PIX/ASA： ASDM/CLI を介した VPN クライアント ユーザに対する Kerberos 認証および LDAP 認証サーバ グループの設定例

目次

概要

このドキュメントでは、Cisco Adaptive Security Device Manager（ASDM）を使用して、Cisco PIX 500 シリーズ セキュリティ アプライアンスで Kerberos 認証および LDAP 許可サーバ グループを設定する方法について説明します。 この例では、VPN トンネル グループのポリシーによってサーバ グループが使用され、着信ユーザが認証および許可されます。

前提条件

要件

このドキュメントでは、PIX が完全に動作していて、Cisco ASDM で設定を変更できるように設定されていると想定しています。

注: PIX を ASDM で設定できるようにするには、「ASDM での HTTPS アクセスの許可」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 PIX Security Appliance ソフトウェア バージョン 7.x 以降
- Cisco ASDM バージョン 5.x 以降

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。

関連製品

この設定は、Cisco Adaptive Security Appliance（ASA）バージョン 7.x でも使用できます。

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。

背景説明

VPN ユーザに対応する場合は、PIX/ASA 7.x ソフトウェアで使用可能な認証および許可方式がすべてサポートされているとは限りません。 次の表は、VPN ユーザに対して使用可能な方式の詳細を示します。

	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
認証	○	○	○	○	○	○	なし
許可	○	○	なし	なし	なし	なし	○

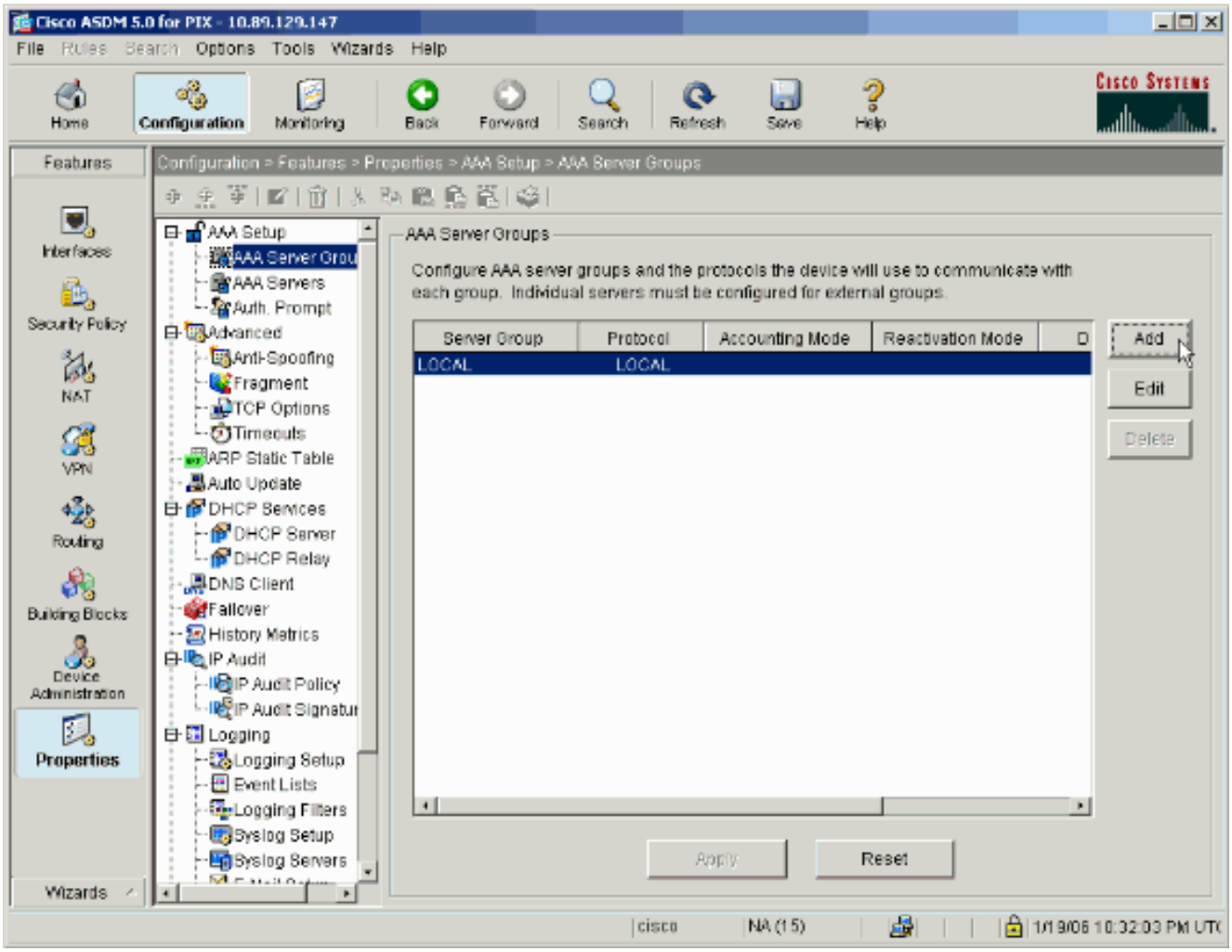
注: この例では、Kerberos が認証に使用され、LDAP が VPN ユーザの許可に使用されます。

ASDM による VPN ユーザの認証および許可の設定

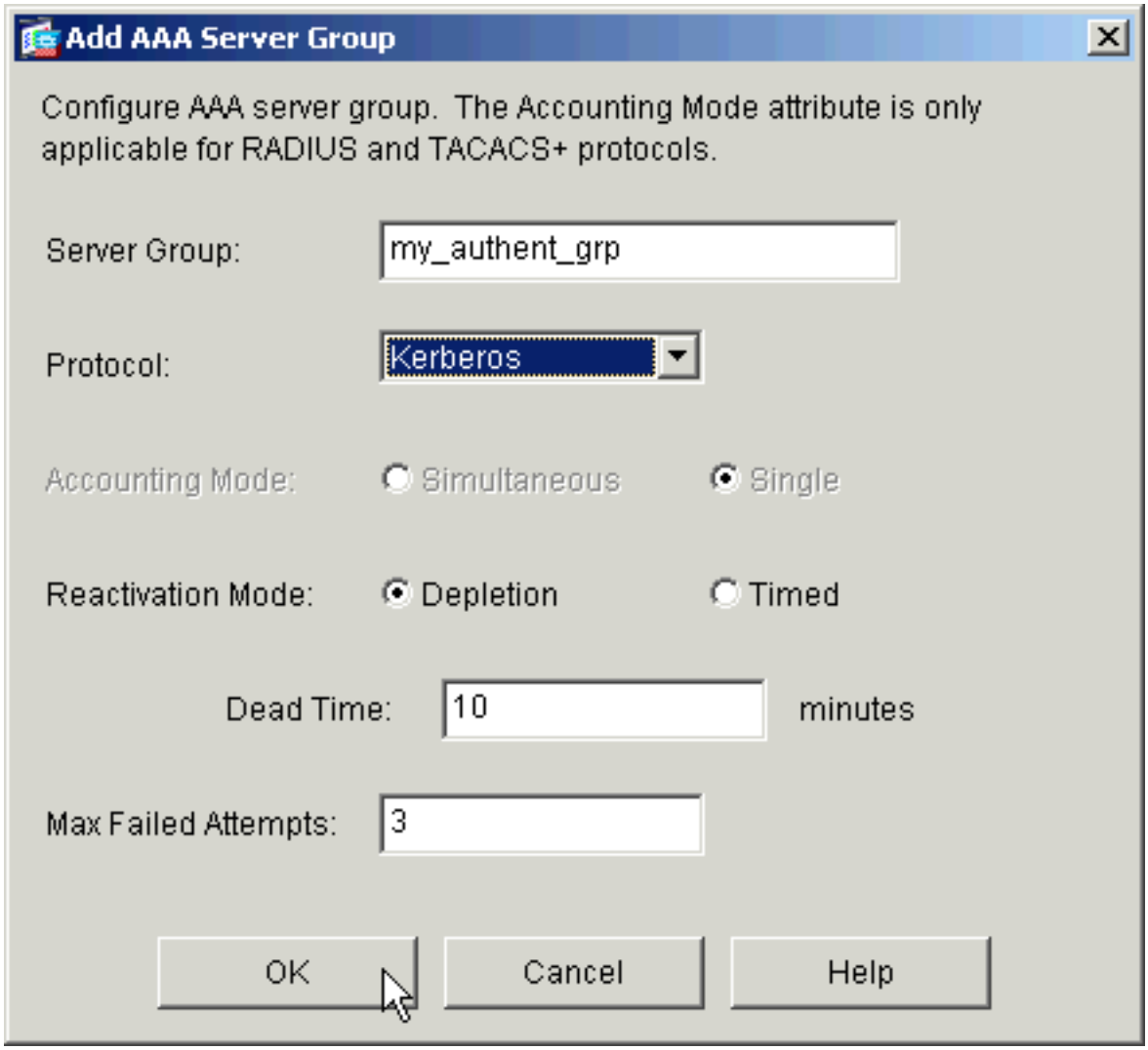
認証サーバと許可サーバの設定

次の手順を実行して、ASDM による VPN ユーザの認証および許可サーバ グループを設定します。

1. [Configuration] > [Properties] > [AAA Setup] > [AAA Server Groups] を選択し、[Add] をクリックします。

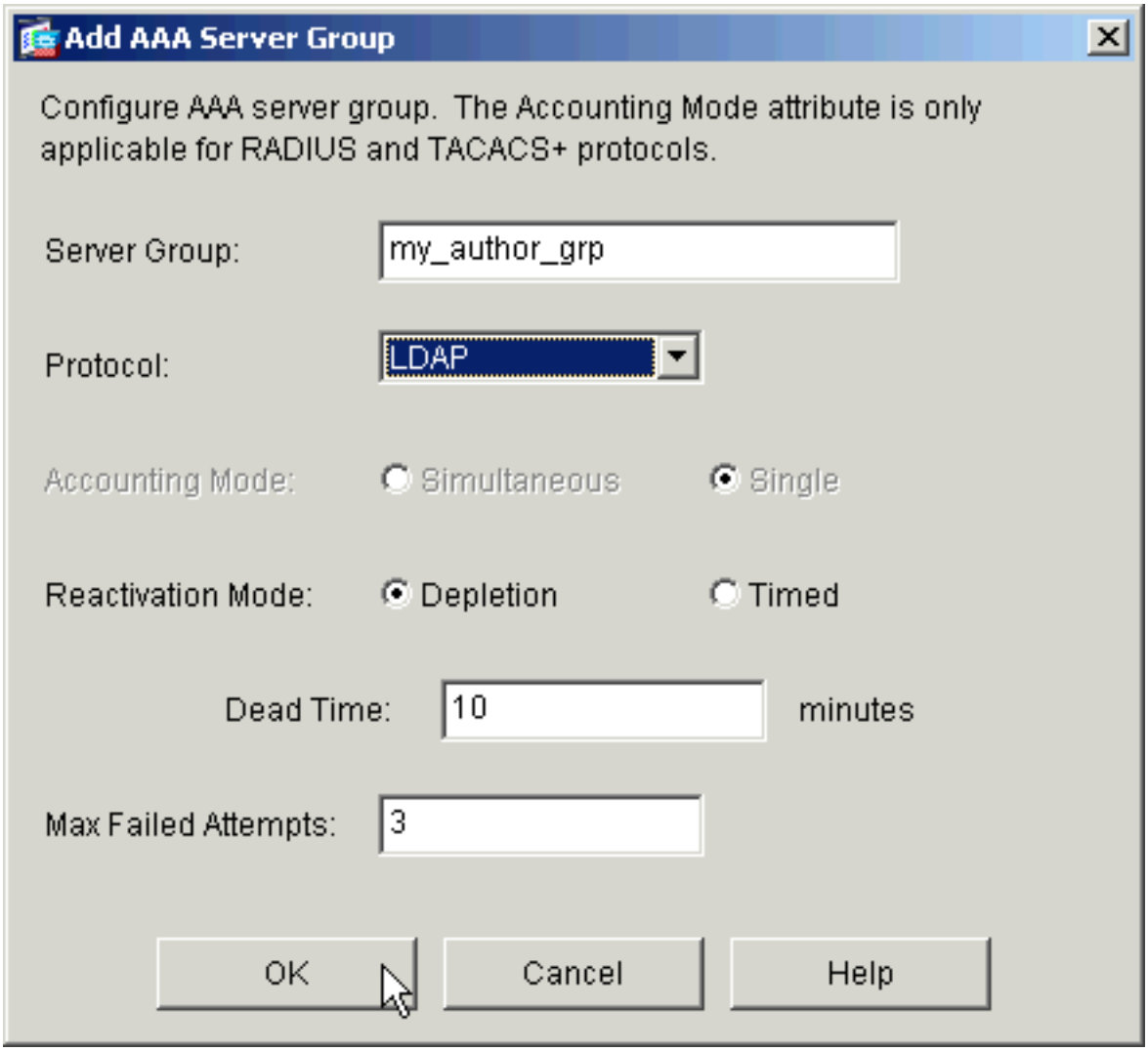


2. 新しい認証サーバ グループの名前を定義し、プロトコルを選択します。[Accounting Mode] オプションは、RADIUS および TACACS+ 専用です。 完了したら、[OK] をクリックします

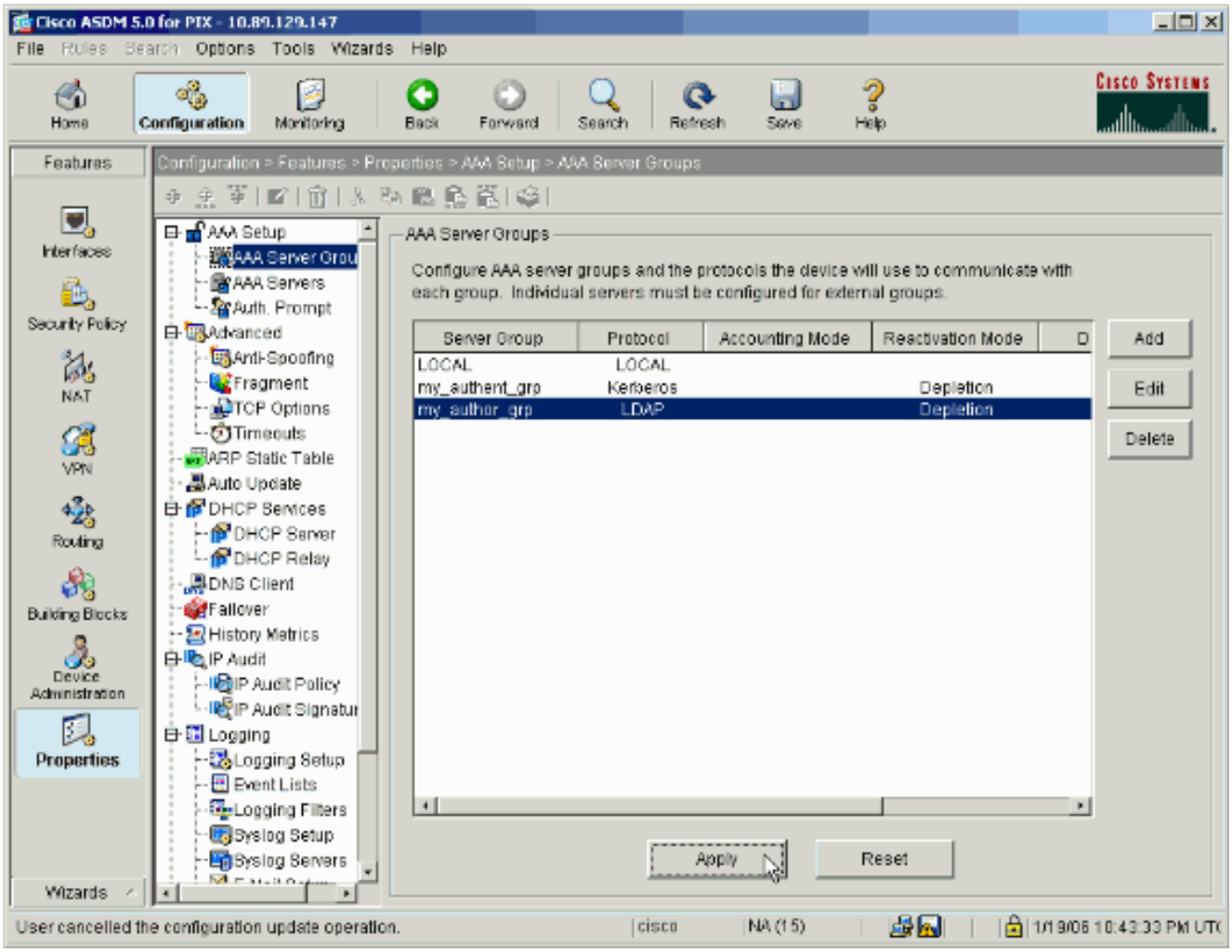


。

3. ステップ 1 および 2 を繰り返して、新しい許可サーバ グループを作成します。

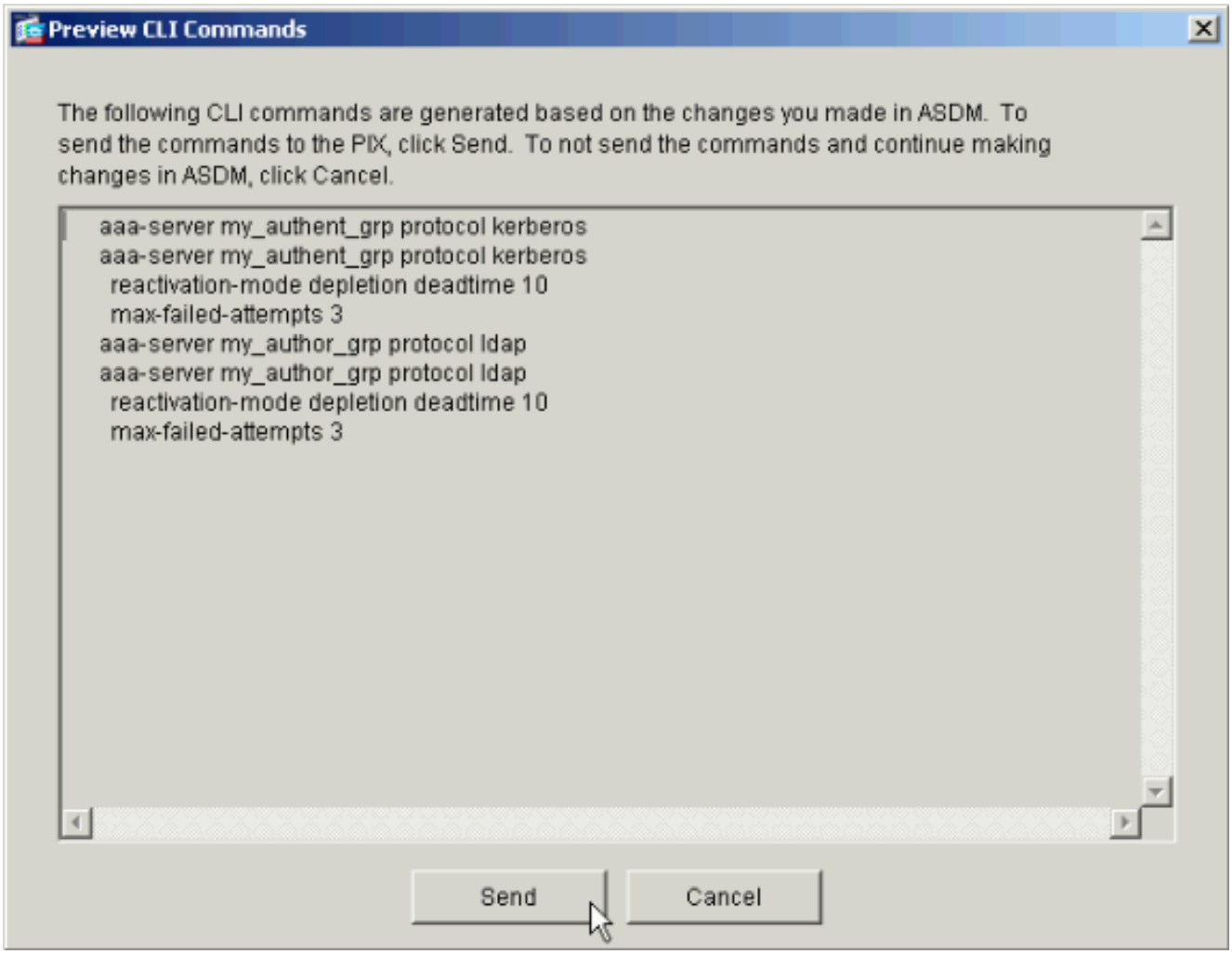


4. [Apply] をクリックしてデバイスに変更を送信します。



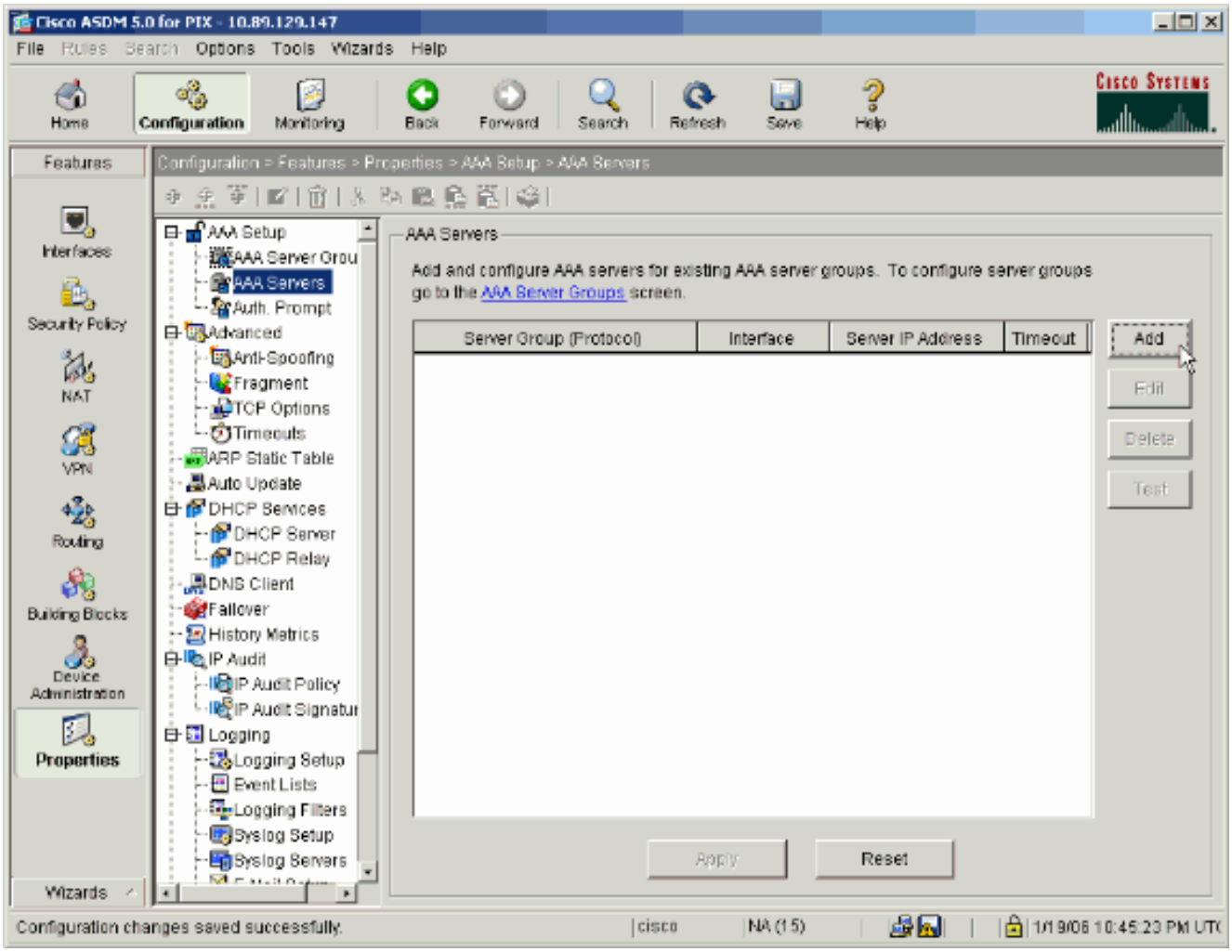
プレビューするようにデバイスを設定している場合は、実行中の設定に追加されるコマンドがデバイスでプレビューされます。

5. [Send] をクリックしてデバイスにコマンドを送信します。

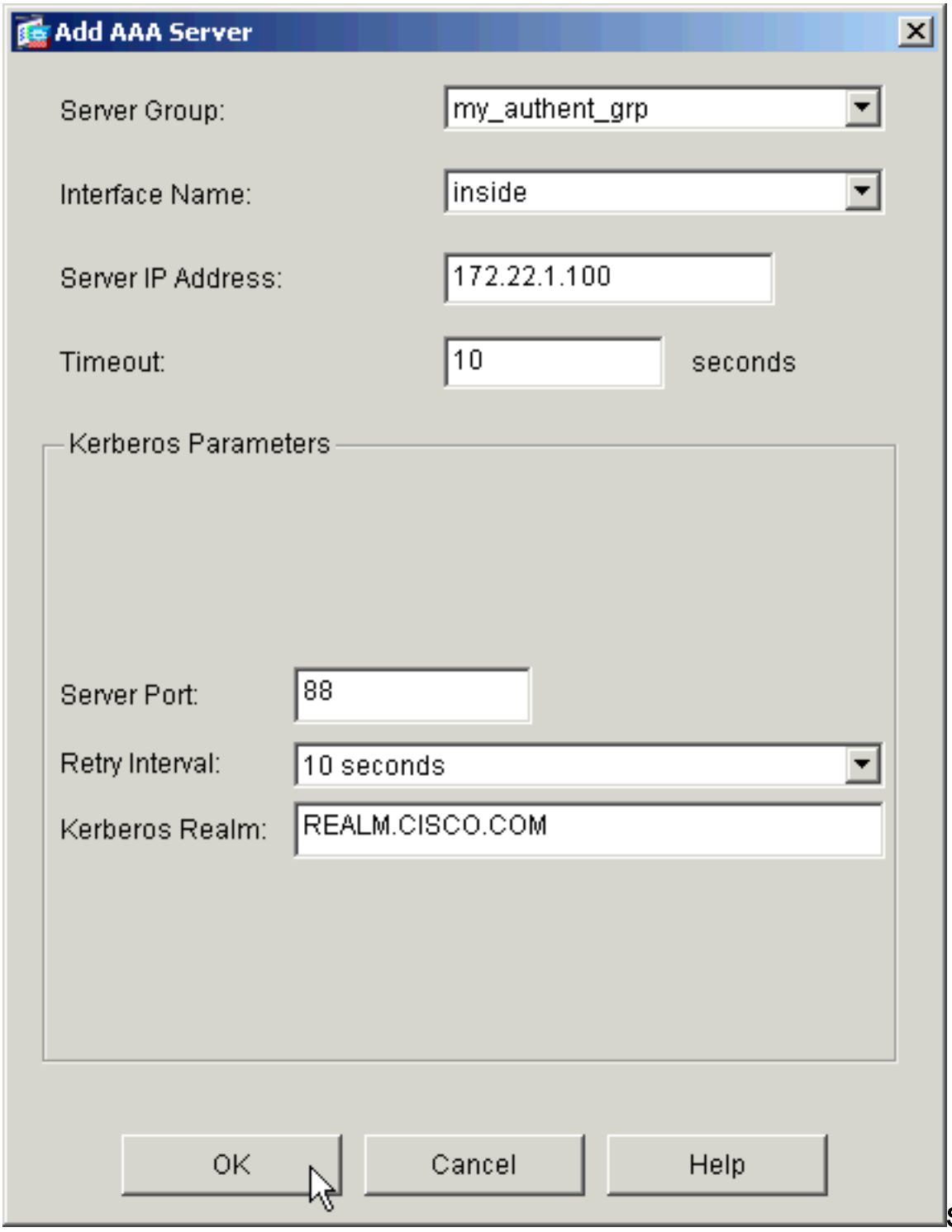


新しく作成したサーバ グループには、認証および許可サーバを入力する必要があります。

6. [Configuration] > [Properties] > [AAA Setup] > [AAA Servers] を選択し、[Add] をクリックします。

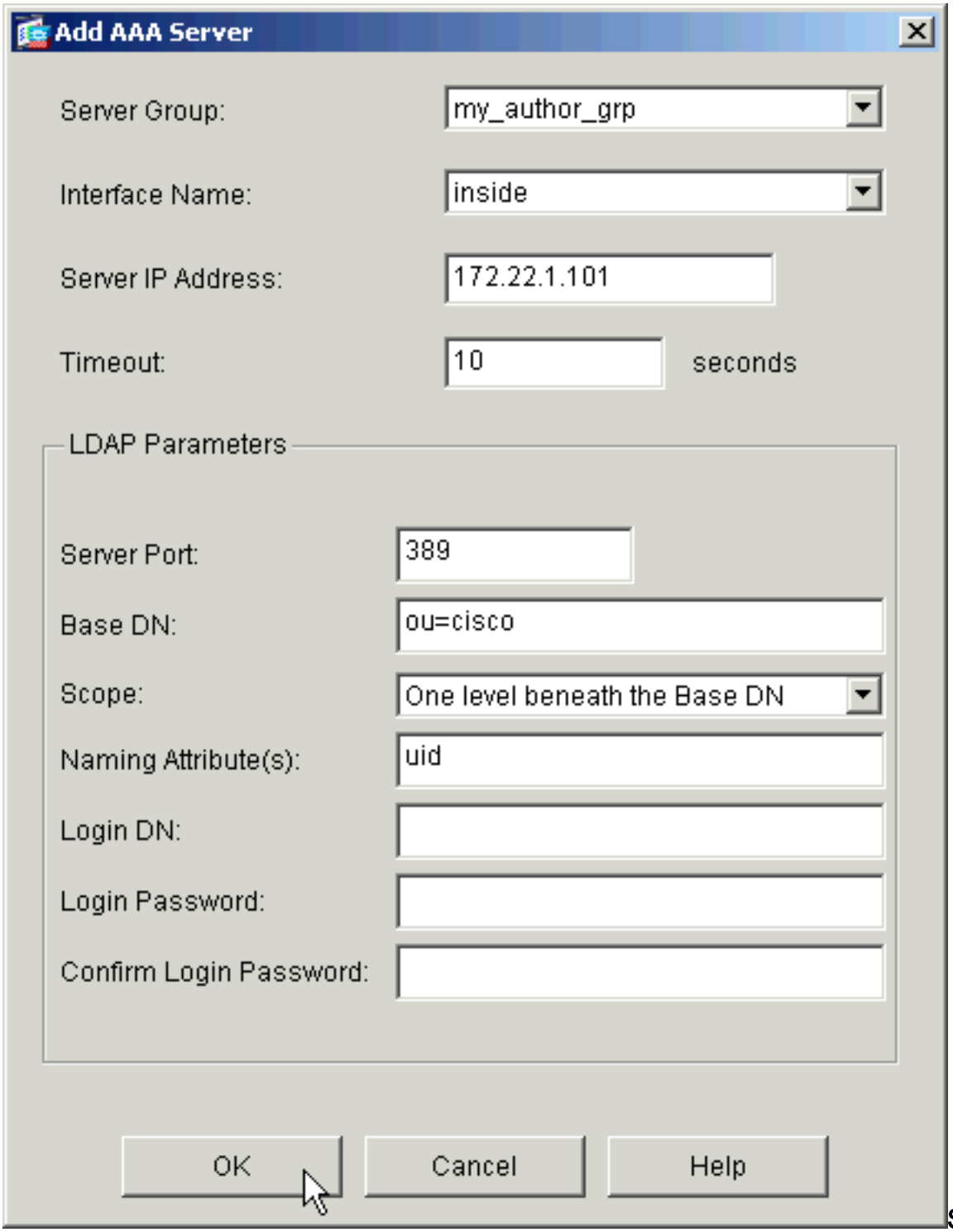


7. 認証サーバを設定します。 完了したら、[OK] をクリックします。



Server Group：ステップ 2 で設定した認証サーバ グループを選択します。**Interface Name**：サーバが常駐するインターフェイスを選択します。**Server IP Address**：認証サーバの IP アドレスを指定します。**Timeout**：サーバからの応答を待機する最大時間（秒単位）を指定します。**Kerberos パラメータ**：**Server Port**：88 が、Kerberos の標準ポートです。**Retry Interval**：必要な再試行間隔を選択します。**Kerberos Realm**：使用する Kerberos レルムの名前を入力します。 これは、通常、すべて大文字の Windows ドメイン ネームです。

8. 許可サーバを設定します。 完了したら、[OK] をクリックします。



Server Group：ステップ 3 で設定した許可サーバ グループを選択します。**Interface Name**：サーバが常駐するインターフェイスを選択します。**Server IP Address**：許可サーバの IP アドレスを指定します。**Timeout**：サーバからの応答を待機する最大時間（秒単位）を指定します。**LDAP パラメータ**：**Server Port**：389 が、LDAP のデフォルト ポートです。**Base DN**：サーバが許可要求を受信したら検索を開始する必要のある、LDAP 階層内の場所を入力します。**Scope**：サーバが許可要求を受信したら検索する必要のある LDAP 階層の範囲を選択します。**Naming Attribute(s)**：LDAP サーバのエントリを一意に識別するために使用する相対識別名属性を入力します。 一般的な命名属性は、一般名（cn）とユーザ ID（uid）です。**Login DN**：Microsoft Active Directory サーバなど、一部の LDAP サーバでは、他の LDAP 操作の要求を受け入れる前に、認証済みバインディング経由でデバイスがハンドシェイクを確立する必要があります。 [Login DN] フィールドは、管理特権を持つユーザの特性に対応する、デバイスの認証特性を定義します。 たとえば、cn=administrator と定義します。 匿名アクセスの場合は、このフィールドをブランクのままにします。**Login Password**：Login DN の

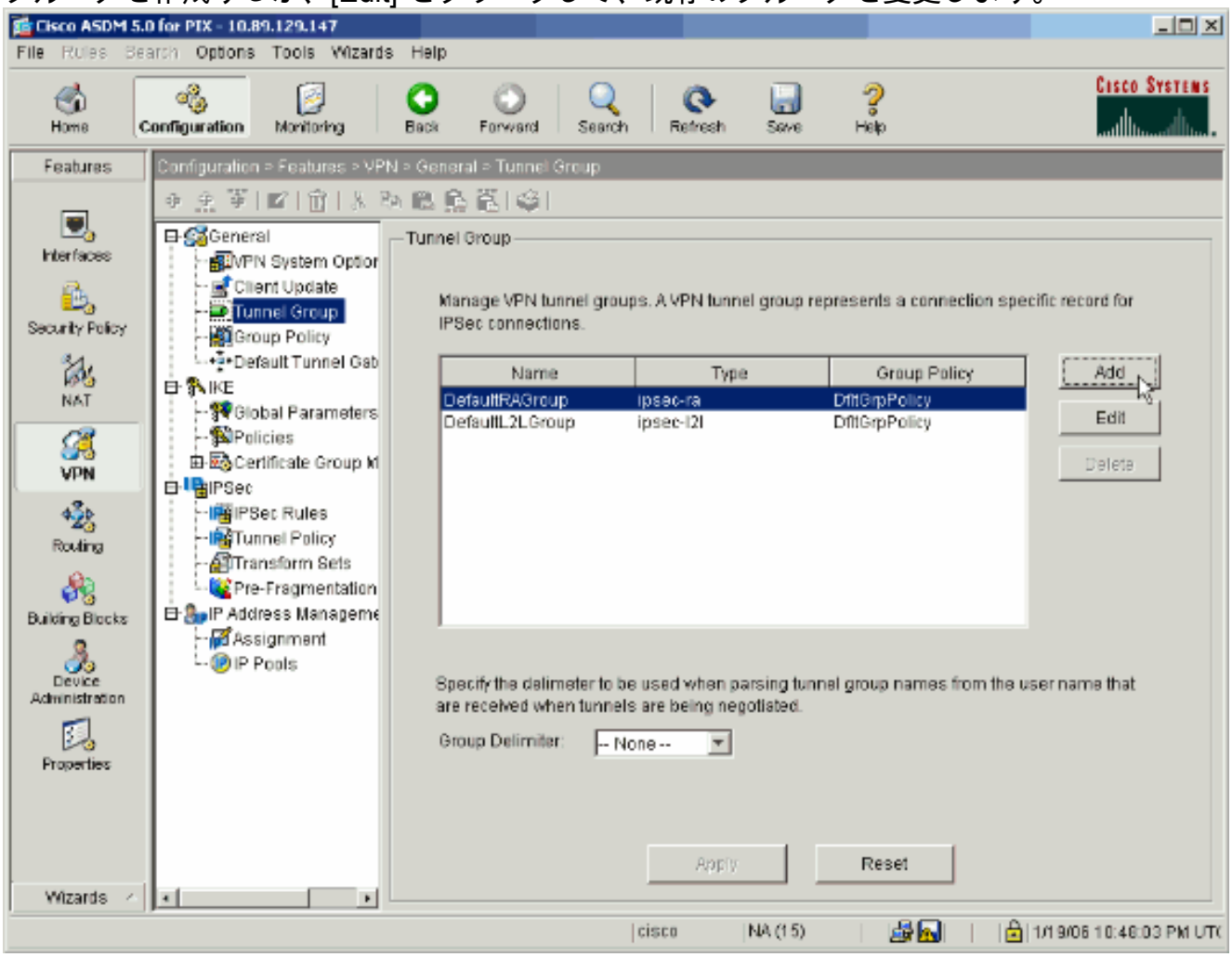
パスワードを入力します。**Confirm Login Password**：Login DN のパスワードを確認します。

9. すべての認証サーバと許可サーバを追加したら、[Apply] をクリックしてデバイスに変更を送信します。プレビューするように PIX を設定している場合は、実行中の設定に追加されるコマンドが PIX でプレビューされます。
10. [Send] をクリックしてデバイスにコマンドを送信します。

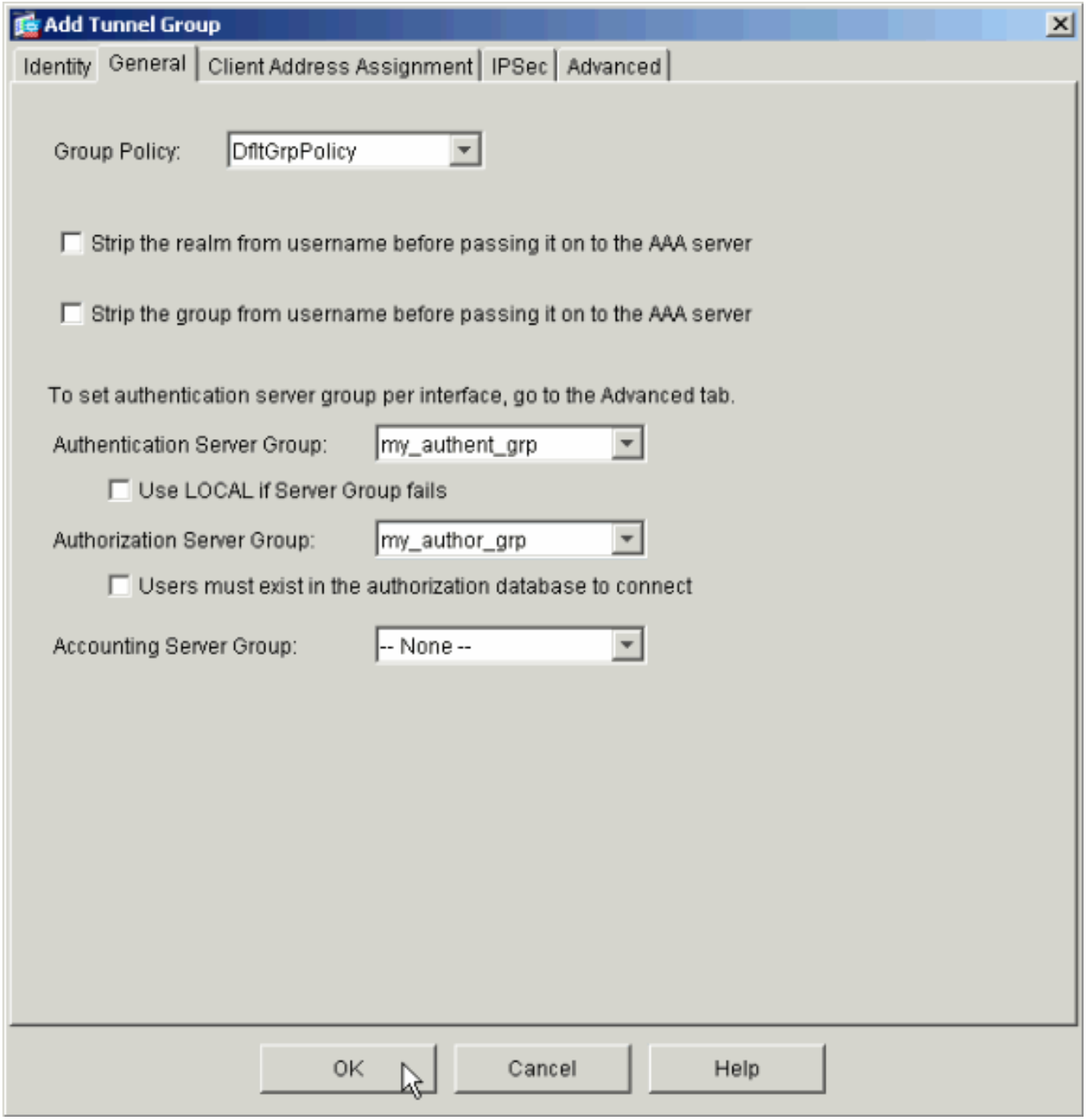
認証および許可のための VPN トンネル グループの設定

次の手順を実行して、VPN トンネル グループに設定したサーバ グループを追加します。

1. [Configuration] > [VPN] > [Tunnel Group] を選択し、[Add] をクリックして、新しいトンネル グループを作成するか、[Edit] をクリックして、既存のグループを変更します。



2. 表示されるウィンドウの [General] タブで、先ほど設定したサーバ グループを選択します。



3. *オプション：* 新しいトンネル グループを追加した場合は、その他のタブの残りのパラメータを設定します。
4. 完了したら、[OK] をクリックします。
5. トンネル グループの設定を完了したら、[Apply] をクリックしてデバイスに変更を送信します。プレビューするように PIX を設定している場合は、実行中の設定に追加されるコマンドが PIX でプレビューされます。
6. [Send] をクリックしてデバイスにコマンドを送信します。

CLI による VPN ユーザの認証および許可の設定

次に示すのは、VPN ユーザの認証および許可サーバ グループの、同等の CLI 設定です。

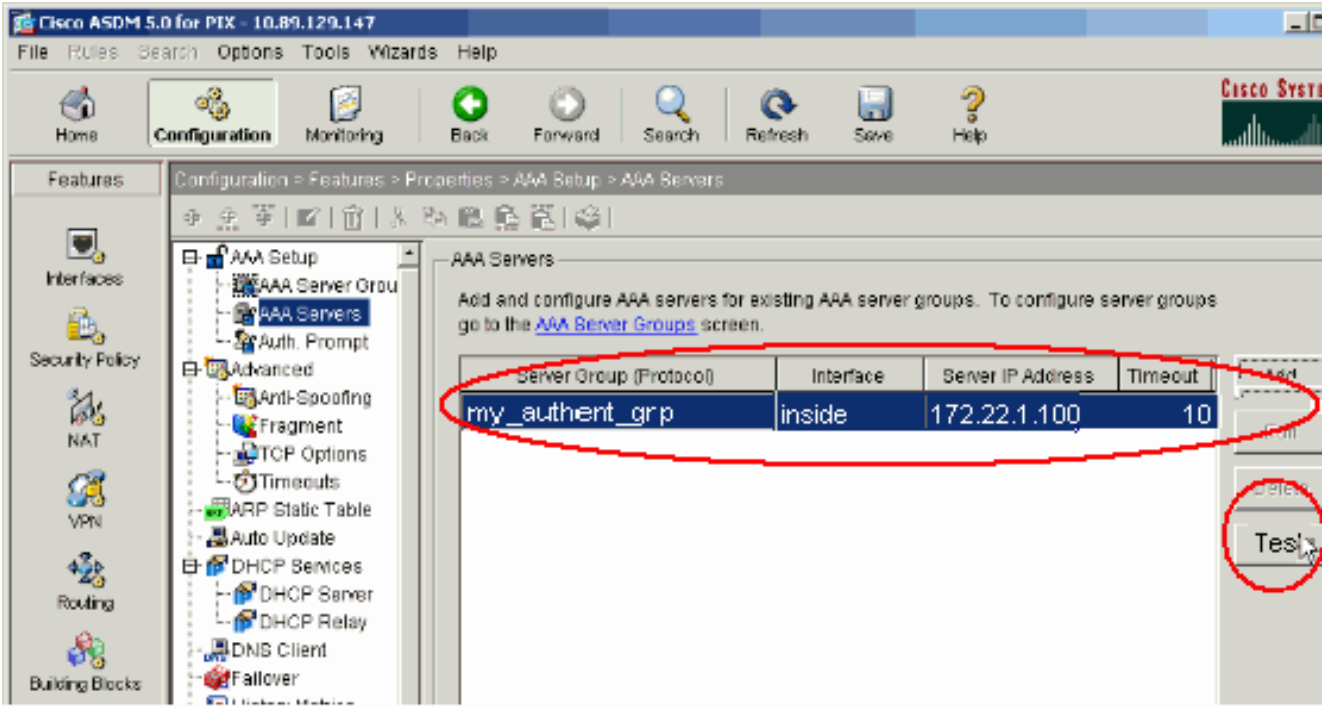
セキュリティ アプライアンスの CLI 設定
pixfirewall#**show run** : Saved : PIX Version 7.2(2) ! hostname pixfirewall domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names !

```
interface Ethernet0 shutdown no nameif no security-level
no ip address ! interface Ethernet1 nameif inside
security-level 100 ip address 172.22.1.105 255.255.255.0
! !--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid pager lines 24 mtu
inside 1500 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image flash:/asdm-522.bin !--- Output
is suppressed. aaa-server my_authent_grp protocol
kerberos aaa-server my_authent_grp host 172.22.1.100
kerberos-realm REALM.CISCO.COM aaa-server my_author_grp
protocol ldap aaa-server my_author_grp host 172.22.1.101
ldap-base-dn ou=cisco ldap-scope onelevel ldap-naming-
attribute uid http server enable http 0.0.0.0 0.0.0.0
inside no snmp-server location no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart tunnel-group DefaultRAGroup general-
attributes authentication-server-group my_authent_grp
authorization-server-group my_author_grp ! !--- Output
is suppressed.
```

確認

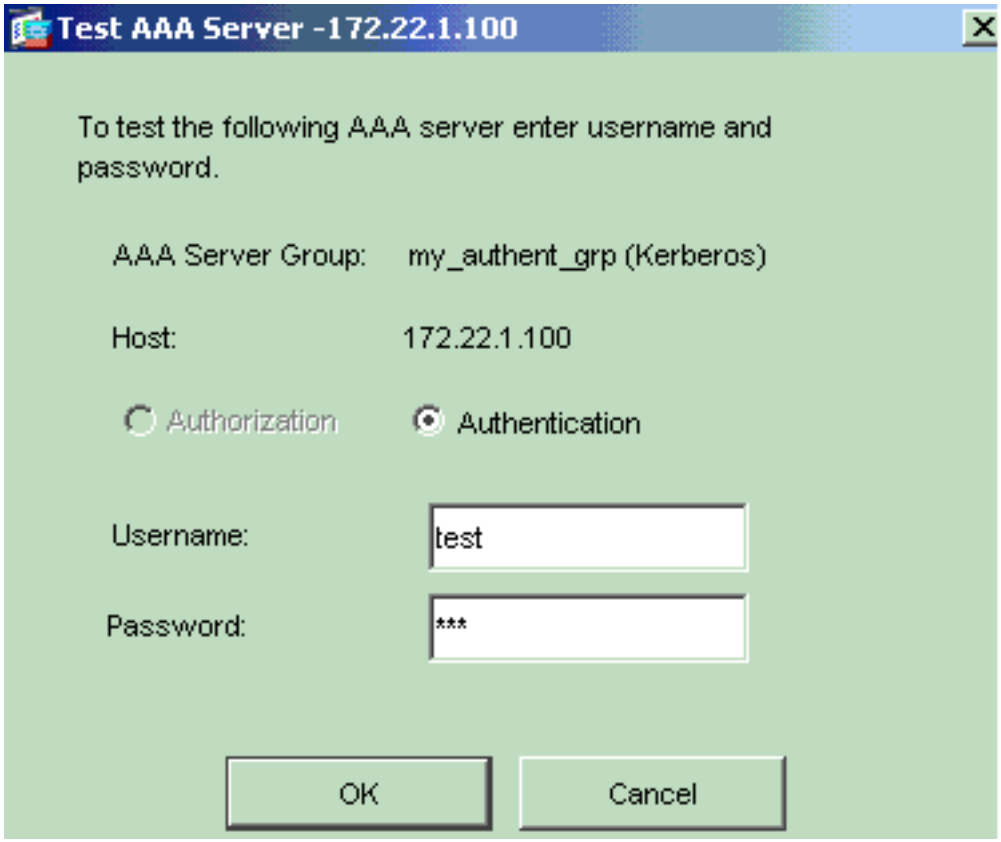
次の手順を実行して、PIX/ASA と AAA サーバの間のユーザ認証を確認します。

1. [Configuration] > [Properties] > [AAA Setup] > [AAA Servers] を選択し、サーバ グループ（my_authent_grp）を選択します。 次に、[Test] をクリックしてユーザ クレデンシャルを許可します。

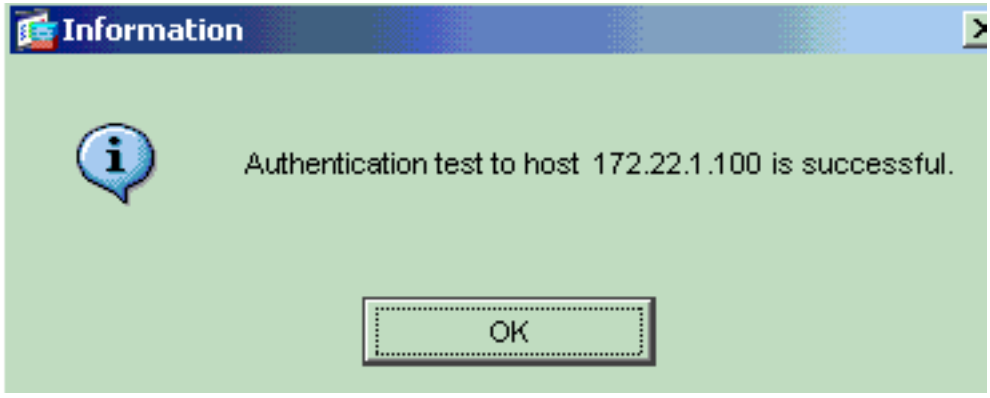


2. ユーザ名とパスワード（username: test と password: test など）を入力し、[OK] をクリック

して検証します。



3. 認証が成功したことが表示されます。



トラブルシューティング

1. 認証エラーの一般的な原因の 1 つは、時間のずれです。 PIX または ASA のクロックと認証サーバが同期していることを確認します。認証が時間のずれによって失敗すると、 `--ERROR: Authentication Rejected: Clock skew greater than 300 seconds..`」というエラー メッセージを受信する場合があります。 また、次のログ メッセージが表示されます。`%%PIX|ASA-3-113020: Kerberos error : Clock skew with server ip_address greater than 300 seconds` ip_address — The IP address of the Kerberos server.このメッセージは、Kerberos サーバ経由の IPSec または WebVPN ユーザの認証が、セキュリティ アプライアンスのクロックとサーバのクロックのずれが 5 分（300 秒）を超えているために失敗した場合に表示されます。これが発生した場合は、接続しようとしても拒否されます。この問題を解決するには、セキュリティ アプライアンスと Kerberos サーバのクロックを同期します。
2. Active Directory（AD）の事前認証は、無効にする必要があります。そうしないと、ユーザ認証が失敗する可能性があります。
3. VPN Client ユーザは、Microsoft 証明書サーバに対して認証することはできません。 次のエラー メッセージが表示されます。`""Error processing payload" (Error 14)` この問題を解決するには、認証サーバの [do not require kerberose preauthentication] チェックボックスをオフ

にします。

関連情報

- AAA サーバとローカル データベースの設定
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス製品のサポート
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems