PIX/ASA: Esempio di configurazione dell'autenticazione Kerberos e dei gruppi di server di autorizzazione LDAP per utenti client VPN tramite ASDM/CLI

Sommario

Introduzione

In questo documento viene descritto come usare Cisco Adaptive Security Device Manager (ASDM) per configurare i gruppi di server di autenticazione Kerberos e autorizzazione LDAP sull'appliance di sicurezza Cisco PIX serie 500. In questo esempio, i gruppi di server vengono utilizzati dai criteri di un gruppo di tunnel VPN per autenticare e autorizzare gli utenti in ingresso.

Prerequisiti

Requisiti

In questo documento si presume che il PIX sia completamente operativo e configurato per consentire all'ASDM di apportare modifiche alla configurazione.

Nota: per consentire la configurazione del PIX da parte di ASDM, consultare il documento sulla concessione dell'accesso HTTPS per ASDM.

Componenti usati

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

- Software Cisco PIX Security Appliance versione 7.x e successive
- Cisco ASDM versione 5.x e successive

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.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco Adaptive Security Appliance (ASA) versione 7.x.

Convenzioni

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

Premesse

Non tutti i possibili metodi di autenticazione e autorizzazione disponibili nel software PIX/ASA 7.x sono supportati quando si ha a che fare con utenti VPN. In questa tabella vengono descritti i metodi disponibili per gli utenti VPN:

	Locale	RAGGIO	TACACS+	SDI	NT	Kerberos	LDAP
Autenticazione	Sì	Sì	Sì	Sì	Sì	Sì	No
Authorization	Sì	Sì	No	No	No	No	Sì

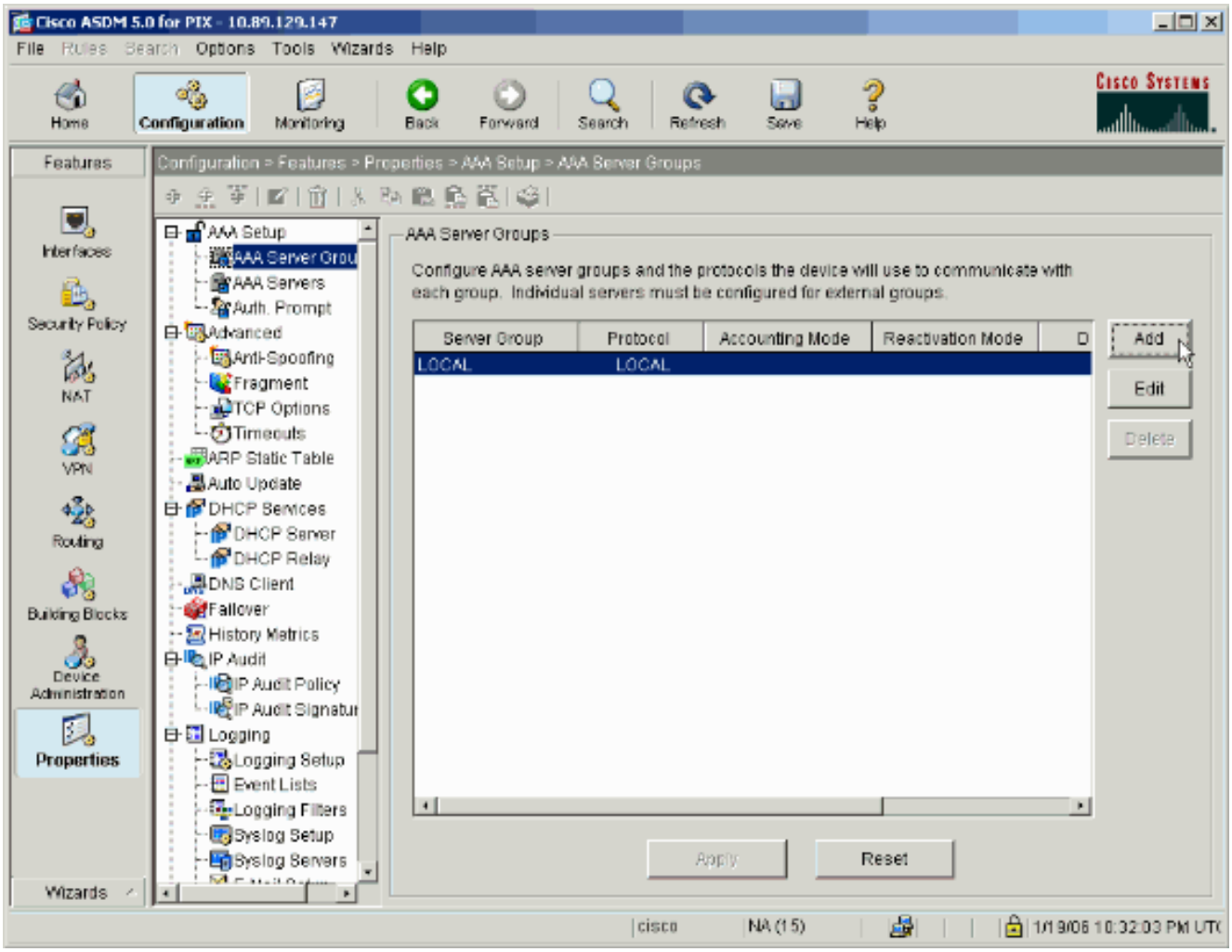
Nota: Kerberos viene utilizzato per l'autenticazione e LDAP per l'autorizzazione degli utenti VPN in questo esempio.

Configurazione dell'autenticazione e dell'autorizzazione per gli utenti VPN tramite ASDM

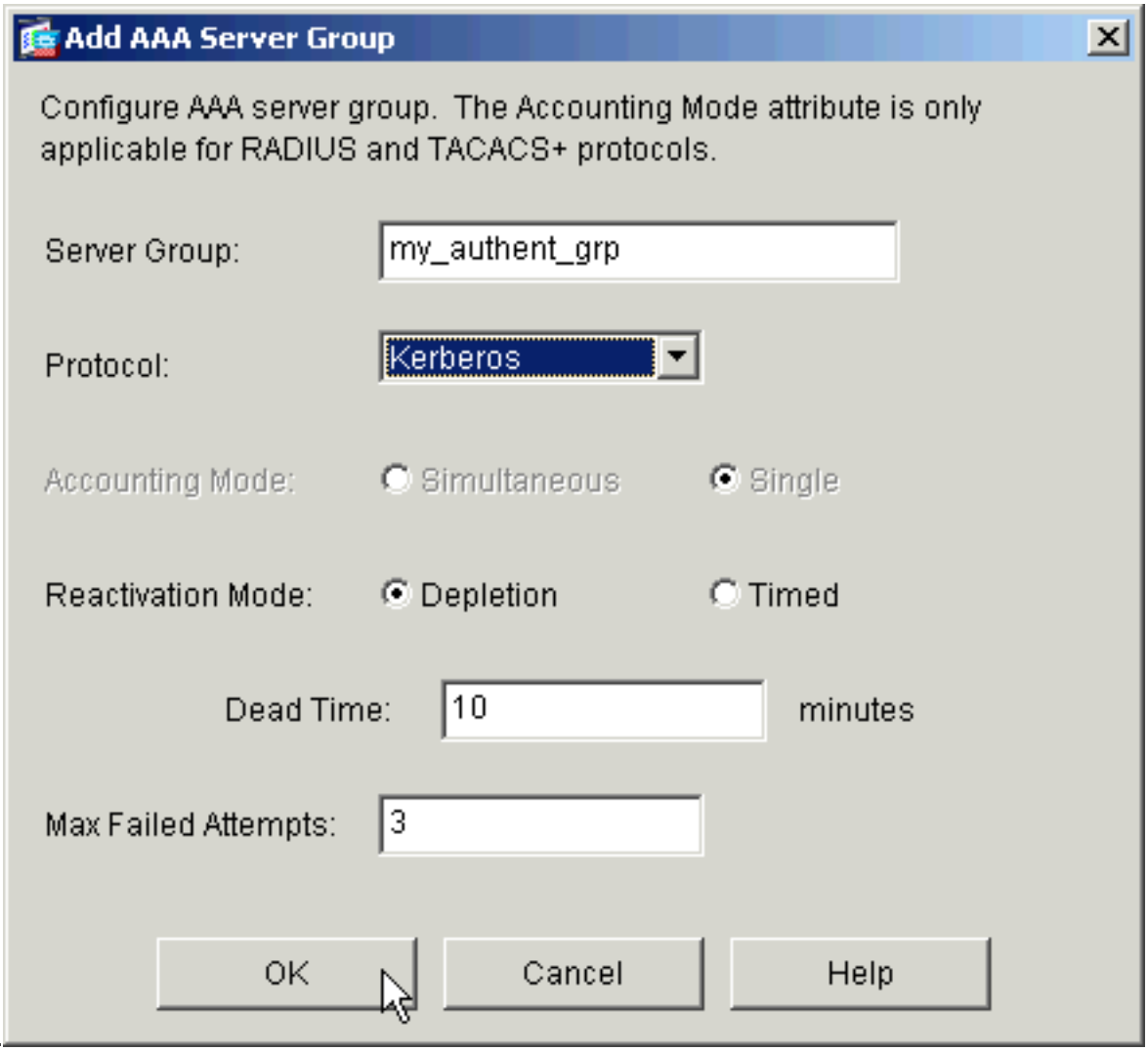
Configura server di autenticazione e autorizzazione

Completare questa procedura per configurare i gruppi di server di autenticazione e autorizzazione per gli utenti VPN tramite ASDM.

1. Scegliere **Configurazione > Proprietà > Impostazione AAA > Gruppi di server AAA**, quindi fare clic su
Aggiungi.

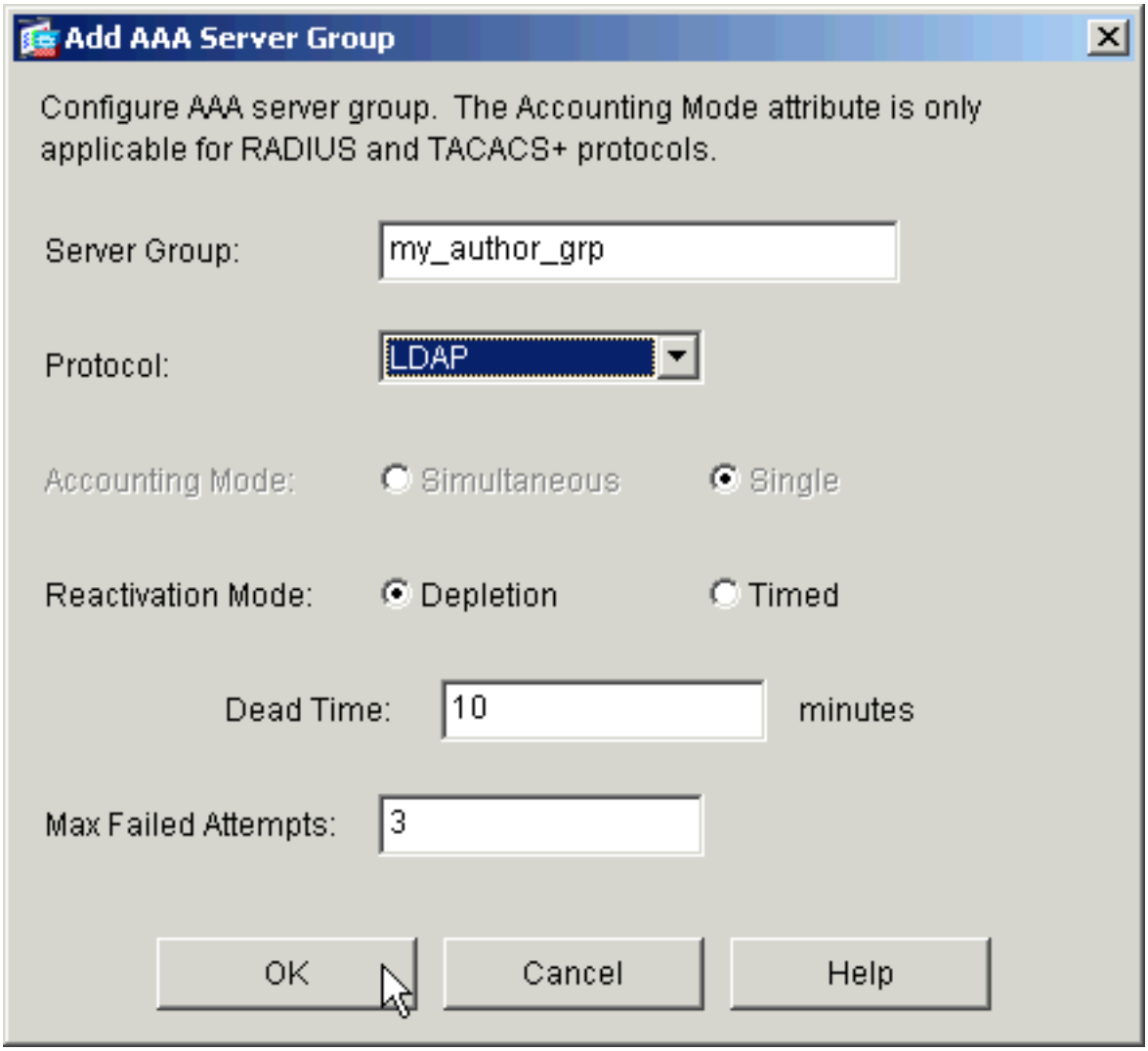


2. Definire un nome per il nuovo gruppo di server di autenticazione e scegliere un protocollo.L'opzione Modalità accounting è disponibile solo per RADIUS e TACACS+. Al termine, fare clic su

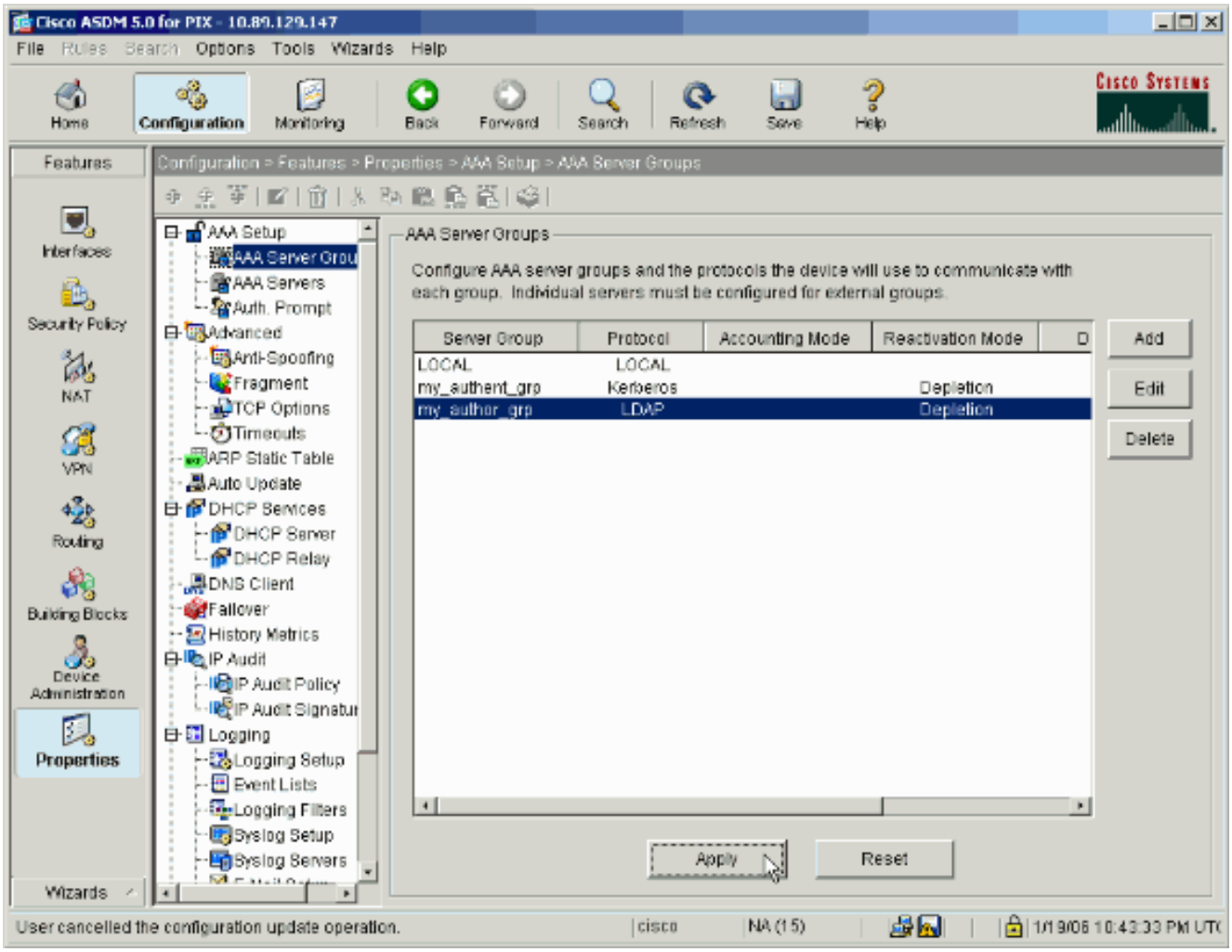


OK.

3. Ripetere i passaggi 1 e 2 per creare un nuovo gruppo di server di autorizzazione.

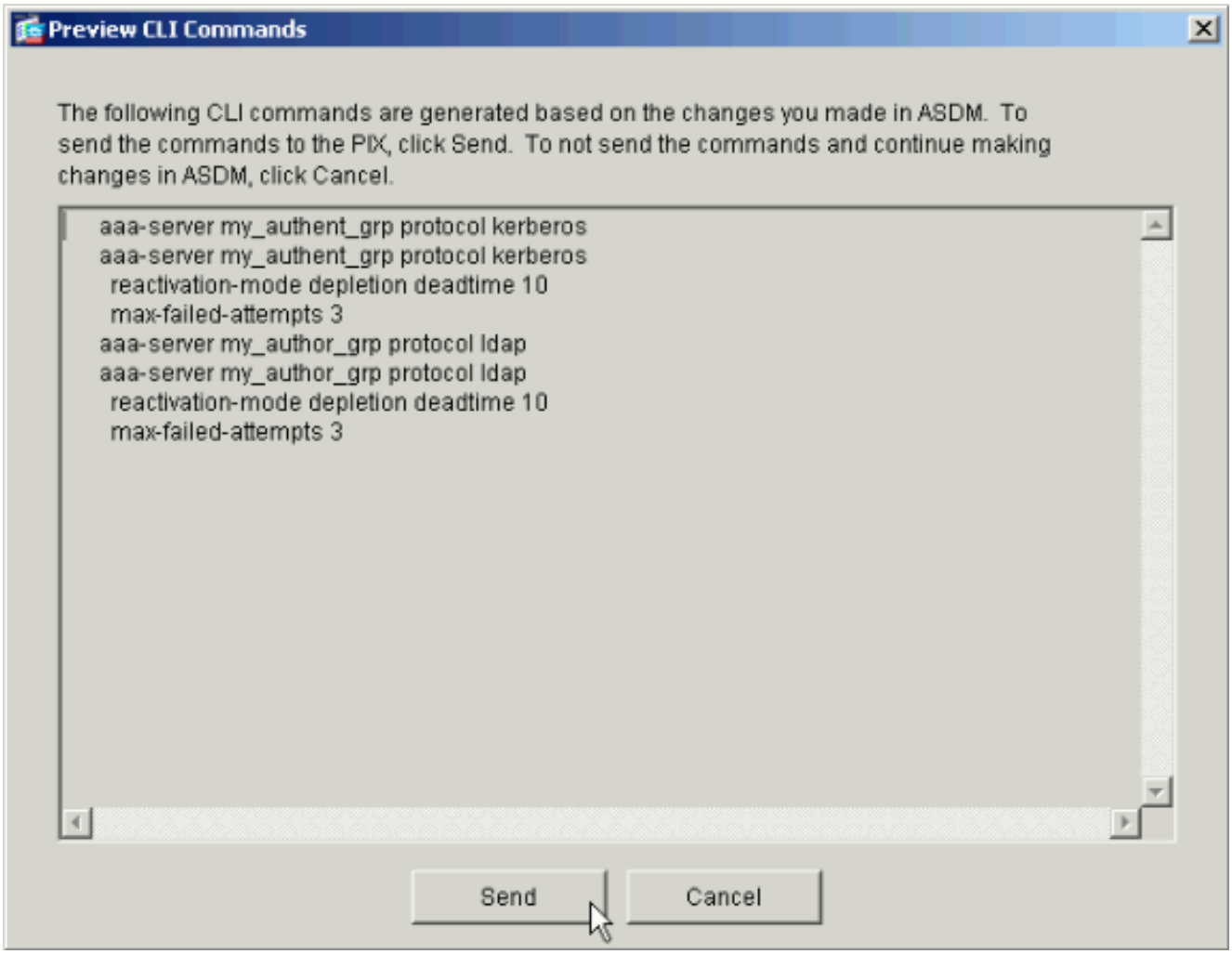


4. Per inviare le modifiche al dispositivo, fare clic su **Apply** (Applica).



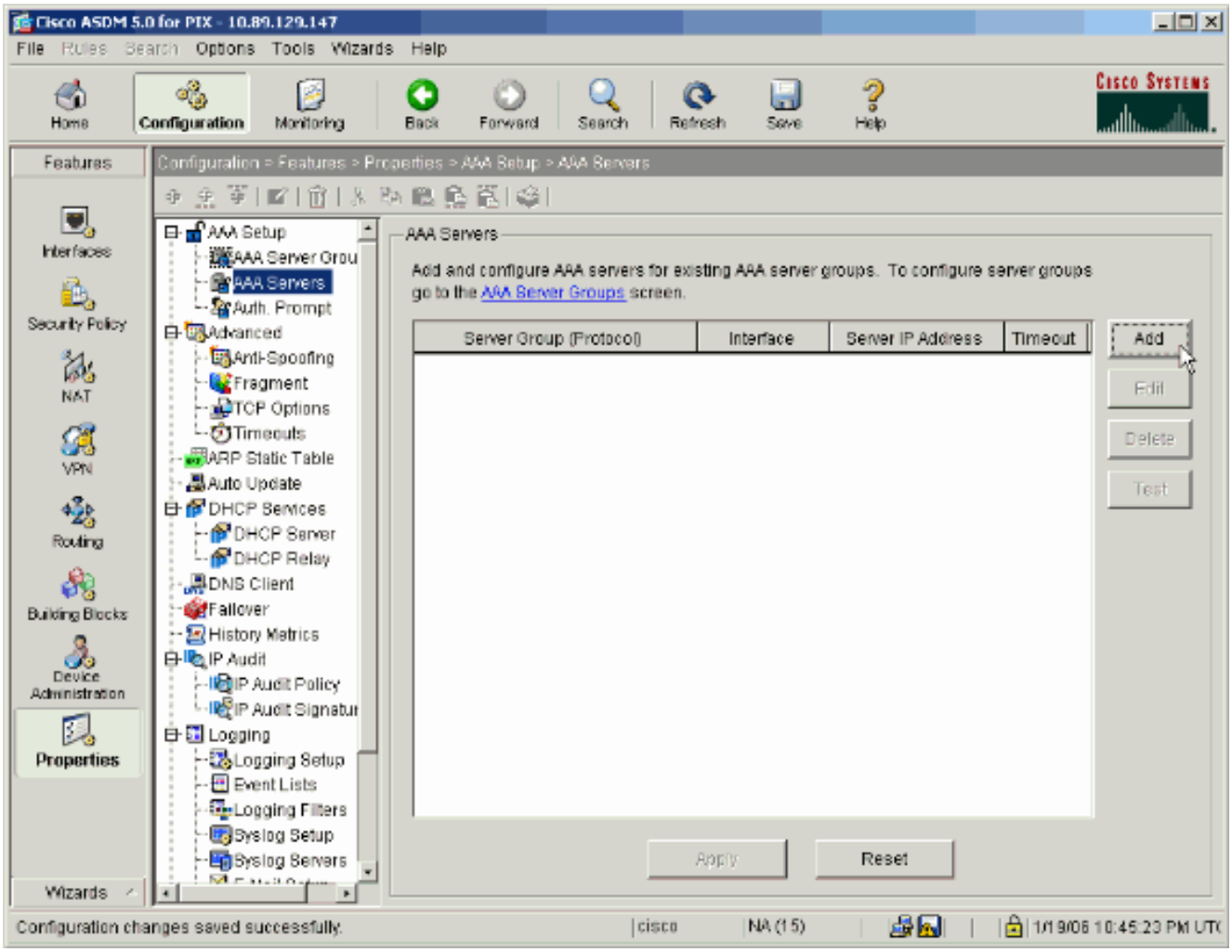
Se è stato configurato per tale operazione, il dispositivo visualizza ora in anteprima i comandi aggiunti alla configurazione in esecuzione.

5. Per inviare i comandi al dispositivo, fare clic su **Send**.

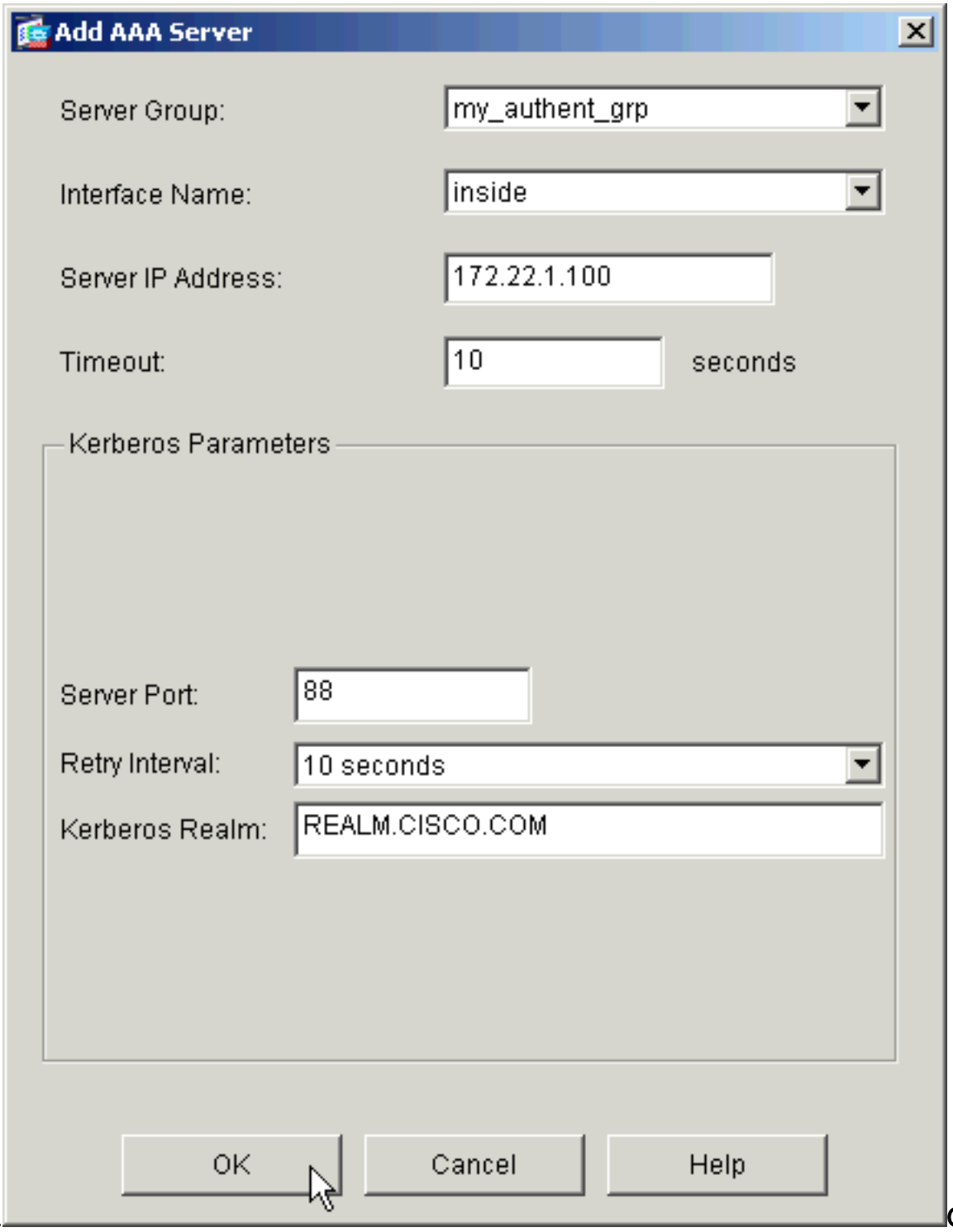


I gruppi di server appena creati devono ora essere popolati con server di autenticazione e autorizzazione.

6. Scegliere **Configurazione > Proprietà > Impostazione AAA > Server AAA**, quindi fare clic su **Aggiungi**.

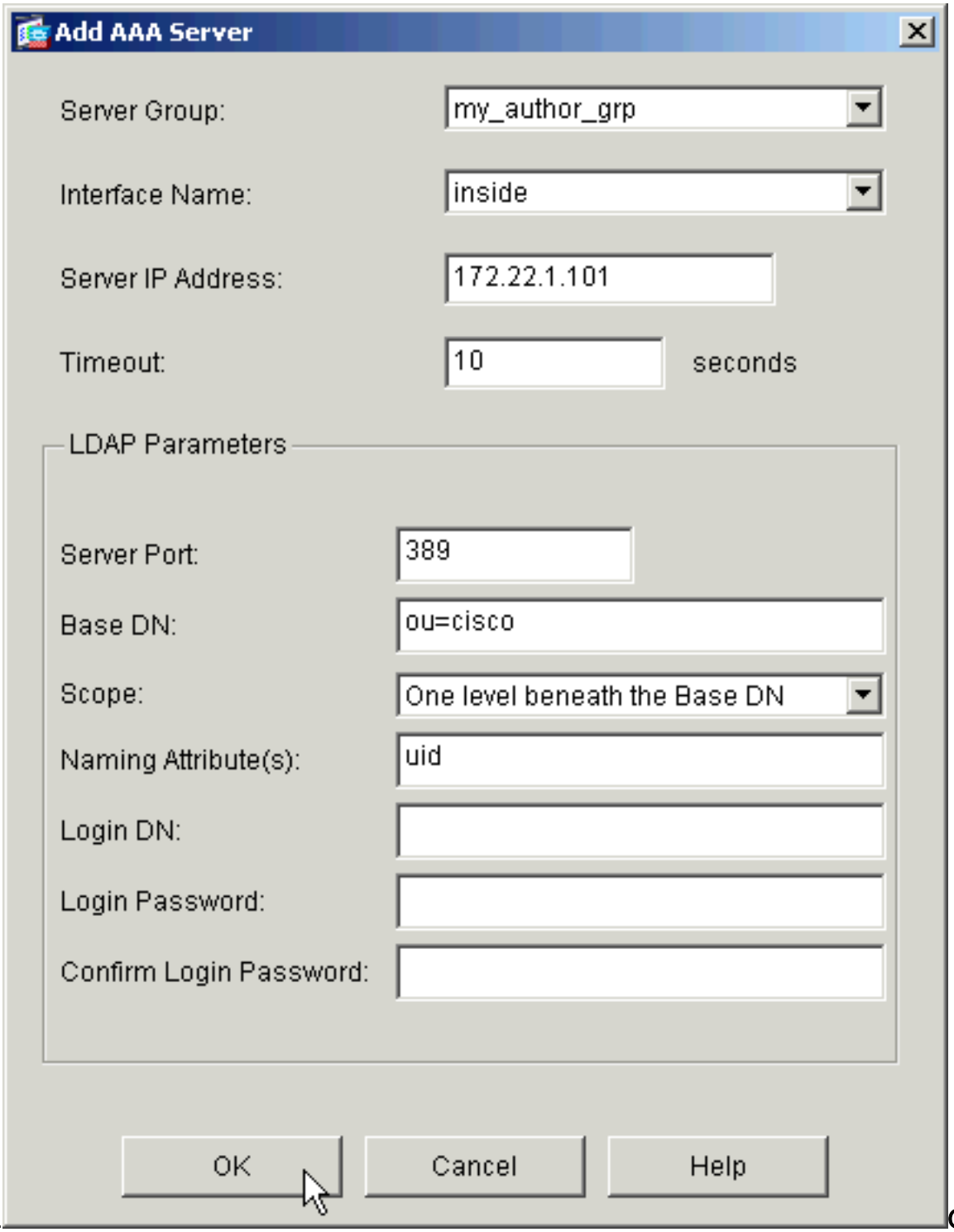


7. Configurare un server di autenticazione. Al termine, fare clic su



OK.**Gruppo server**: scegliere il gruppo di server di autenticazione configurato nel passaggio 2.**Nome interfaccia (Interface Name)** - Consente di scegliere l'interfaccia su cui risiede il server.**Indirizzo IP server**: specificare l'indirizzo IP del server di autenticazione.**Timeout**: specificare il tempo massimo, in secondi, di attesa per una risposta dal server.**Parametri Kerberos:Porta server**—88 è la porta standard per Kerberos.**Intervallo tentativi (Retry Interval)** - Consente di scegliere l'intervallo dei tentativi desiderato.**Realm Kerberos**: immettere il nome dell'area di autenticazione Kerberos. Si tratta spesso del nome di dominio di Windows in lettere maiuscole.

8. Configurare un server di autorizzazione. Al termine, fare clic su



OK.**Gruppo server**: scegliere il gruppo di server di autorizzazione configurato nel passaggio 3.**Nome interfaccia (Interface Name)** - Consente di scegliere l'interfaccia su cui risiede il server.**Indirizzo IP server**: specificare l'indirizzo IP del server di autorizzazione.**Timeout**: specificare il tempo massimo, in secondi, di attesa per una risposta dal server.**Parametri LDAP:Porta server (Server Port)** - 389 è la porta di default per LDAP.**DN di base**: immettere la posizione nella gerarchia LDAP in cui il server deve iniziare la ricerca dopo aver ricevuto una richiesta di autorizzazione.**Ambito**: scegliere l'estensione in base alla quale il server deve eseguire la ricerca nella gerarchia LDAP dopo aver ricevuto una richiesta di autorizzazione.**Attributi di denominazione**: immettere gli attributi Nome distinto relativo in base ai quali le voci sul server LDAP sono definite in modo univoco. Gli attributi di denominazione comuni sono il nome comune (cn) e l'ID utente (uid).**DN accesso**: alcuni server LDAP, incluso il server Microsoft Active Directory, richiedono al dispositivo di stabilire un handshake tramite binding autenticato prima di accettare richieste per altre operazioni

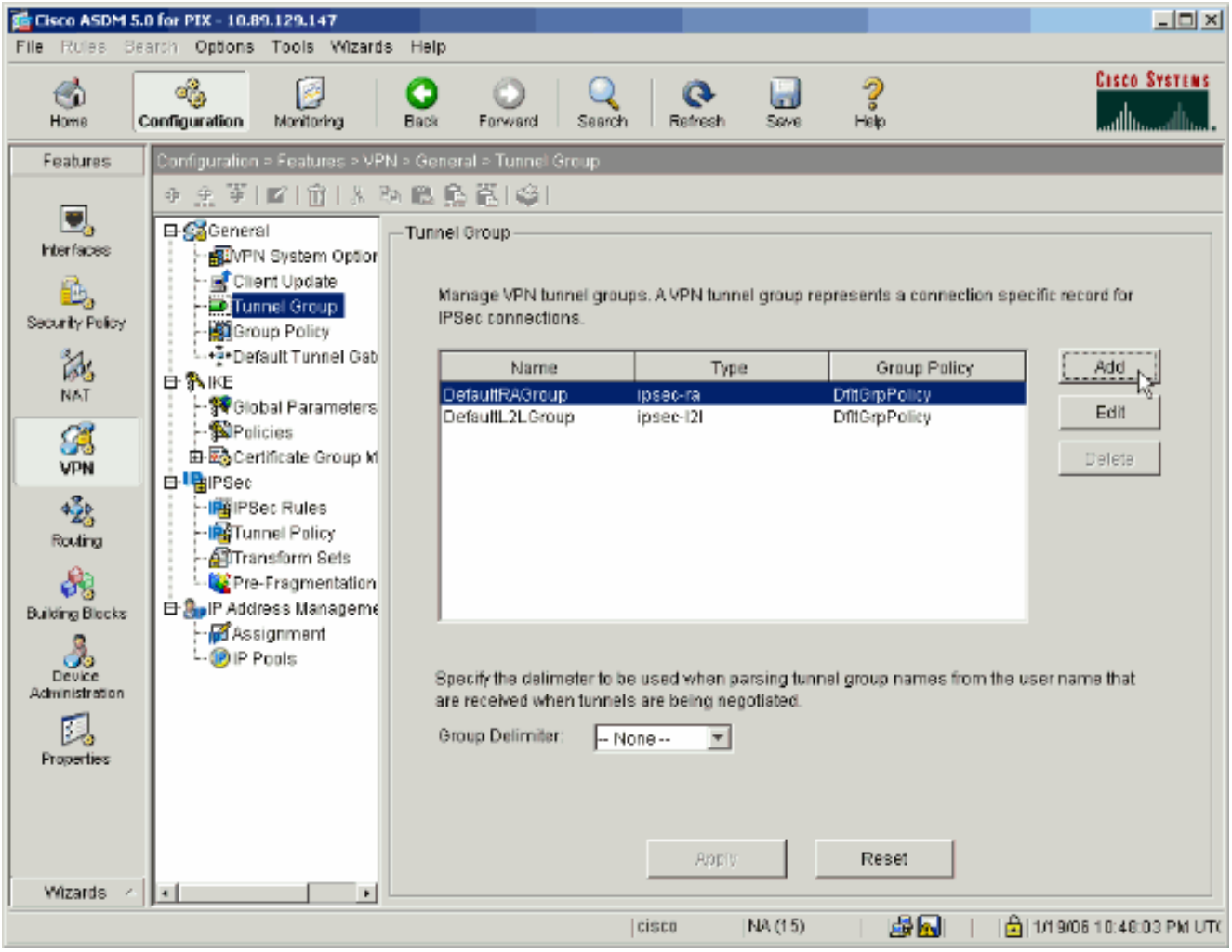
LDAP. Il campo DN di accesso definisce le caratteristiche di autenticazione del dispositivo, che devono corrispondere a quelle di un utente con privilegi amministrativi. Ad esempio, cn=administrator. Per l'accesso anonimo, lasciare vuoto questo campo.**Password di login**: immettere la password per il DN di login.**Conferma password di accesso**: conferma la password per il DN di accesso.

9. Fare clic su **Apply** (Applica) per inviare le modifiche al dispositivo dopo l'aggiunta di tutti i server di autenticazione e autorizzazione.Se è stato configurato per tale operazione, PIX visualizza ora in anteprima i comandi aggiunti alla configurazione in esecuzione.
10. Per inviare i comandi al dispositivo, fare clic su **Send**.

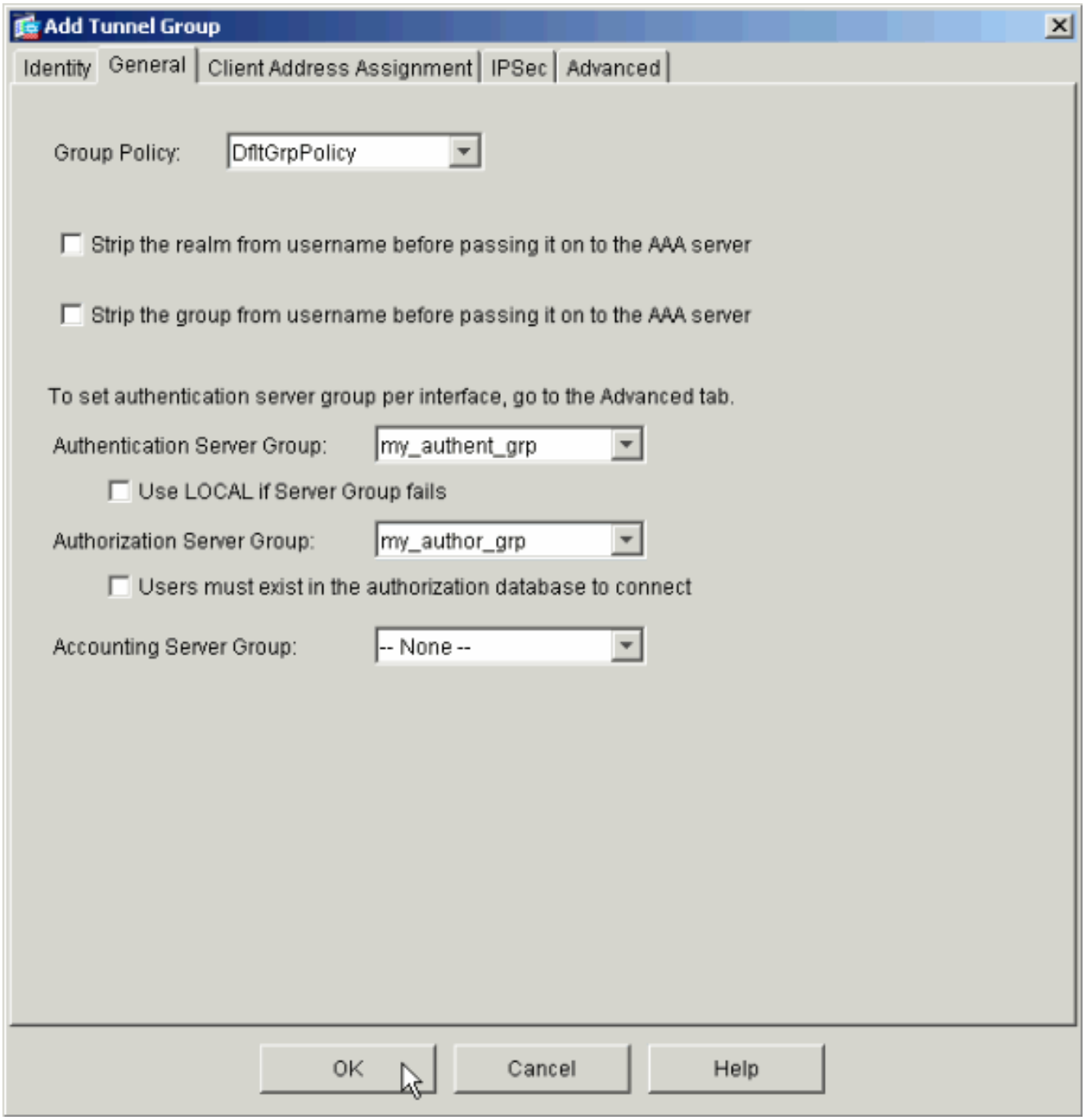
Configurare un gruppo di tunnel VPN per l'autenticazione e l'autorizzazione

Completare questa procedura per aggiungere i gruppi di server appena configurati a un gruppo di tunnel VPN.

1. Scegliere **Configurazione > VPN > Gruppo di tunnel** e fare clic su **Aggiungi** per creare un nuovo gruppo di tunnel oppure su **Modifica** per modificare un gruppo esistente.



2. Nella scheda Generale della finestra visualizzata, selezionare i gruppi di server configurati in precedenza.



3. *Facoltativo:* Configurare i parametri rimanenti nelle altre schede se si aggiunge un nuovo gruppo di tunnel.
4. Al termine, fare clic su **OK**.
5. Fare clic su **Apply** (Applica) per inviare le modifiche al dispositivo dopo aver completato la configurazione del gruppo di tunnel.Se è stato configurato per tale operazione, PIX visualizza ora in anteprima i comandi aggiunti alla configurazione in esecuzione.
6. Per inviare i comandi al dispositivo, fare clic su **Send**.

Configurazione dell'autenticazione e dell'autorizzazione per gli utenti VPN tramite CLI

Questa è la configurazione CLI equivalente per i gruppi di server di autenticazione e autorizzazione per gli utenti VPN.

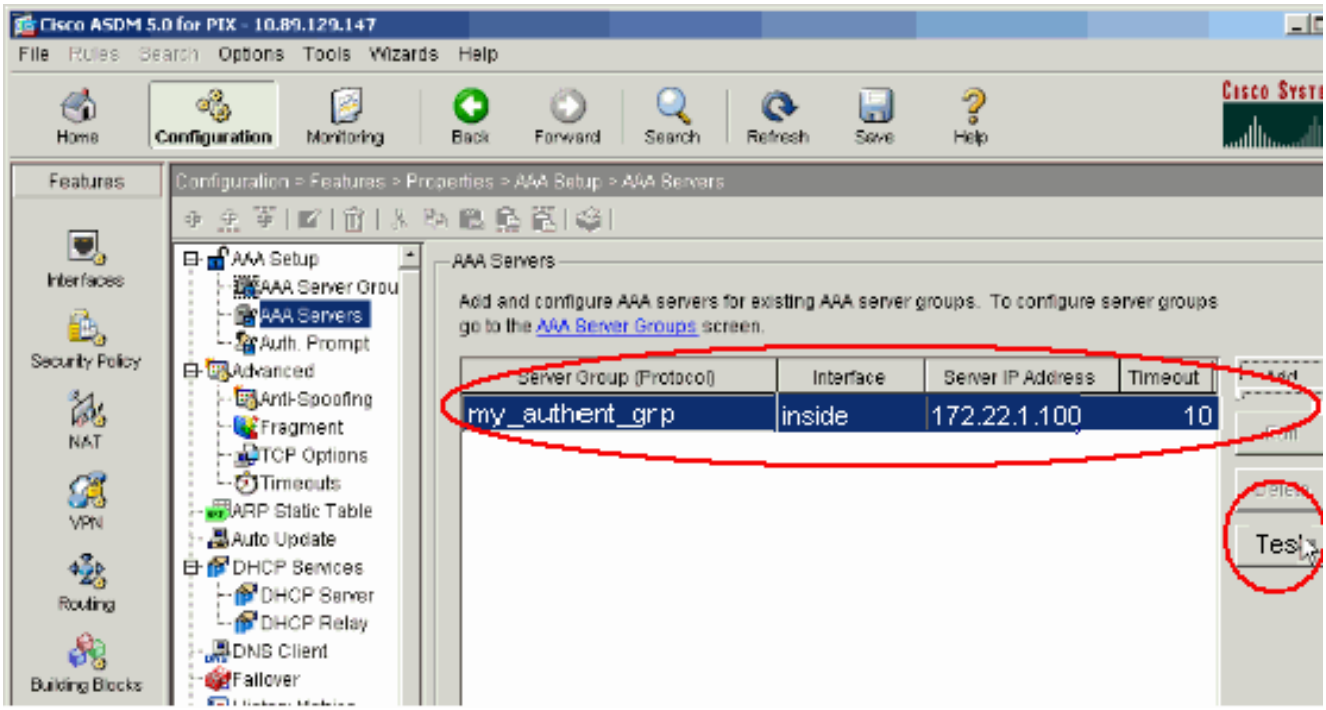
Configurazione CLI di Security Appliance

```
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.
```

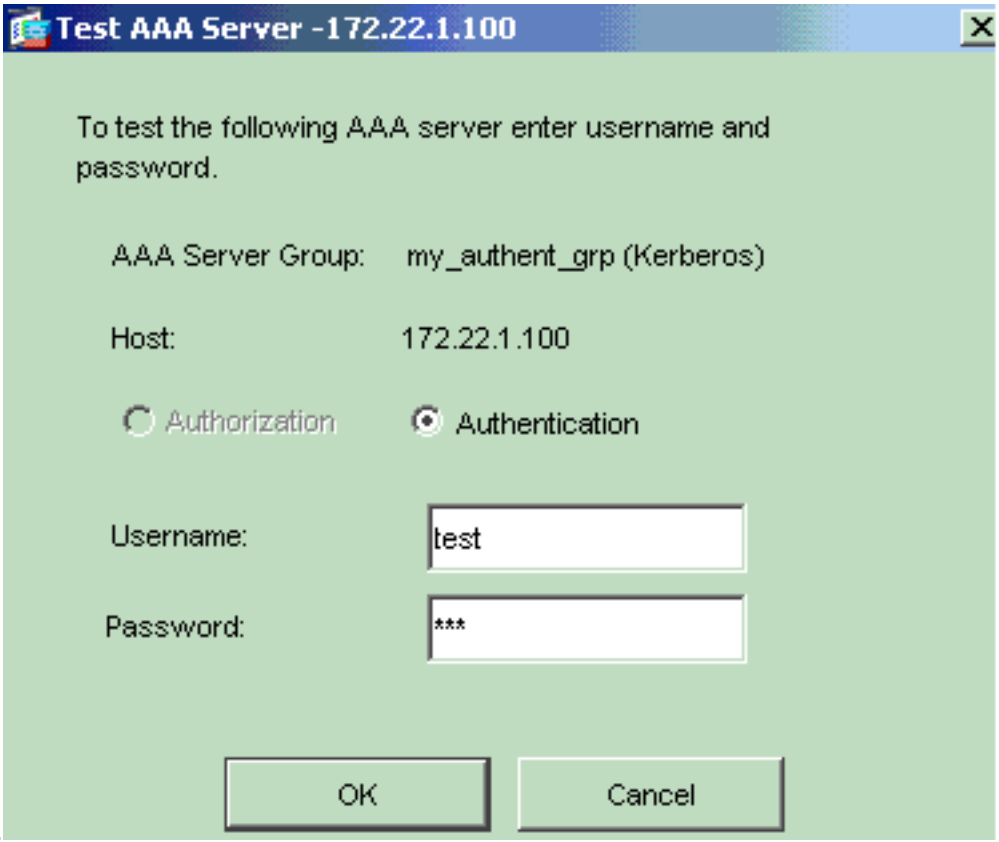
Verifica

Completare questa procedura per verificare l'autenticazione dell'utente tra il server PIX/ASA e il server AAA:

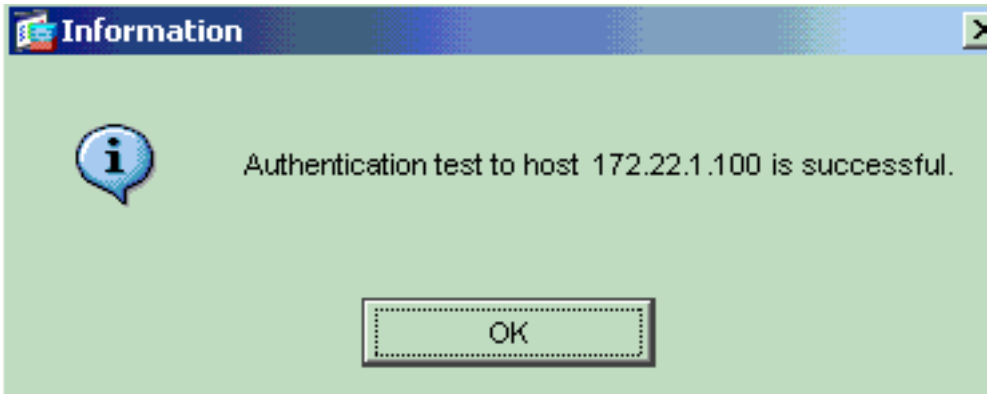
1. Scegliere **Configurazione > Proprietà > Impostazione AAA > Server AAA**, quindi selezionare il gruppo di server (my_authent_grp). Quindi fare clic su **Test** per convalidare le credenziali dell'utente.



2. Fornire il nome utente e la password (ad esempio, nome utente: test e password: test) e fare clic su **OK** per convalidare.



3. L'autenticazione ha esito

positivo. 

Risoluzione dei problemi

1. Una causa frequente degli errori di autenticazione è lo sfasamento dell'orologio. Accertarsi quindi che gli orologi del PIX o dell'ASA e del server di autenticazione siano sincronizzati.Quando l'autenticazione non riesce a causa dell'inclinazione dell'orologio, è possibile ricevere questo messaggio di errore: `:- ERRORE: Autenticazione rifiutata: Inclinazione dell'orologio maggiore di 300 secondi.`. Viene inoltre visualizzato il seguente messaggio di registro:`%PIX|ASA-3-113020: Errore Kerberos: Sfasamento dell'orologio con indirizzo_ip del server maggiore di 300 secondi ip_address`: l'indirizzo IP del server Kerberos.Questo messaggio viene visualizzato quando l'autenticazione di un utente IPSec o WebVPN tramite un server Kerberos ha esito negativo a causa di una differenza di tempo tra gli orologi dell'accessorio di protezione e del server di più di cinque minuti (300 secondi). In questo caso, il tentativo di connessione viene rifiutato.Per risolvere il problema, sincronizzare gli orologi dell'accessorio di protezione e del server Kerberos.
2. È necessario disabilitare la preautenticazione in Active Directory (AD) oppure potrebbe verificarsi un errore di autenticazione utente.
3. Gli utenti del client VPN non sono in grado di eseguire l'autenticazione sul server certificati Microsoft. Viene visualizzato questo messaggio di errore:`"Errore durante l'elaborazione del payload" (Errore 14)` Per risolvere il problema, deselezionare la casella di controllo **Non richiedere preautenticazione kerberosa** nel server di autenticazione.

Informazioni correlate

- Configurazione dei server AAA e del database locale
- Cisco ASA serie 5500 Adaptive Security Appliance - Supporto dei prodotti
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems