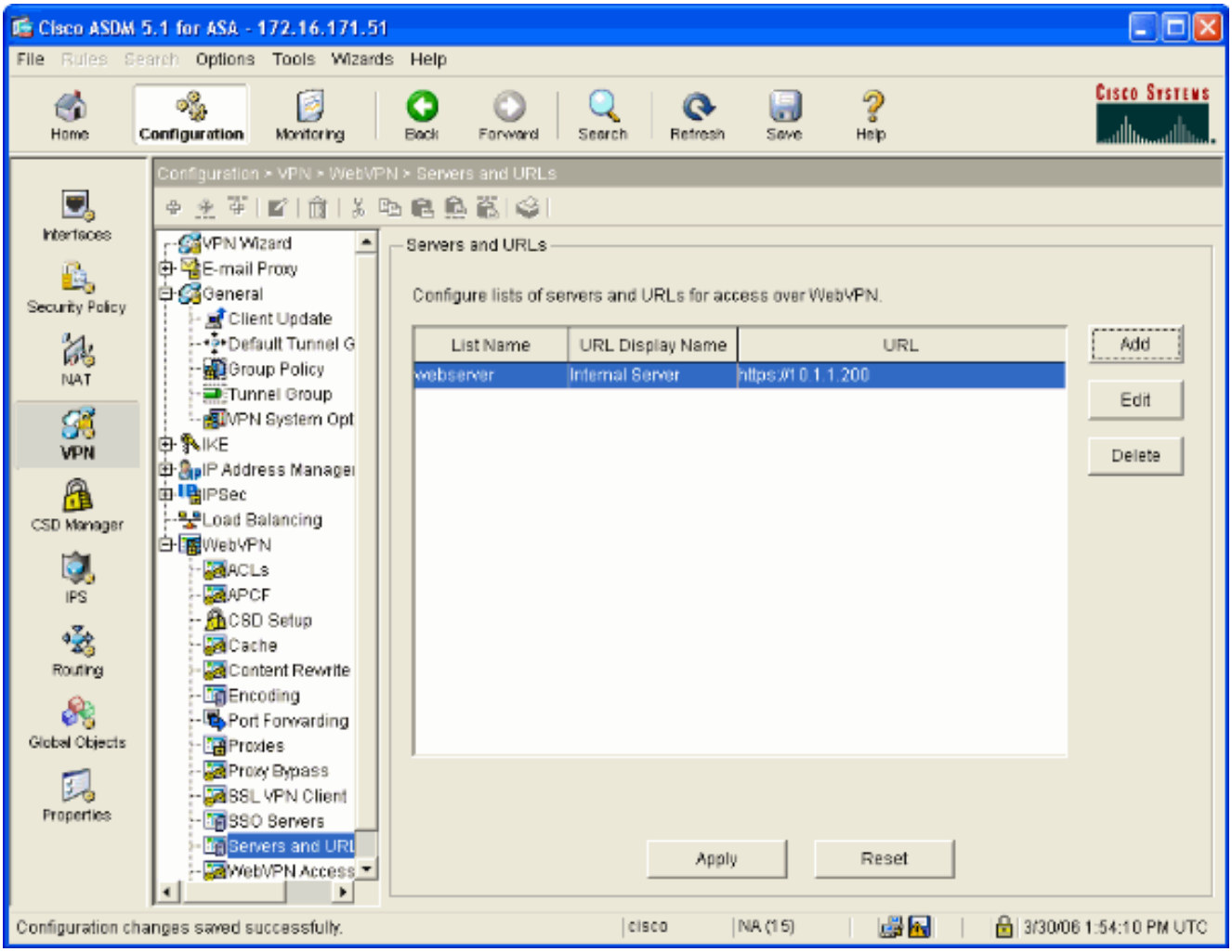
内部サーバ用 URL リストの設定

WebVPN ユーザ アクセス権を付与するサーバを格納したリストを作成するために、次の手順を実行します。

1. [Configuration] > [VPN] > [WebVPN] > [Servers and URLs] を選択し、[Add] をクリックします。
2. URL リストの名前を入力します。 この名前は、エンド ユーザに表示されません。 [Add] をクリックします。
3. これがユーザに表示される名前であるため、[URL Display Name] を入力します。 サーバの URL 情報を入力します。 これは、サーバに通常アクセスする方法である必要があります。



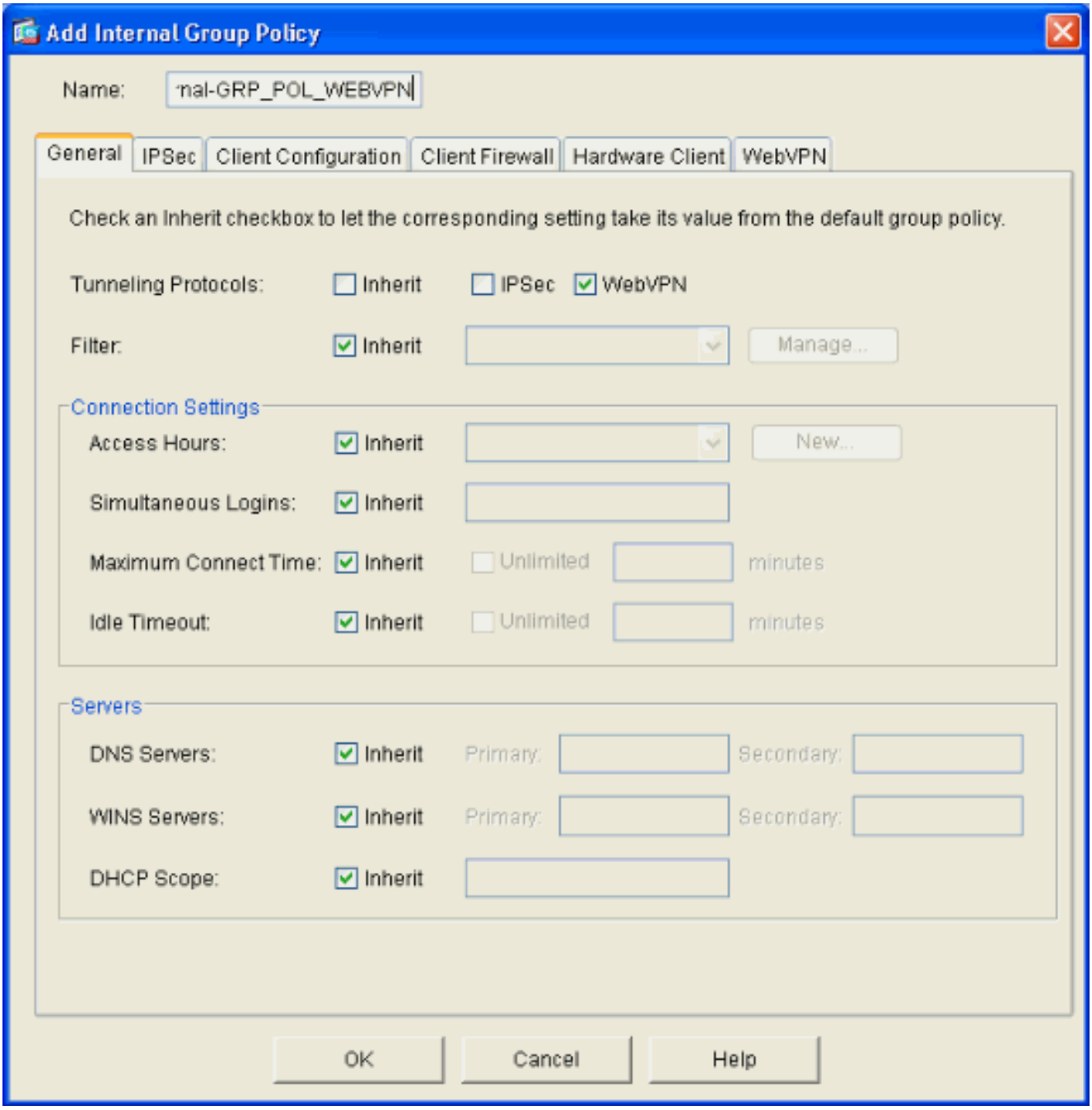
4. [OK]、[OK]、[Apply] の順にクリックします。



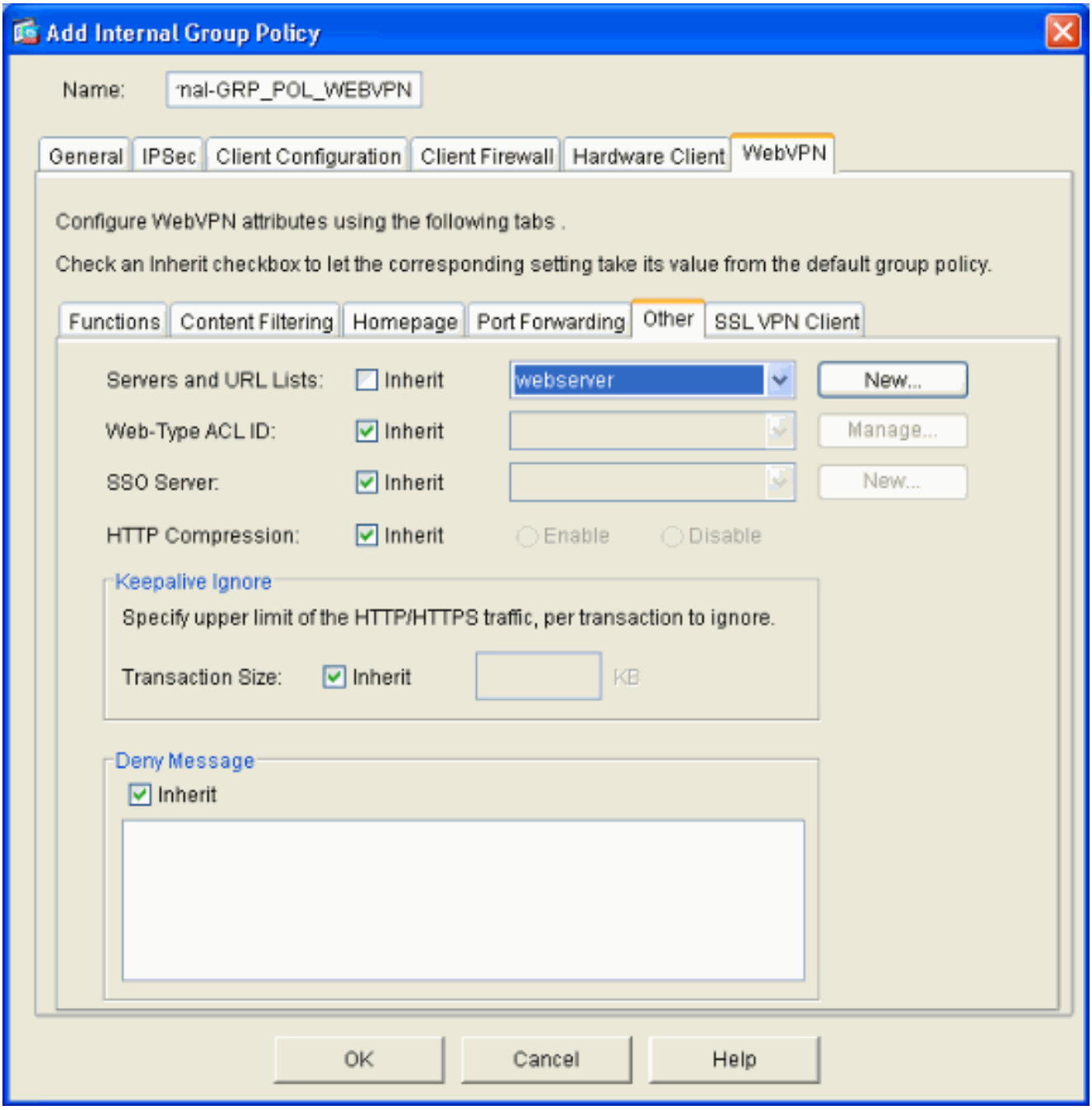
内部グループ ポリシーの設定

WebVPN ユーザのグループ ポリシーを設定するために、次の手順を実行します。

1. [Configuration] > [VPN] > [General] > [Group Policy] を選択し、[Add] をクリックして、[Internal Group Policy] を選択します。
2. [General] タブで、ポリシー名（Internal-Group_POL_WEBVPN など）を指定します。 次に、トンネリング プロトコルの横の [Inherit] をオフにし、[WebVPN] をオンにします。



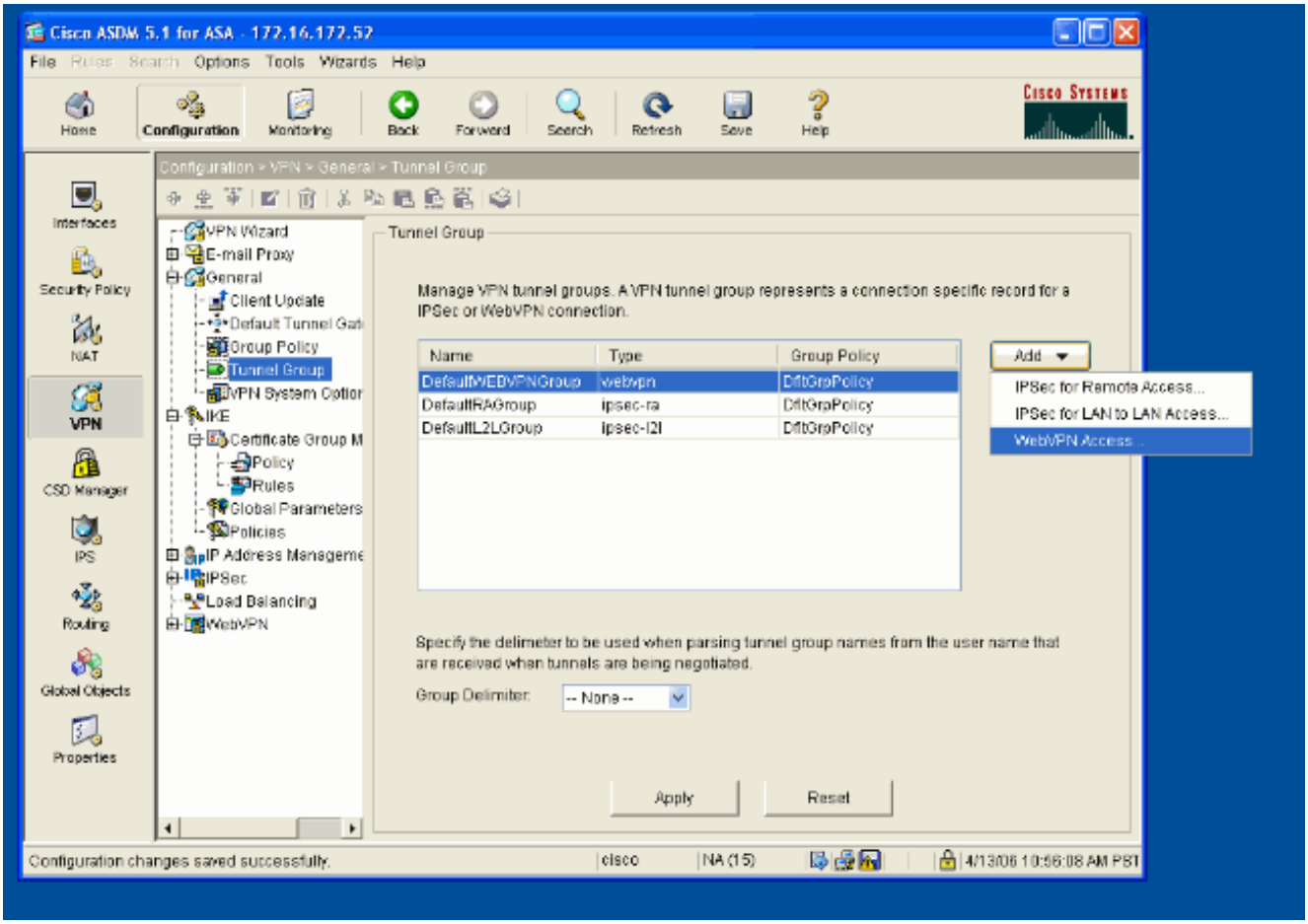
3. [WebVPN] タブで、[Other] サブタブを選択します。 サーバおよび URL リストの横の [Inherit] をオフにし、設定した URL リストをドロップダウン リストから選択します。 完了したら、[OK] をクリックします。



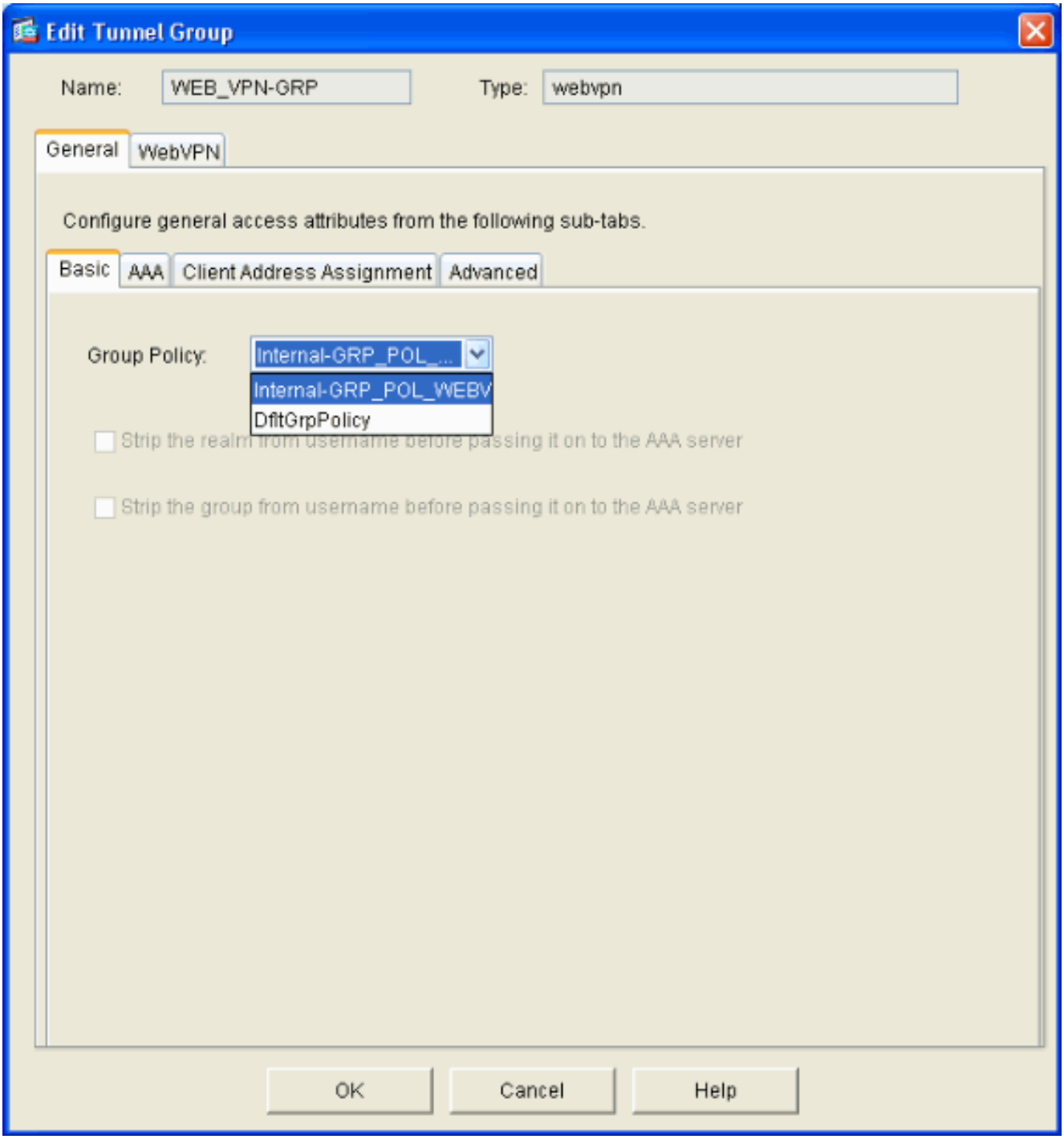
トンネル グループの設定

WebVPN ユーザのトンネル グループを設定するために、次の手順を実行します。

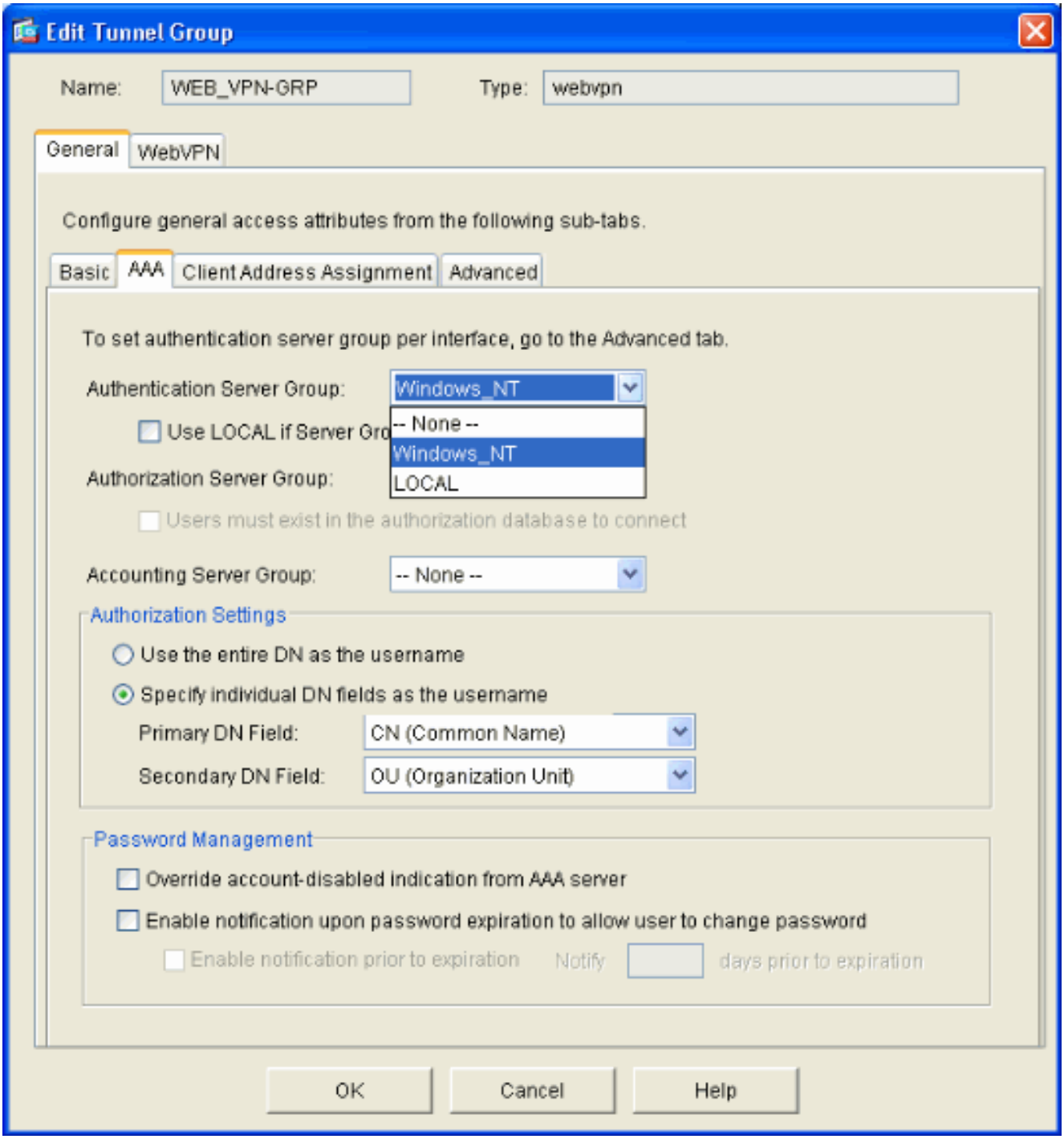
1. [Configuration] > [VPN] > [General] > [Tunnel Group] を選択し、[Add] をクリックして、[WebVPN Access...] を選択します。



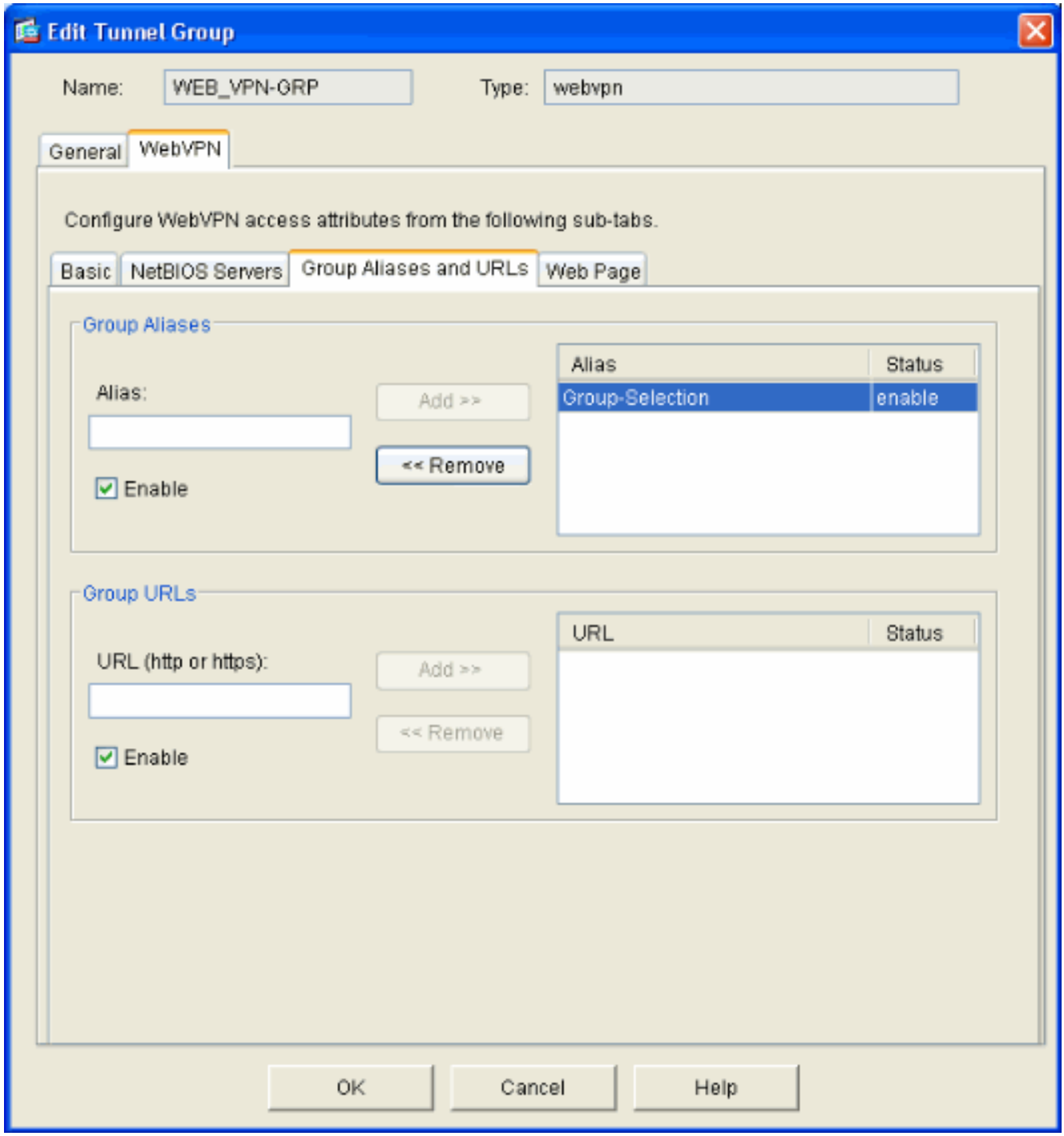
2. トンネル グループの名前（WEB_VPN-GRP など）を入力します。 [Basic] タブで、作成したグループ ポリシーを選択し、グループ タイプが **webvpn** であることを確認します。



3. [AAA] タブに移動します。[Authentication Server Group] で、ドメイン コントローラとの NTLMv1 認証を有効にするために、設定済みのグループを選択します。**オプション**： [Use LOCAL if Server Group Fails] をオンにして、設定済みの AAA グループが失敗するときに、ローカル ユーザ データベースを使用できるようにします。 これは、後でトラブルシューティングするときに役立ちます。



4. [WebVPN] タブに移動し、次に [Group Aliases and URLs] サブタブに移動します。
5. [Group Aliases] の下にエイリアスを入力し、[Add] をクリックします。 このエイリアスは、ログイン時に WebVPN ユーザに示されるドロップダウン リストに表示されます。



6. [OK] をクリックし、次に [Apply] をクリックします。

サーバの Auto-Signon の設定

内部サーバの SSO を有効に設定するために、コマンド ラインに切り替えます。

注: この手順は、ASDM では実行できないため、コマンド ラインを使用して実行する必要があります。 詳細は、『コマンドライン インターフェイスへのアクセス』を参照してください。

auto-signon コマンドを使用して、ユーザにアクセス権を与える、サーバなどのネットワーク リソースを指定します。 ここでは、単一のサーバ IP アドレスを設定していますが、**10.1.1.0 /24** などのネットワーク範囲も指定できます。 詳細は、auto-signon コマンドを参照してください。

```
ASA>enable ASA#configure terminal ASA(config)#webvpn ASA(config-webpvn)#auto-signon allow ip
10.1.1.200 255.255.255.255 auth-type ntlm ASA(config-webvpn)#quit ASA(config)#exit ASA#write
memory
```

この出力例では、WebVPN グローバルで **auto-signon** コマンドを設定しています。 このコマンドは、WebVPN グループ設定モードまたは WebVPN ユーザ名設定モードでも使用できます。 WebVPN グループ設定モードでこのコマンドを使用すると、特定のグループに限定されます。 同様に WebVPN ユーザ名設定モードでこのコマンドを使用すると、特定の個々のユーザに限定されます。 詳細は、auto-signon コマンドを参照してください。

ASA の最終設定

このドキュメントでは次の設定を使用しています。

ASA バージョン 7.1(1)

```
ASA#show running-config : Saved : ASA Version 7.1(1) !
terminal width 200 hostname ASA domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface GigabitEthernet0/0 nameif outside security-
level 0 ip address 172.16.171.51 255.255.255.0 !
interface GigabitEthernet0/1 nameif inside security-
level 100 ip address 10.1.1.1 255.255.255.0 ! interface
GigabitEthernet0/2 shutdown no nameif no security-level
no ip address ! interface GigabitEthernet0/3 shutdown no
nameif no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
cisco.com pager lines 24 mtu inside 1500 mtu outside
1500 no failover asdm image disk0:/asdm512.bin no asdm
history enable arp timeout 14400 route outside 0.0.0.0
0.0.0.0 172.16.171.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute !---
AAA server configuration aaa-server Windows_NT protocol
nt aaa-server Windows_NT host 10.1.1.200 nt-auth-domain-
controller ESC-SJ-7800 !--- Internal group policy
configuration group-policy Internal-GRP_POL_WEBVPN
internal group-policy Internal-GRP_POL_WEBVPN attributes
vpn-tunnel-protocol webvpn webvpn url-list value
webserver username cisco password Q/odgwmtmVIw4Dcm
encrypted privilege 15 aaa authentication http console
LOCAL aaa authentication ssh console LOCAL aaa
authentication enable console LOCAL http server enable
8181 http 0.0.0.0 0.0.0.0 outside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !---
Trustpoint/certificate configuration crypto ca
trustpoint Local-TP enrollment self crl configure crypto
ca certificate chain Local-TP certificate 31 308201b0
30820119 a0030201 02020131 300d0609 2a864886 f70d0101
04050030 1e311c30 1a06092a 864886f7 0d010902 160d4153
412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334
3930345a 170d3136 30333237 31333439 30345a30 1e311c30
1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e
636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d
00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a
1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434
561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404
9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17
68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3
776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06
```

```
092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544
59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d
3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b
af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de
775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a
f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c
quit !--- Tunnel group configuration tunnel-group
WEB_VPN-GRP type webvpn tunnel-group WEB_VPN-GRP
general-attributes authentication-server-group
Windows_NT default-group-policy Internal-GRP_POL_WEBVPN
tunnel-group WEB_VPN-GRP webvpn-attributes group-alias
Group-Selection enable telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
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 Configuration webvpn enable outside url-list
webserver "Internal Server" https://10.1.1.200 1 tunnel-
group-list enable auto-signon allow ip 10.1.1.200
255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6 : end
```

確認

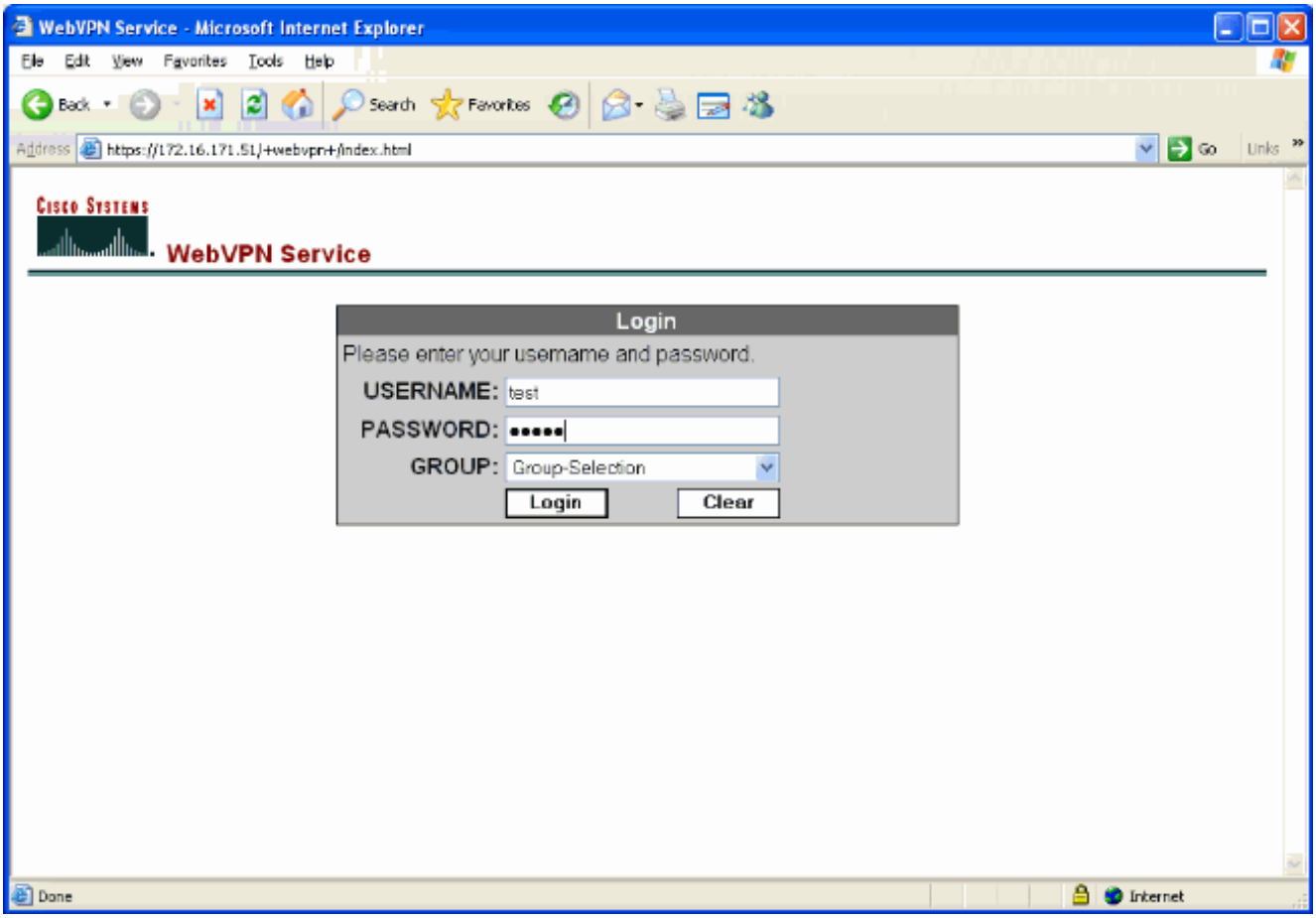
ここでは、設定が正常に動作していることを確認します。

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。

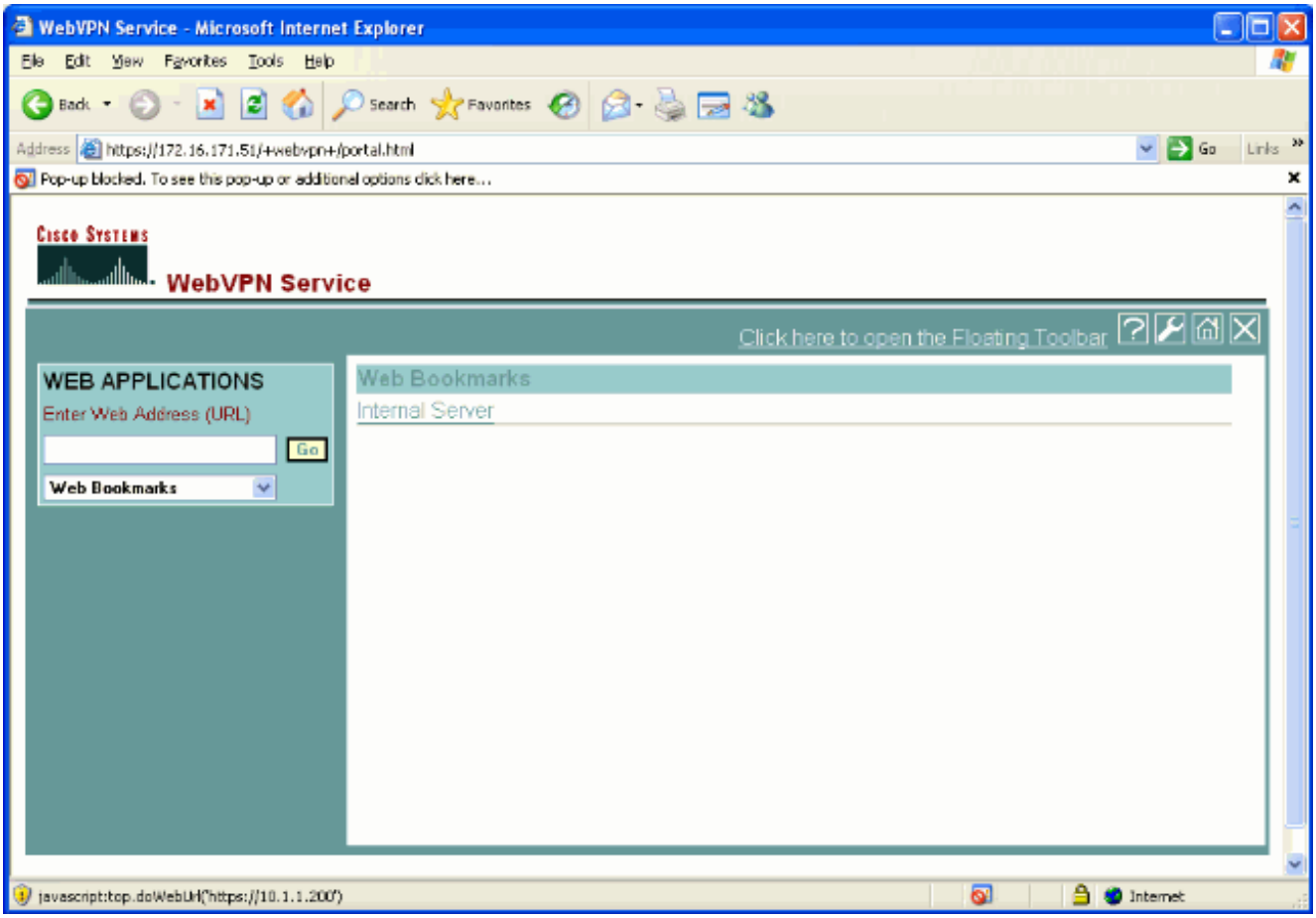
WebVPN ログインのテスト

設定をテストするためにユーザとしてログインします。

1. NT ドメインからのユーザ情報で ASA へのログインを試行します。 [Configure a Tunnel Group] の下で、ステップ 5 で設定したグループ エイリアスを選択します。

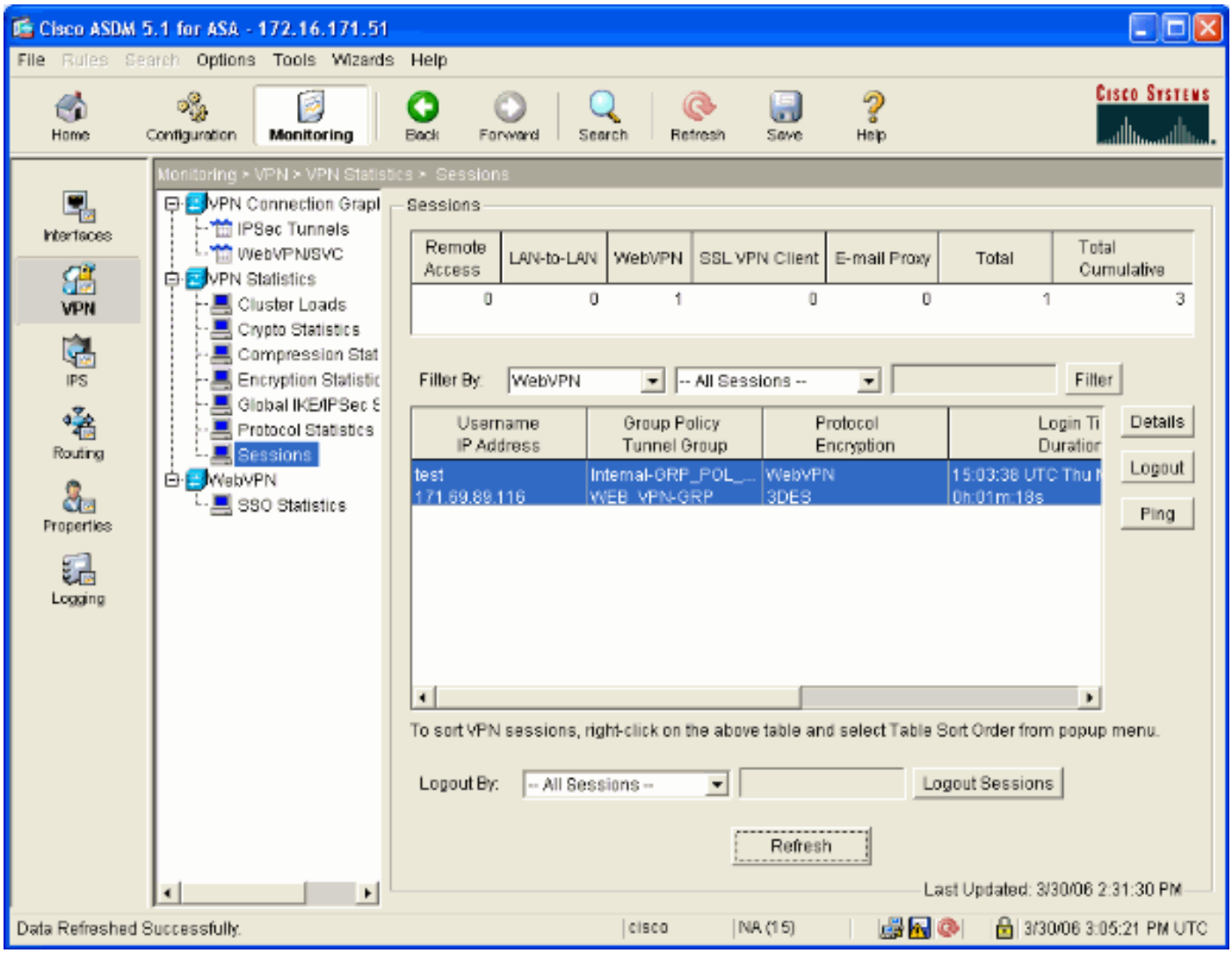


2. 内部サーバに宛てに設定されているリンクを検索します。 リンクをクリックして確認します。



セッションのモニタ

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] を選択し、このドキュメントで設定したグループに属している WebVPN セッションを探します。



WebVPN セッションのデバッグ

次の出力は、正常な WebVPN セッションのサンプル デバッグです。

注: 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。

```
ASA#debug webvpn 255 INFO: debug webvpn enabled at level 255 ASA# ASA#
webvpn_portal.c:ewaFormServe_webvpn_login[1570] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286] WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782] !--- Begin AAA WebVPN: calling AAA with
ewsContext (78986968) and nh (78960800)! WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422] WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095] WebVPN: user: (test) authenticated. !--- End
AAA webvpn_auth.c:http_webvpn_auth_accept[2093] webvpn_session.c:http_webvpn_create_session[159]
webvpn_session.c:http_webvpn_find_session[136] WebVPN session created!
webvpn_session.c:http_webvpn_find_session[136] webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202] traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421] webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. !--- Output supressed webvpn_auth.c:webvpn_auth[286]
```

```
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

- WebVPN ログイン ページに [Group] ドロップダウン ボックスが表示されない場合は、「外部インターフェイスで WebVPN をイネーブルにする」のステップ 2 および「トンネル グループの設定」のステップ 5 を実行したことを確認してください。 これらのステップを実行しておらず、このドロップダウンが表示されない場合は、デフォルト グループでの認証が行われ、通常は失敗します。
- ASDM 内および ASA 上のユーザにアクセス権を割り当てることできませんが、ドメイン コントローラ上の Microsoft Windows アクセス権によってユーザを制限することはできます。 ユーザを認証する Web ページで必要な NT グループ権限を追加してください。 ユーザがグループの権限で WebVPN にログインすると、指定したページへのアクセスがそれに応じて許可または拒否されます。 ASA は、ドメイン コントローラに代わるプロキシ認証ホストとしてのみ動作し、ここでのすべて通信は NTLMv1 になります。
- Sharepoint Server ではフォーム ベースの認証をサポートしていないため、WebVPN 上の Sharepoint に対しては SSO を設定できません。 したがって、post を含むブックマークおよび post プラグイン手順は、適用されません。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- テクニカルサポートとドキュメント - Cisco Systems