PIX/ASA: Konfigurationsbeispiel für die Kerberos-Authentifizierung und LDAP-Autorisierungsserver-Gruppen für VPN-Client-Benutzer über ASDM/CLI

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie mit dem Cisco Adaptive Security Device Manager (ASDM) die Kerberos-Authentifizierung und LDAP-Autorisierungsserver-Gruppen auf den Sicherheitslösungen der Serie Cisco PIX 500 konfigurieren. In diesem Beispiel werden die Servergruppen von der Richtlinie einer VPN-Tunnelgruppe verwendet, um eingehende Benutzer zu authentifizieren und zu autorisieren.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass das PIX vollständig betriebsbereit ist und so konfiguriert ist, dass der ASDM Konfigurationsänderungen vornehmen kann.

Hinweis: Informationen zur Konfiguration des PIX durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Verwendete Komponenten

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

- Cisco PIX Security Appliance Software Version 7.x oder höher
- Cisco ASDM Version 5.x und höher

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.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Adaptive Security Appliance (ASA) Version 7.x verwendet werden.

Konventionen

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

Hintergrundinformationen

Nicht alle möglichen Authentifizierungs- und Autorisierungsmethoden, die in der PIX/ASA 7.x-Software verfügbar sind, werden unterstützt, wenn Sie mit VPN-Benutzern umgehen. In dieser Tabelle sind die für VPN-Benutzer verfügbaren Methoden aufgeführt:

	Lokal	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
Authentifizierung	Ja	Ja	Ja	Ja	Ja	Ja	Nein
Autorisierung	Ja	Ja	Nein	Nein	Nein	Nein	Ja

Hinweis: Kerberos wird für die Authentifizierung und LDAP für die Autorisierung von VPN-Benutzern in diesem Beispiel verwendet.

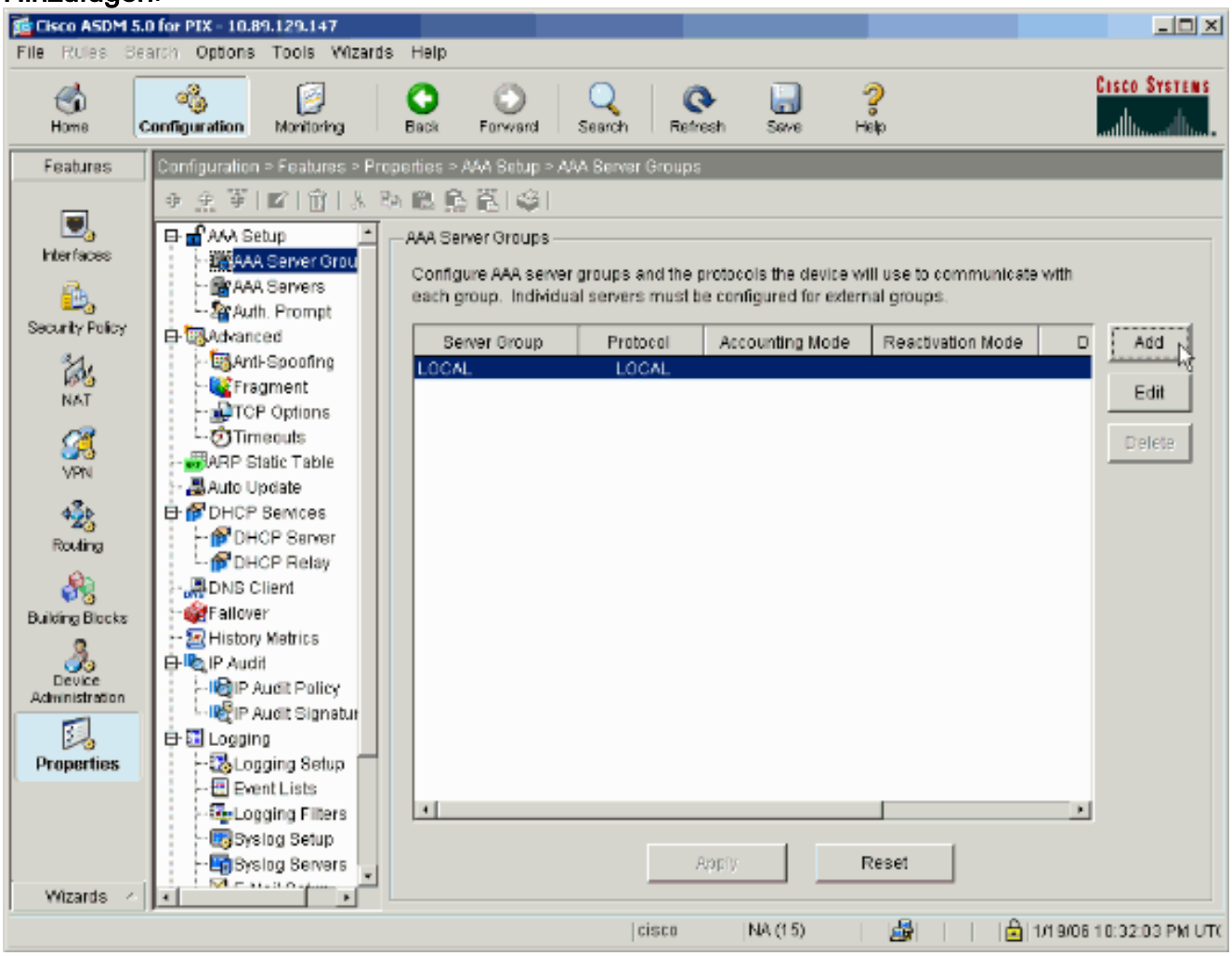
Konfigurieren der Authentifizierung und Autorisierung für VPN-Benutzer mithilfe von ASDM

Authentifizierungs- und Autorisierungsserver konfigurieren

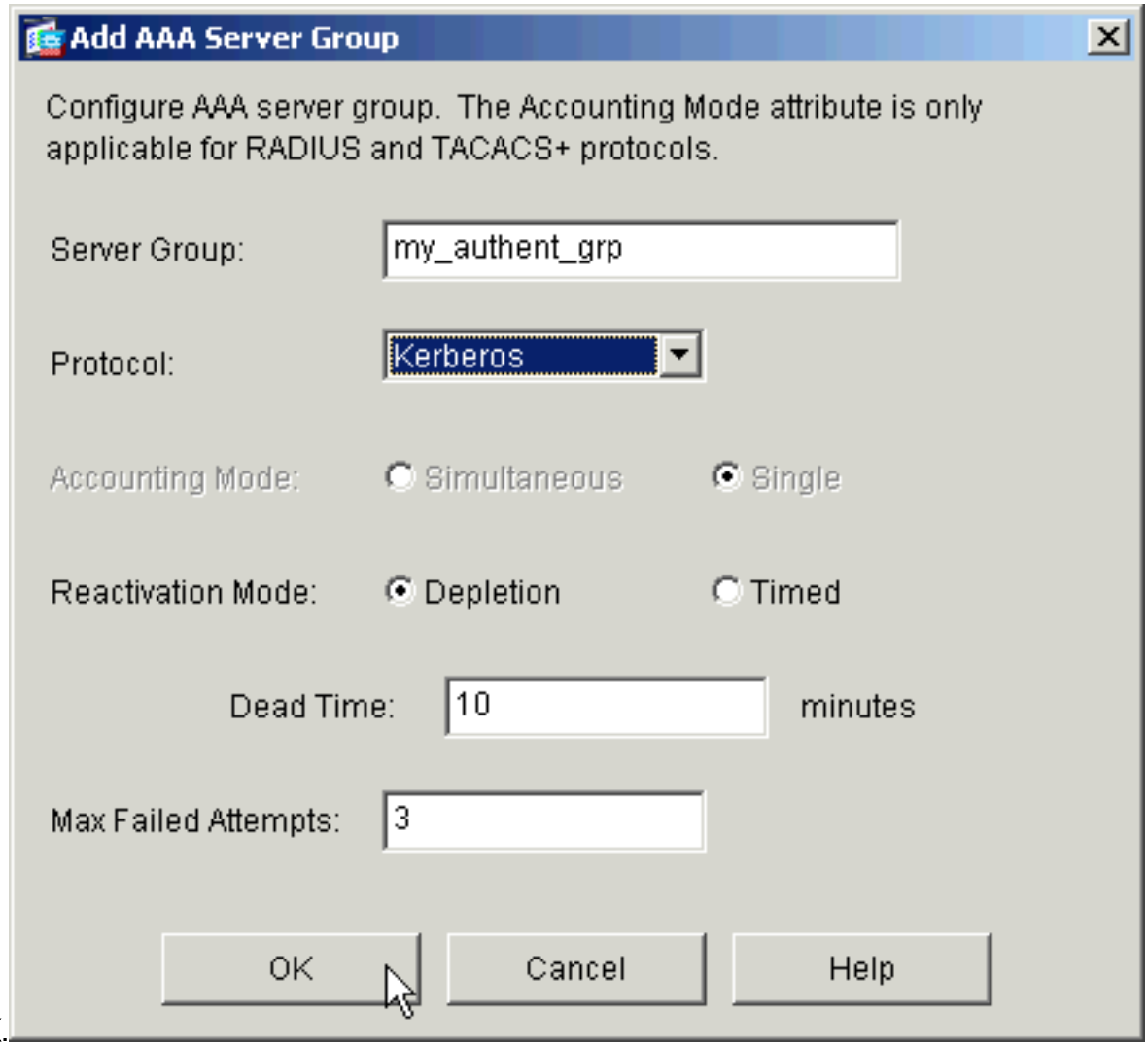
Führen Sie diese Schritte aus, um die Authentifizierungs- und Autorisierungsserver-Gruppen für VPN-Benutzer über ASDM zu konfigurieren.

1. Wählen Sie **Konfiguration > Eigenschaften > AAA-Setup > AAA-Servergruppen aus**, und

klicken Sie auf
Hinzufügen.

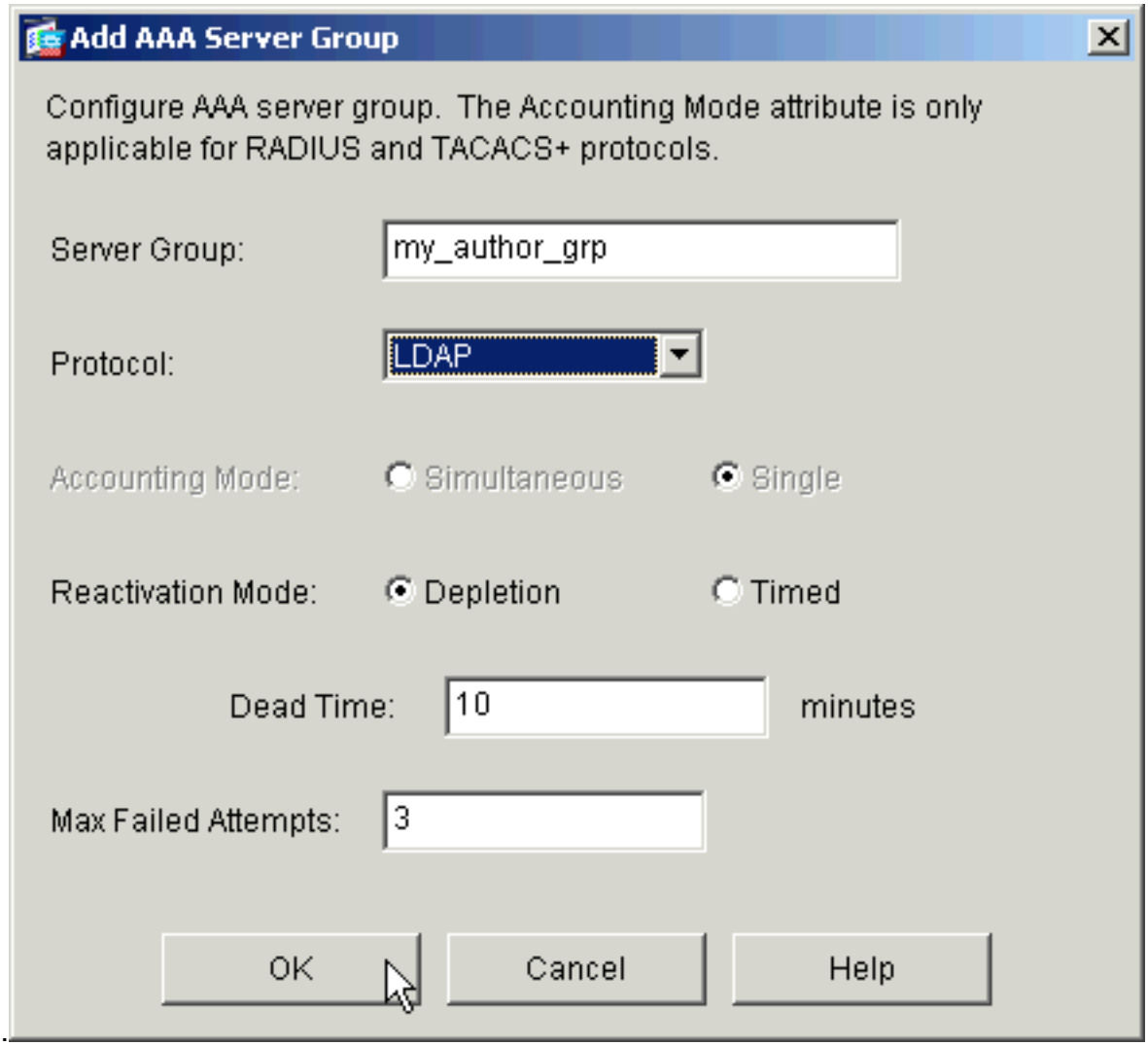


2. Definieren Sie einen Namen für die neue Authentifizierungsservergruppe, und wählen Sie ein Protokoll aus.Die Option Accounting Mode ist nur für RADIUS und TACACS+ verfügbar. Klicken Sie abschließend auf



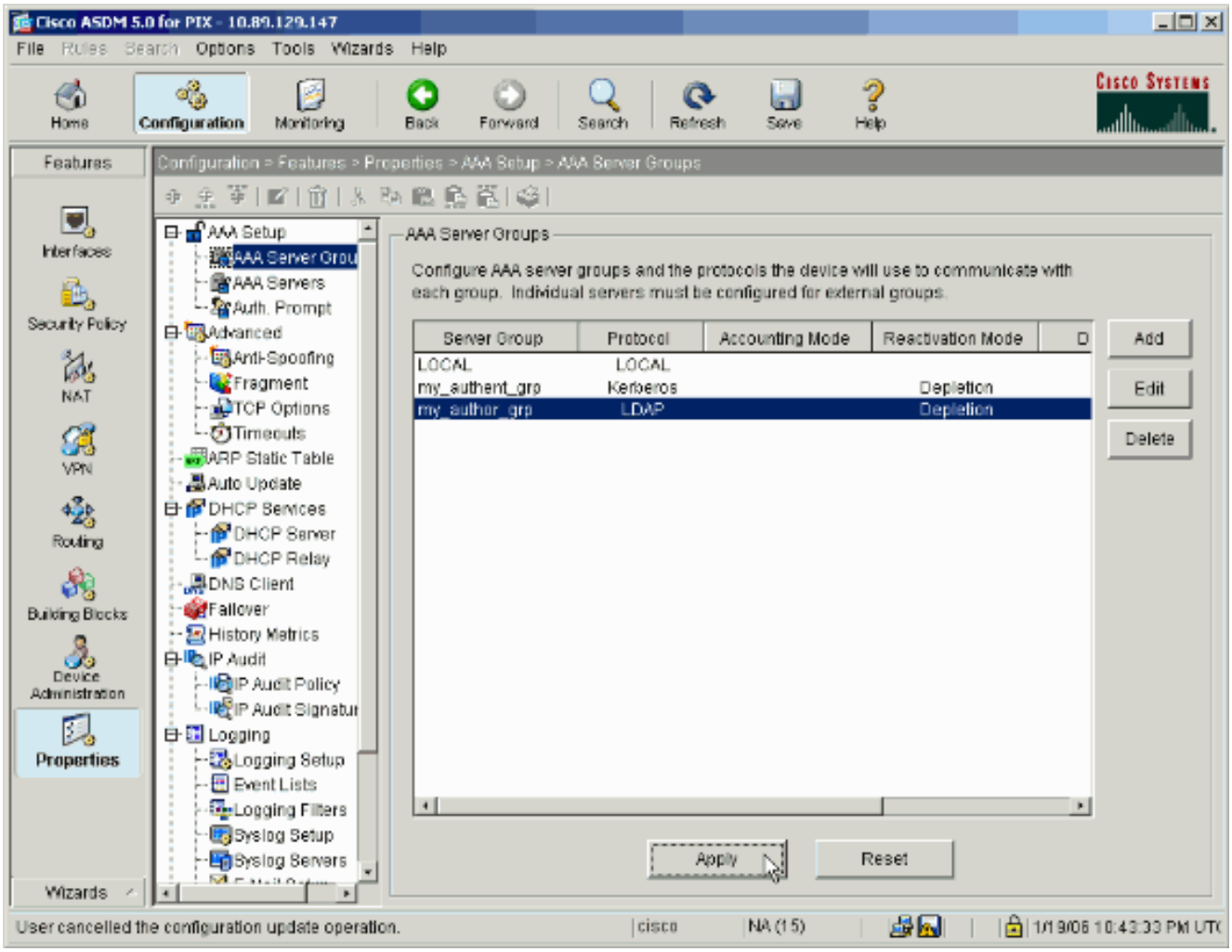
OK.

3. Wiederholen Sie die Schritte 1 und 2, um eine neue Autorisierungsserver-Gruppe zu



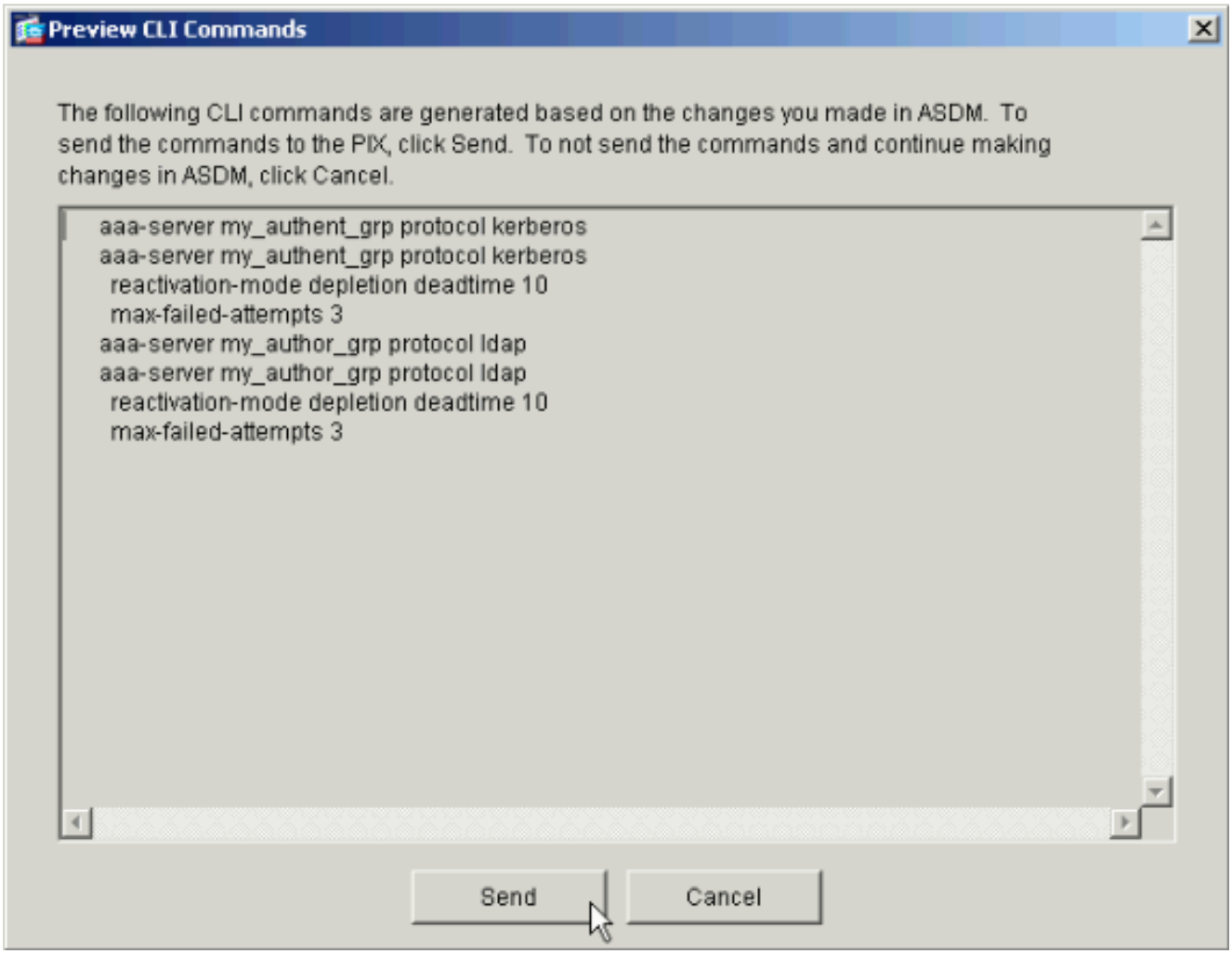
erstellen.

4. Klicken Sie auf **Apply**, um die Änderungen an das Gerät zu senden.



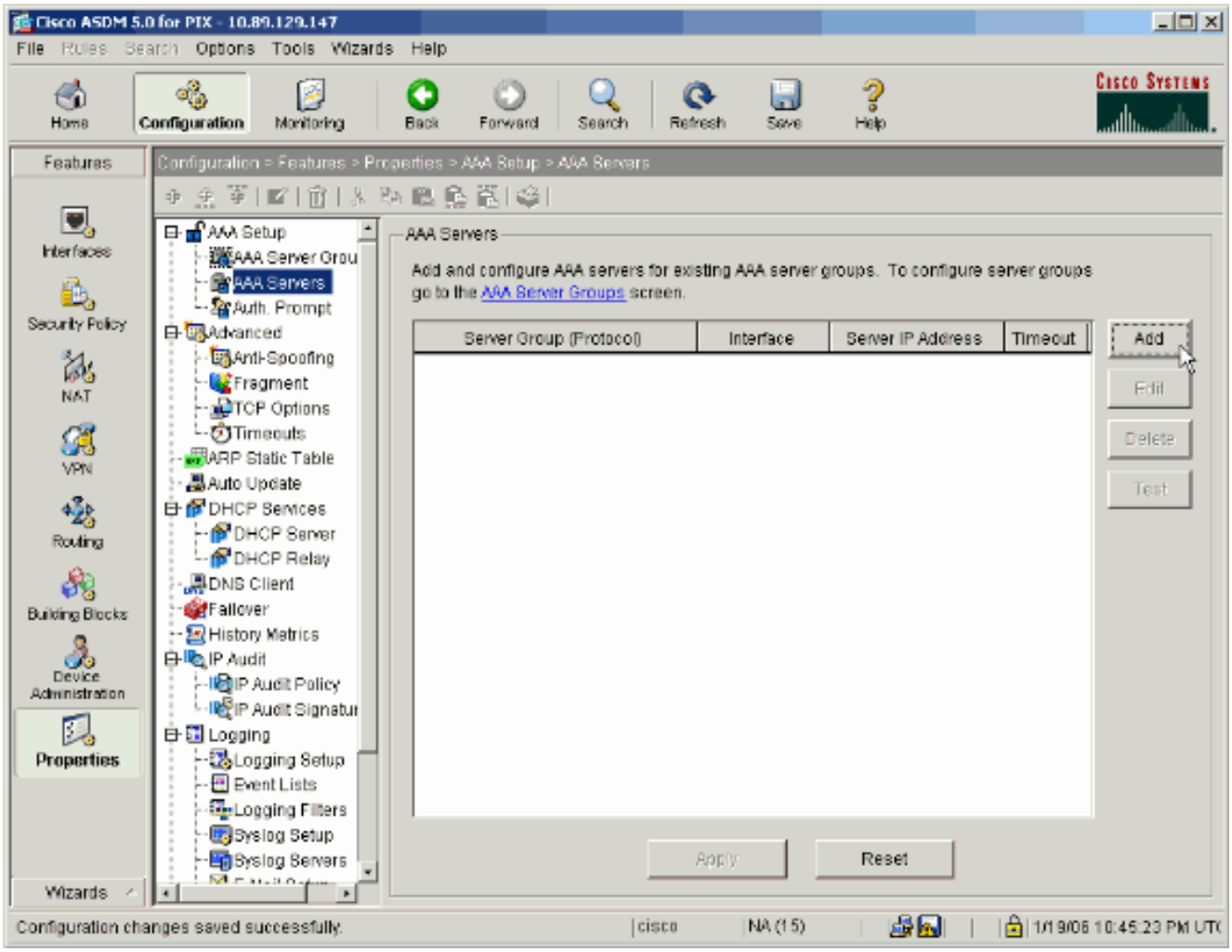
Wenn Sie dies konfiguriert haben, zeigt das Gerät jetzt die Befehle vorab an, die der aktuellen Konfiguration hinzugefügt werden.

5. Klicken Sie auf **Senden**, um die Befehle an das Gerät zu senden.

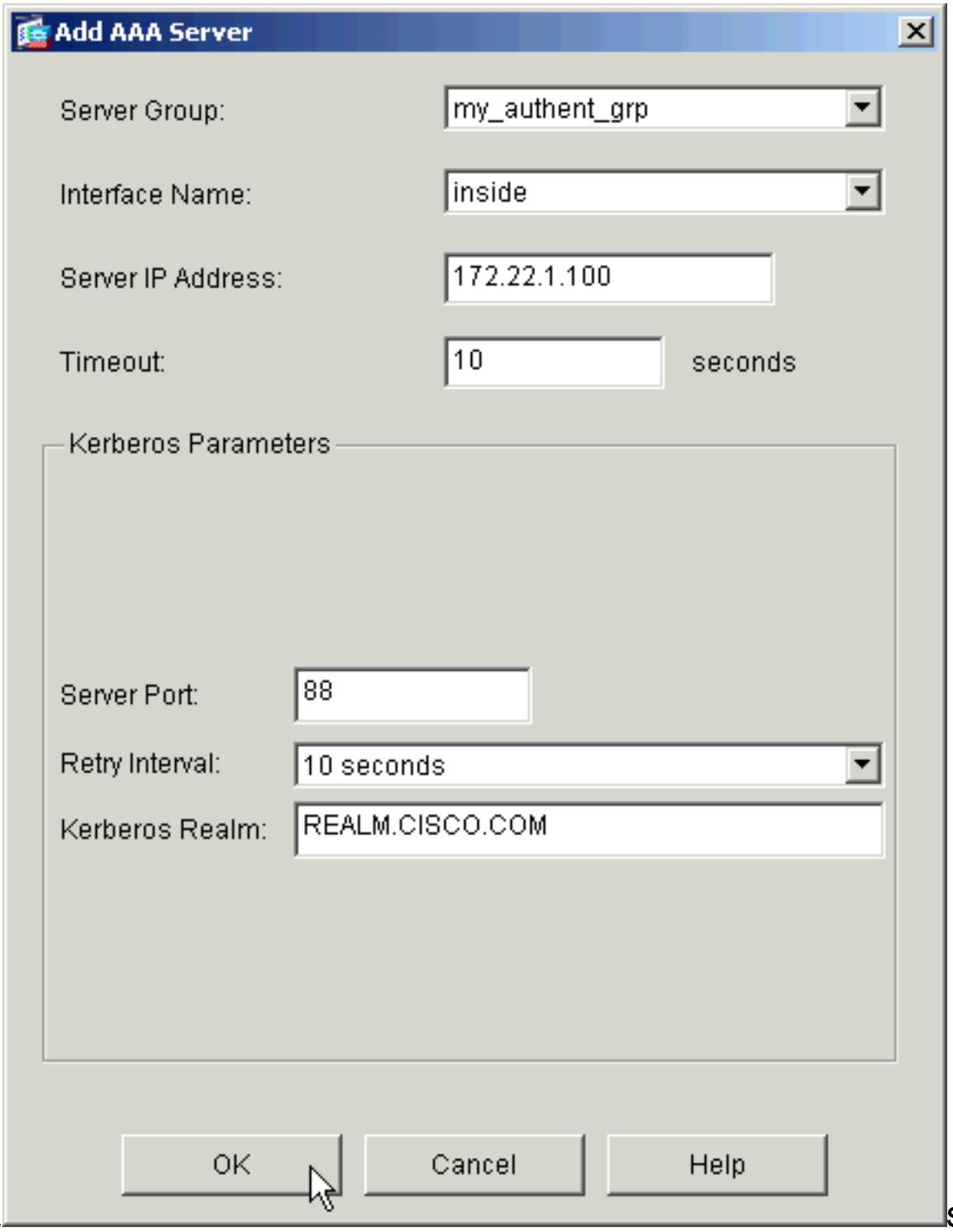


Die neu erstellten Servergruppen müssen nun mit Authentifizierungs- und Autorisierungsservern gefüllt werden.

6. Wählen Sie **Konfiguration > Eigenschaften > AAA-Setup > AAA-Server aus**, und klicken Sie auf
Hinzufügen.

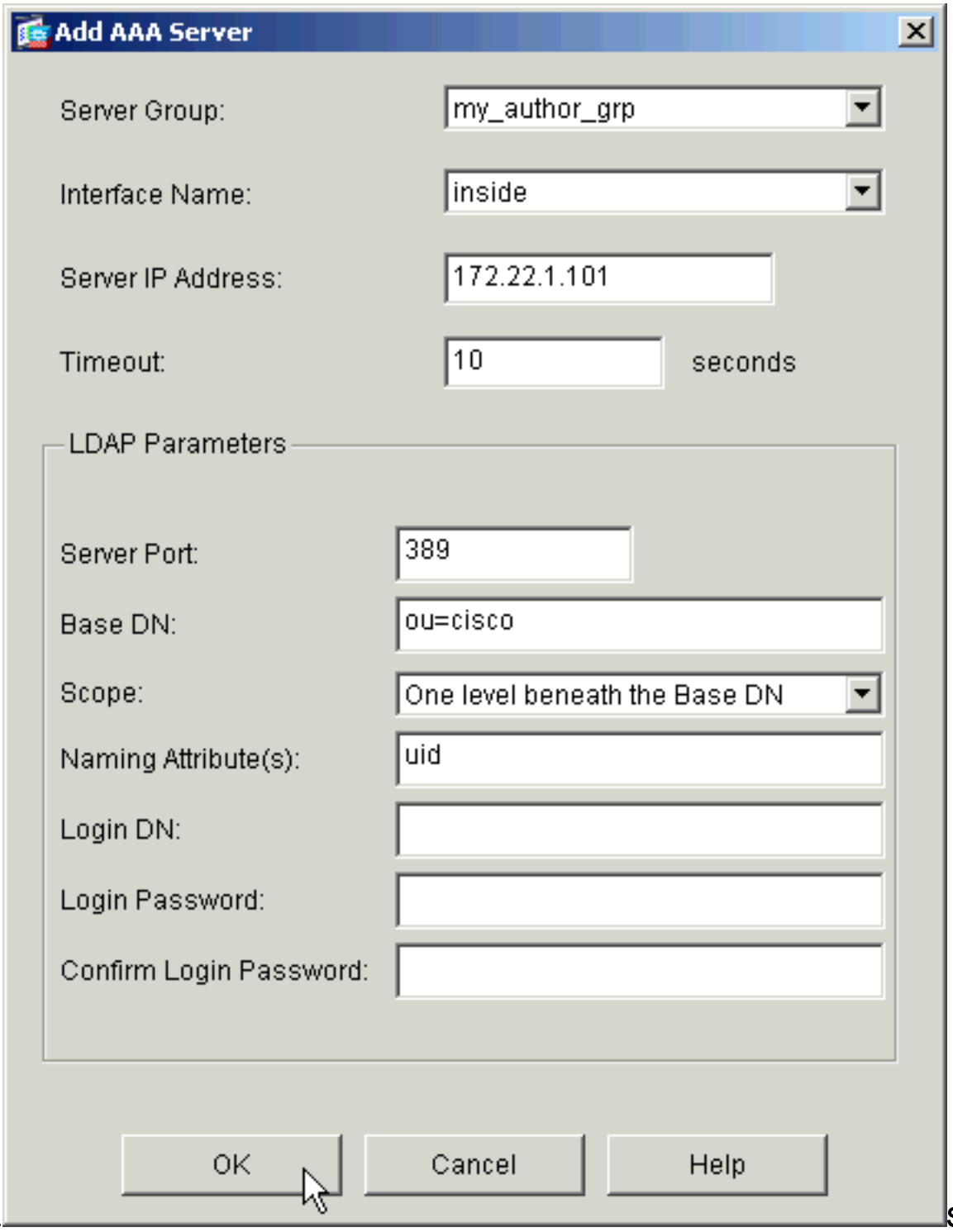


7. Konfigurieren Sie einen Authentifizierungsserver. Klicken Sie abschließend auf



OK.**Servergruppe**: Wählen Sie die in Schritt 2 konfigurierte Authentifizierungsservergruppe aus.**Interface Name** (Schnittstellenname): Wählen Sie die Schnittstelle aus, auf der sich der Server befindet.**Server IP Address (Server-IP-Adresse)**: Geben Sie die IP-Adresse des Authentifizierungsservers an.**Timeout** (Zeitüberschreitung): Geben Sie die maximale Zeit (in Sekunden) an, um auf eine Antwort vom Server zu warten.**Kerberos-Parameter:Server Port** - 88 ist der Standardport für Kerberos.**Retry Interval (Wiederholintervall wiederholen)**: Wählen Sie das gewünschte Wiederholungsintervall aus.**Kerberos Realm**: Geben Sie den Namen Ihres Kerberos-Bereichs ein. Dies ist häufig der Windows-Domänenname in Großbuchstaben.

8. Konfigurieren Sie einen Autorisierungsserver. Klicken Sie abschließend auf



OK.**Servergruppe**: Wählen Sie die in Schritt 3 konfigurierte Autorisierungsservergruppe aus.**Interface Name** (Schnittstellenname): Wählen Sie die Schnittstelle aus, auf der sich der Server befindet.**Server IP Address (Server-IP-Adresse)**: Geben Sie die IP-Adresse des Autorisierungsservers an.**Timeout** (Zeitüberschreitung): Geben Sie die maximale Zeit (in Sekunden) an, um auf eine Antwort vom Server zu warten.**LDAP-Parameter:Server Port** - 389 ist der Standard-Port für LDAP.**Basis-DN** - Geben Sie den Speicherort in der LDAP-Hierarchie ein, an dem der Server nach Erhalt einer Autorisierungsanfrage suchen soll.**Scope** (**Umfang**): Wählen Sie aus, in welchem Umfang der Server nach Erhalt einer Autorisierungsanfrage die LDAP-Hierarchie durchsuchen soll.**Naming Attribute(s)** - Geben Sie die Attribute für den relativen Distinguished Name ein, durch die Einträge auf dem LDAP-Server eindeutig definiert sind. Allgemeine Namensattribute sind Common Name (cn) und User ID (uid).**Anmelde-DN** - Einige LDAP-Server, einschließlich des Microsoft Active Directory-Servers, erfordern, dass das Gerät einen Handshake über authentifizierte Bindung

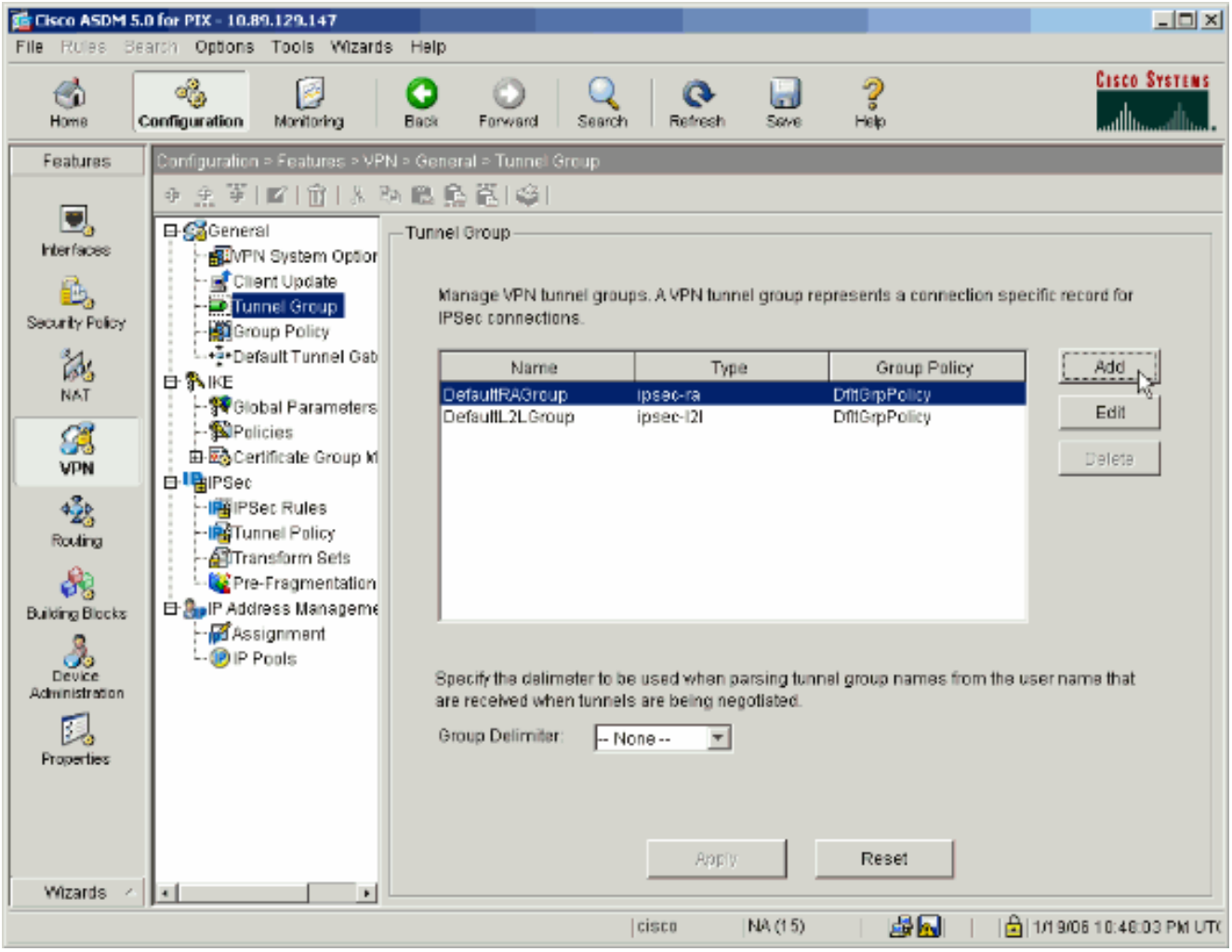
erstellt, bevor Anforderungen für andere LDAP-Operationen akzeptiert werden. Das Feld Login DN definiert die Authentifizierungsmerkmale des Geräts, die denen eines Benutzers mit Administratorberechtigungen entsprechen sollten. Zum Beispiel cn=administrator. Lassen Sie dieses Feld für den anonymen Zugriff leer.**Login Password** (Anmeldekennwort): Geben Sie das Kennwort für die Anmelde-DN ein.**Anmeldungskennwort bestätigen** - Bestätigen Sie das Kennwort für die Anmelde-DN.

9. Klicken Sie auf **Apply**, um die Änderungen nach Hinzufügen aller Authentifizierungs- und Autorisierungsserver an das Gerät zu senden.Wenn Sie dies konfiguriert haben, zeigt das PIX jetzt die Befehle an, die der aktuellen Konfiguration hinzugefügt werden.
10. Klicken Sie auf **Senden**, um die Befehle an das Gerät zu senden.

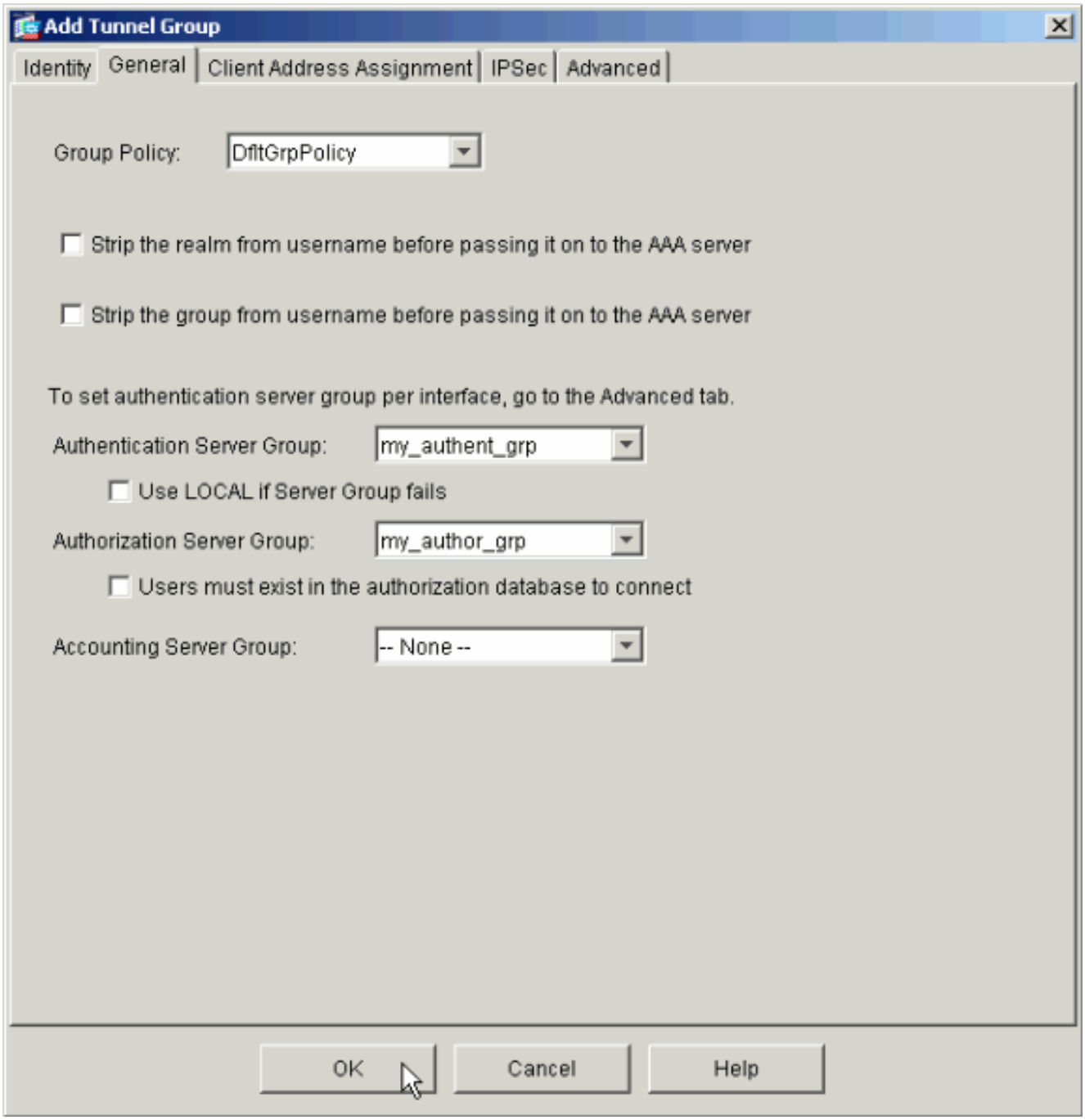
Konfigurieren einer VPN-Tunnel-Gruppe für Authentifizierung und Autorisierung

Gehen Sie wie folgt vor, um die soeben konfigurierten Servergruppen zu einer VPN-Tunnelgruppe hinzuzufügen.

1. Wählen Sie **Configuration > VPN > Tunnel Group**, und klicken Sie auf **Add**, um eine neue Tunnelgruppe zu erstellen, oder **Edit**, um eine vorhandene Gruppe zu ändern.



2. Wählen Sie auf der Registerkarte Allgemein des sich öffnenden Fensters die zuvor konfigurierten Servergruppen aus.



3. *Optional:* Konfigurieren Sie die verbleibenden Parameter auf den anderen Registerkarten, wenn Sie eine neue Tunnelgruppe hinzufügen.
4. Klicken Sie abschließend auf **OK**.
5. Klicken Sie auf **Apply**, um die Änderungen nach Abschluss der Tunnelgruppenkonfiguration an das Gerät zu senden.Wenn Sie dies konfiguriert haben, zeigt das PIX jetzt die Befehle an, die der aktuellen Konfiguration hinzugefügt werden.
6. Klicken Sie auf **Senden**, um die Befehle an das Gerät zu senden.

Konfigurieren der Authentifizierung und Autorisierung für VPN-Benutzer mithilfe der CLI

Dies ist die entsprechende CLI-Konfiguration für die Authentifizierungs- und Autorisierungsservergruppen für VPN-Benutzer.

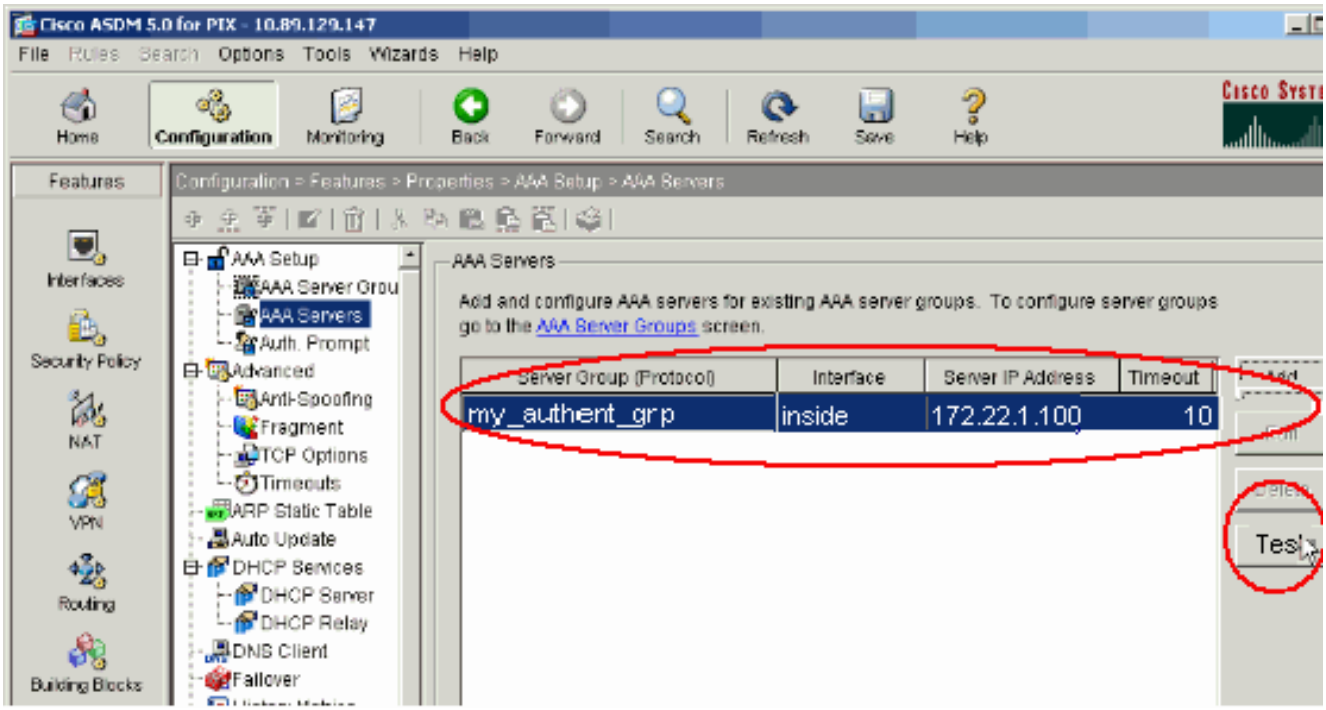
CLI-Konfiguration der Security Appliance

```
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.
```

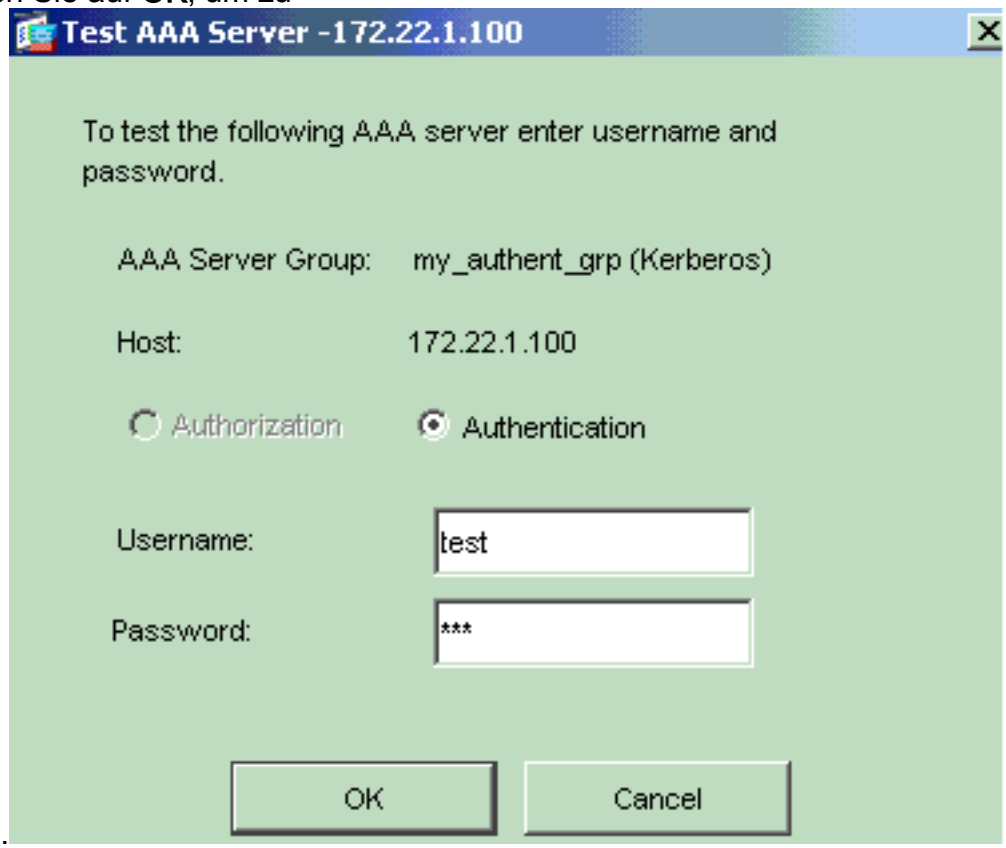
Überprüfen

Gehen Sie wie folgt vor, um die Benutzerauthentifizierung zwischen dem PIX/ASA- und dem AAA-Server zu überprüfen:

1. Wählen Sie **Configuration > Properties > AAA Setup > AAA Servers**, und wählen Sie die Servergruppe (my_authent_grp) aus. Klicken Sie anschließend auf **Test**, um die Benutzeranmeldeinformationen zu validieren.

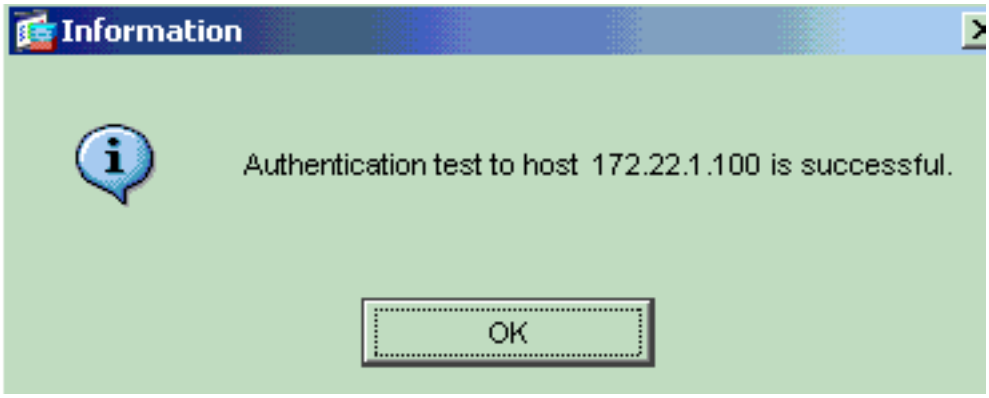


2. Geben Sie Benutzername und Kennwort ein (z. B. Benutzername: Test und Kennwort: Test), und klicken Sie auf **OK**, um zu



validieren.

3. Sie sehen, dass die Authentifizierung erfolgreich

ist. 

Fehlerbehebung

1. Eine häufige Ursache für Authentifizierungsfehler ist die Zeitdifferenz. Stellen Sie sicher, dass die Uhren auf dem PIX oder ASA und Ihr Authentifizierungsserver synchronisiert sind.Wenn die Authentifizierung aufgrund von "Clock Skew" fehlschlägt, können Sie die folgende Fehlermeldung erhalten: `:- FEHLER: Authentifizierung abgelehnt: Die Zeitdifferenz beträgt mehr als 300 Sekunden..` Diese Protokollmeldung wird ebenfalls angezeigt:`%PIX|ASA-3-113020: Kerberos-Fehler: Zeitdifferenz mit Server ip_address größer als 300 Sekunden ip_address`: Die IP-Adresse des Kerberos-Servers.Diese Meldung wird angezeigt, wenn die Authentifizierung für einen IPSec- oder WebVPN-Benutzer über einen Kerberos-Server fehlschlägt, da die Uhren auf der Sicherheits-Appliance und dem Server mehr als fünf Minuten (300 Sekunden) voneinander entfernt sind. In diesem Fall wird der Verbindungsversuch zurückgewiesen.Um dieses Problem zu beheben, synchronisieren Sie die Uhren auf der Sicherheits-Appliance und dem Kerberos-Server.
2. Die Vorauthentifizierung im Active Directory (AD) muss deaktiviert werden, oder sie kann zu Fehlern bei der Benutzerauthentifizierung führen.
3. VPN-Client-Benutzer können sich nicht anhand des Microsoft-Zertifikatsservers authentifizieren. Diese Fehlermeldung wird angezeigt:`"Error Processing Payload" (Fehler bei der Verarbeitung der Payload) (Fehler 14)` Um dieses Problem zu beheben, deaktivieren Sie das Kontrollkästchen **keine Kerberose-Vorauthentifizierung** auf dem Authentifizierungsserver.

Zugehörige Informationen

- Konfigurieren von AAA-Servern und der lokalen Datenbank
- Produkt-Support für Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems