PIX/ASA: Autenticação de Kerberos e de servidor de autorização LDAP grupos para usuários de cliente VPN através do exemplo de configuração ASDM/CLI

Índice

Introdução

Este documento descreve como usar o Cisco Adaptive Security Device Manager (ASDM) para configurar a autenticação de Kerberos e os grupos de servidor de autorização LDAP na ferramenta de segurança da série do Cisco PIX 500. Neste exemplo, os grupos de servidor são usados pela política de um grupo de túneis VPN para autenticar e autorizar novos usuários.

Pré-requisitos

Requisitos

Este documento supõe o PIX é plenamente operacional e configurado para permitir que o ASDM faça alterações de configuração.

Nota: Refira permitir o acesso HTTPS para o ASDM a fim permitir que o PIX seja configurado pelo ASDM.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de software 7.x da ferramenta de segurança de Cisco PIX e mais tarde
- Versão ASDM Cisco 5.x e mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada com versão 7.x adaptável da ferramenta de segurança de Cisco (ASA).

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Não todos os métodos de authentication e autorização possíveis disponíveis no software PIX/ASA 7.x são apoiados quando você trata os usuários VPN. Esta tabela detalha que métodos estão disponíveis para usuários VPN:

	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
Autenticação	Sim	Sim	Sim	Sim	Sim	Sim	Não
Autorização	Sim	Sim	Não	Não	Não	Não	Sim

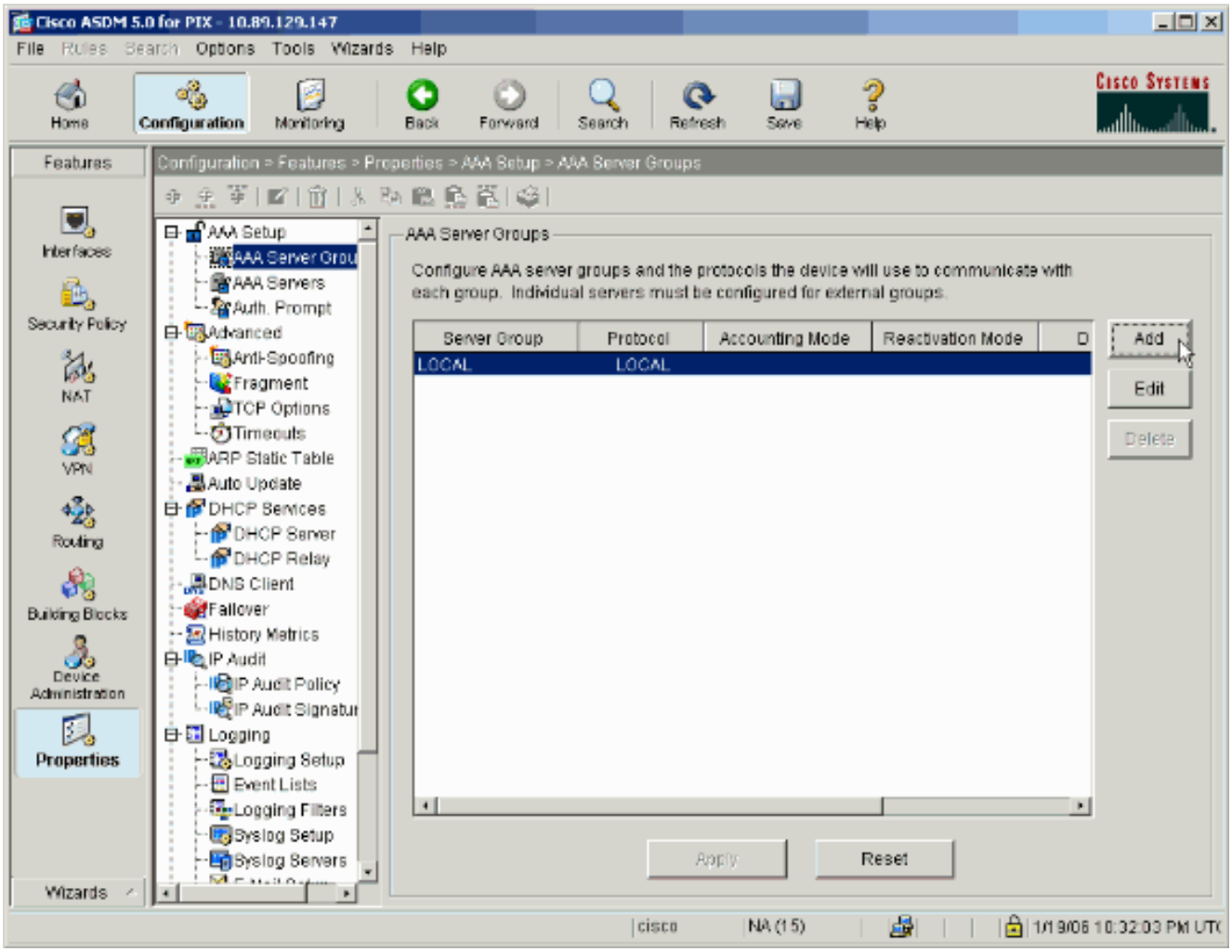
Nota: O Kerberos é usado para a autenticação e o LDAP é usado para a autorização de usuários VPN neste exemplo.

Configurar a authentication e autorização para os usuários VPN que usam o ASDM

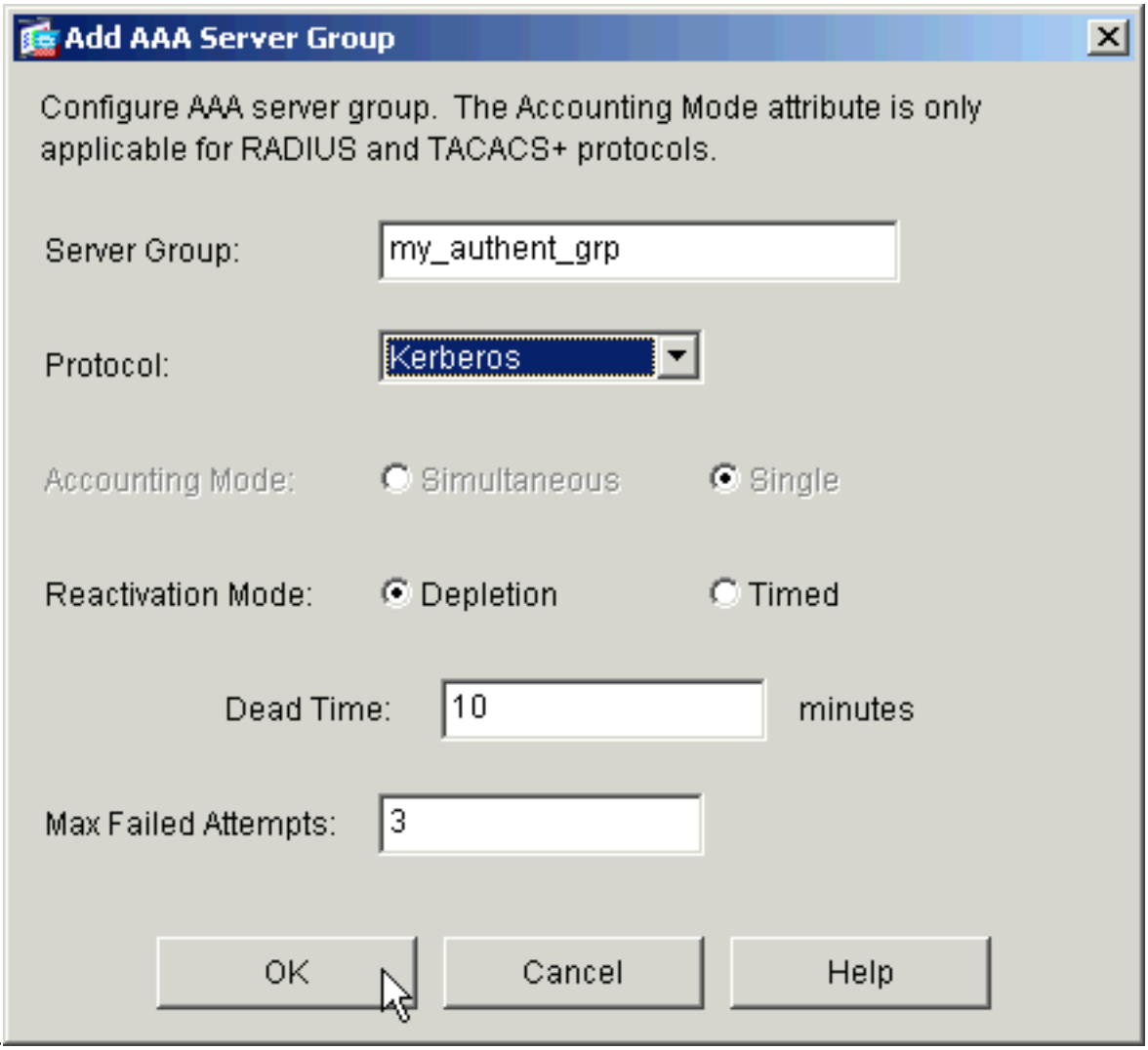
Configurar server da authentication e autorização

Termine estas etapas a fim configurar grupos de servidor da authentication e autorização para usuários VPN com o ASDM.

1. Escolha a **configuração > as propriedades > o AAA Setup > Grupos de servidores AAA**, e o clique
adiciona.

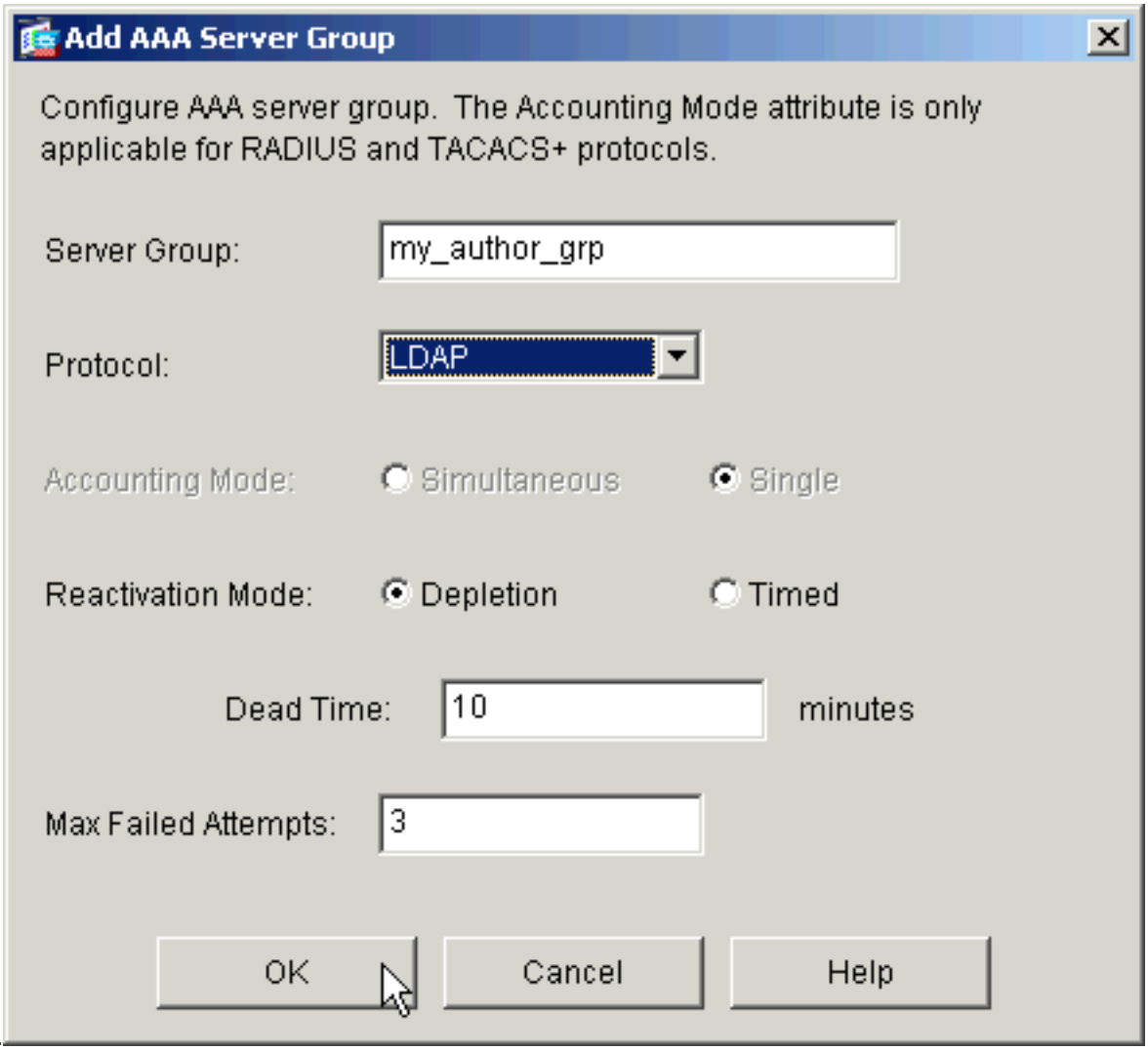


2. Defina um nome para o grupo de Authentication Server novo, e escolha um protocolo.A opção do modo da contabilidade é para o RAIO e o TACACS+ somente. **APROVAÇÃO do** clique quando você for



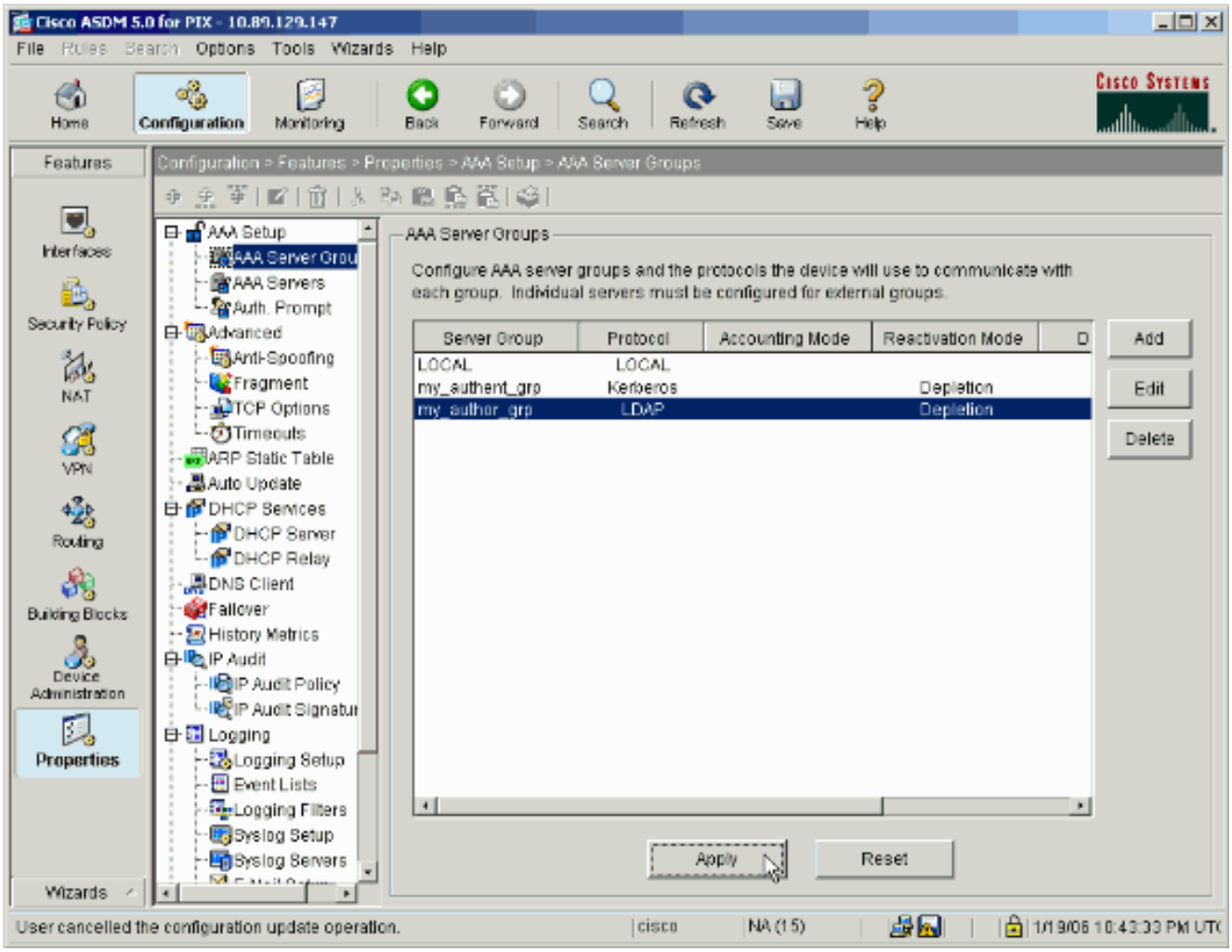
feito.

3. Repita etapas 1 e 2 a fim criar um grupo de servidor de autorização



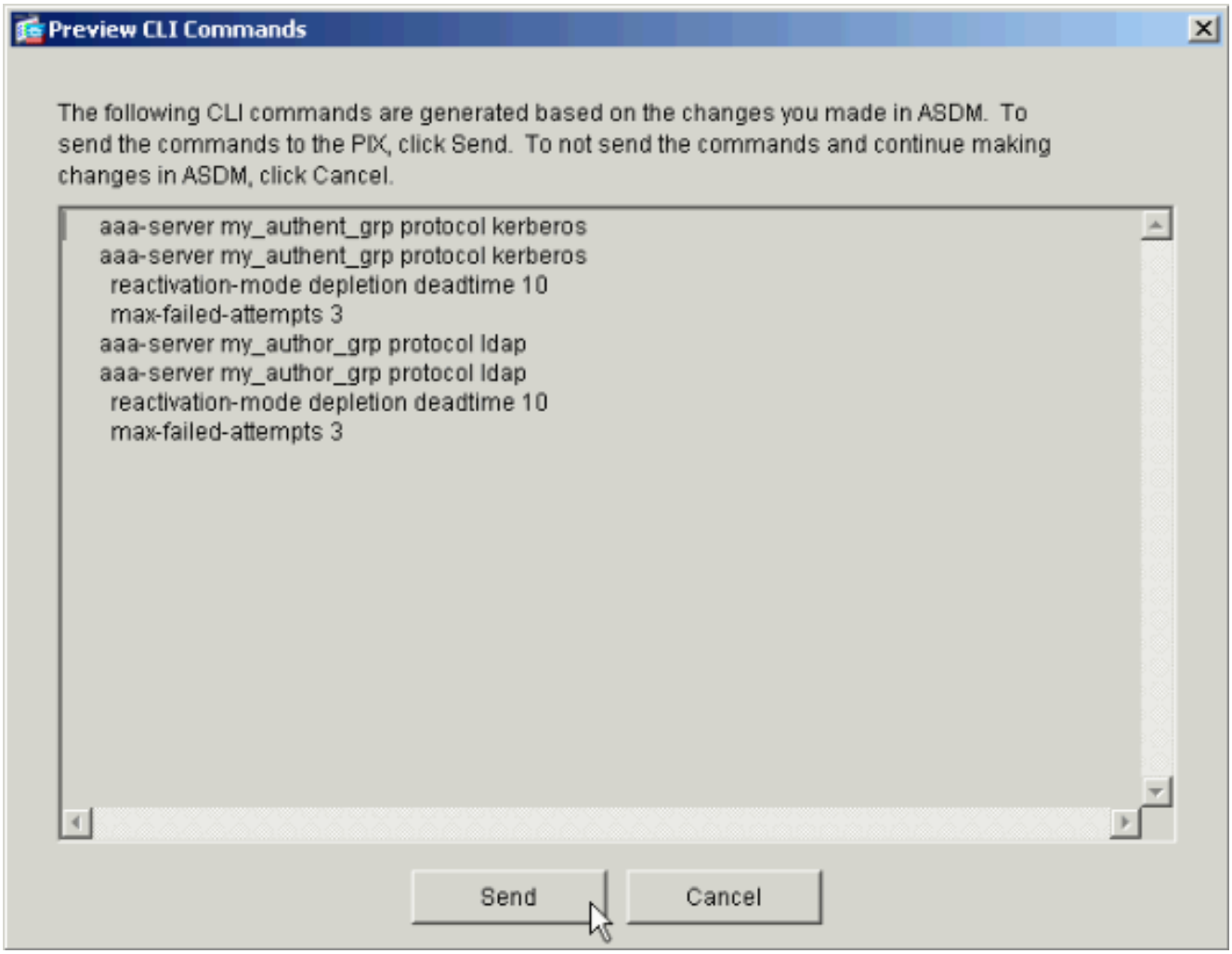
novo.

4. O clique **aplica-se** a fim enviar as mudanças ao dispositivo.



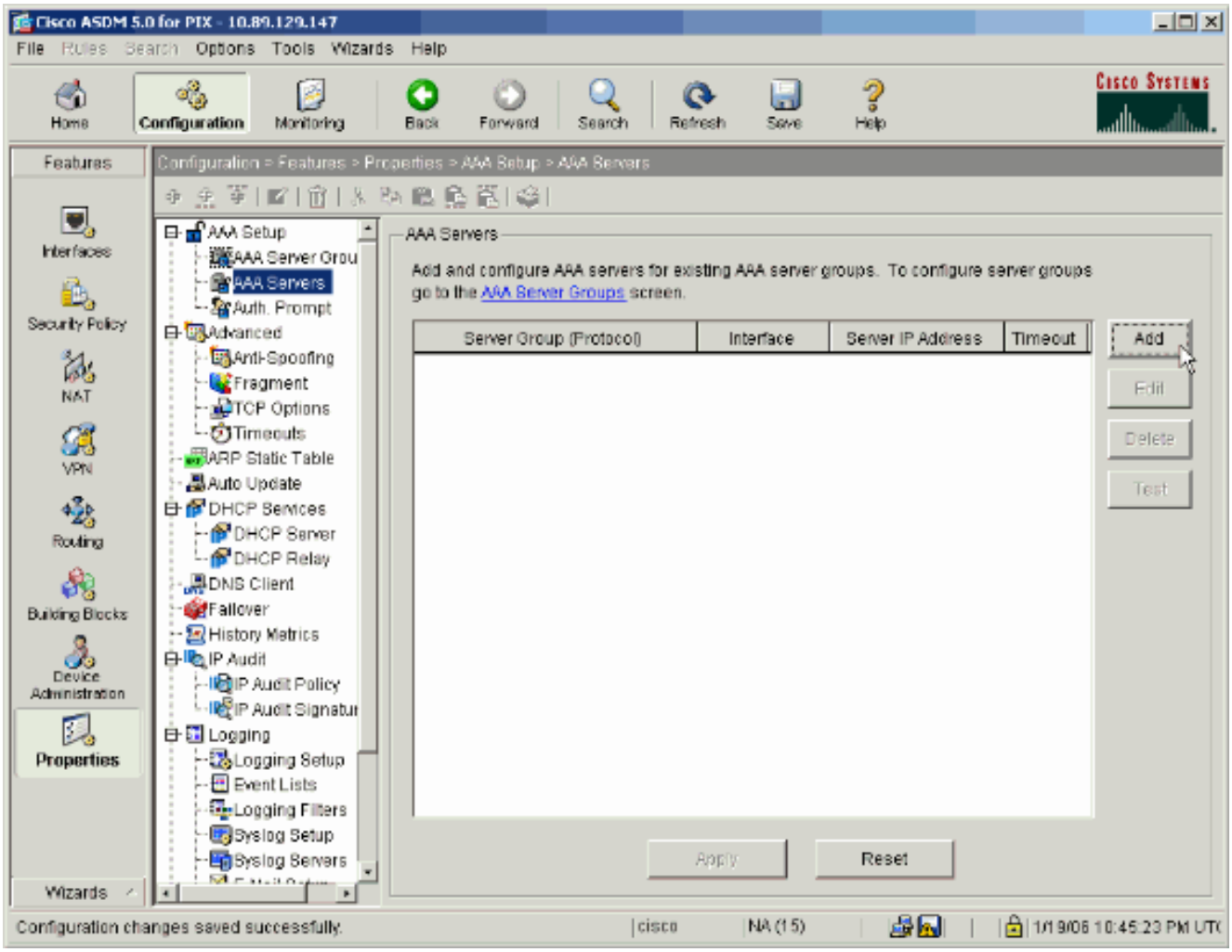
Se você o tem configurado para fazer assim, o dispositivo inspeciona agora os comandos que são adicionados à configuração running.

5. O clique **envia** a fim enviar os comandos ao dispositivo.

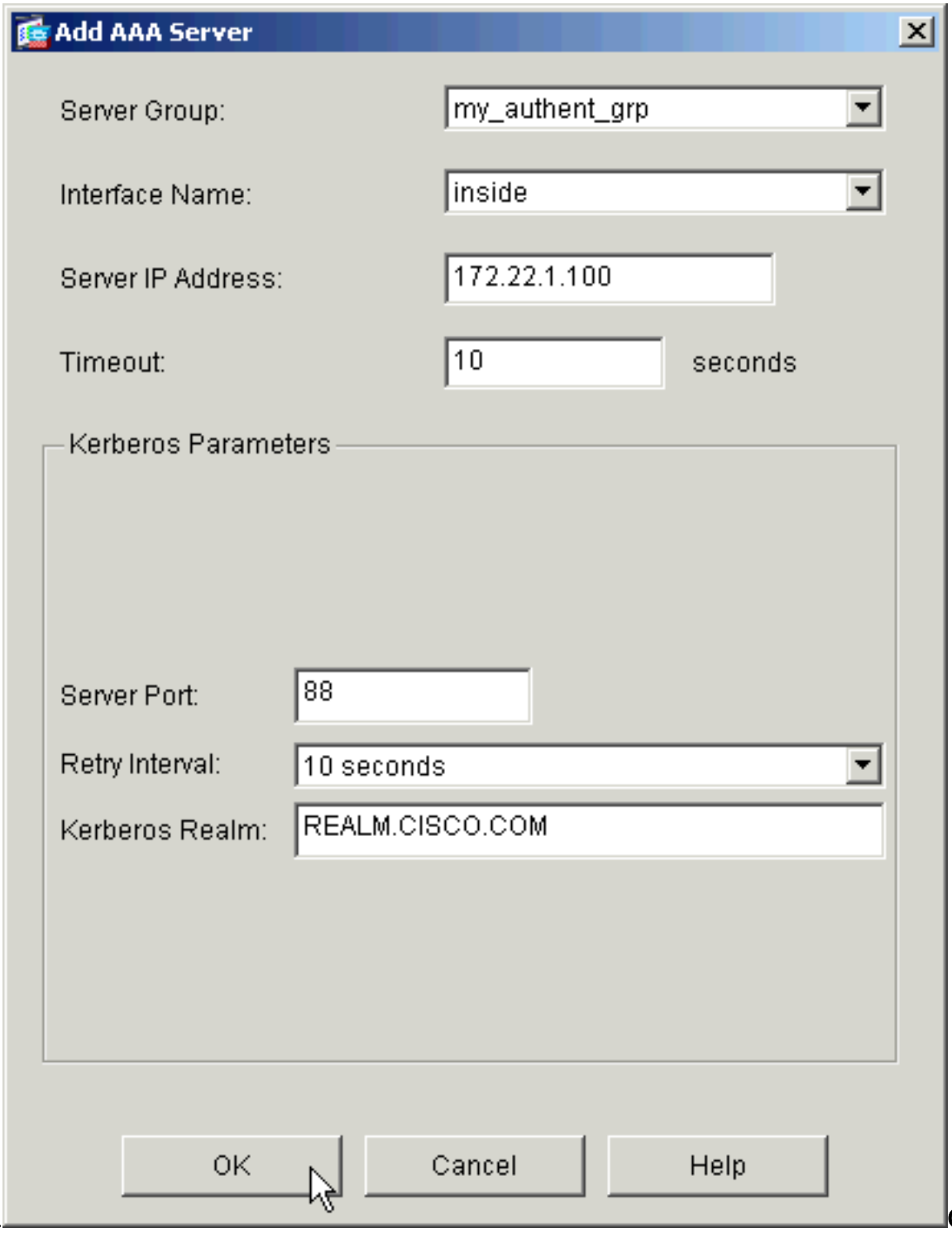


Os grupos de servidor recém-criados devem agora ser povoados com server da authentication e autorização.

6. Escolha a **configuração > as propriedades > o AAA Setup > servidores AAA**, e o clique **adiciona**.

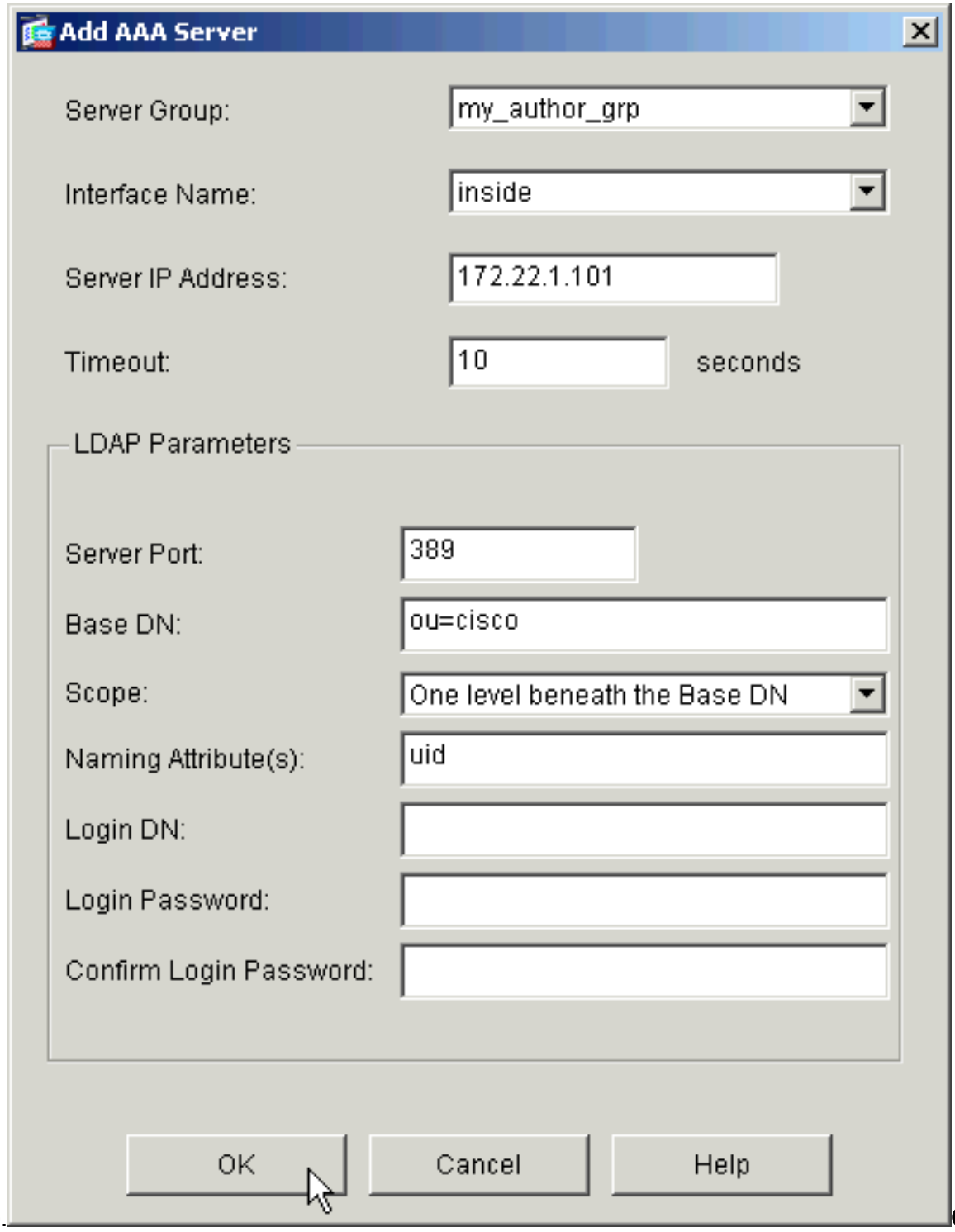


7. Configurar um Authentication Server. Clique a **APROVAÇÃO** quando você é



feito.**Grupo de servidor** — Escolha o grupo de Authentication Server configurado em etapa 2.**Nome da relação** — Escolha a relação em que o server reside.**Endereço IP do servidor** — Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT do Authentication Server.**Intervalo** — Especifique o tempo máximo, nos segundos, esperar uma resposta do server.**Parâmetros Kerberos:Porta de servidor** — 88 são a porta padrão para o Kerberos.**Intervalo de nova tentativa** — Escolha o intervalo de nova tentativa desejado.**Esfera de kerberos** — Dê entrada com o nome de sua esfera de kerberos. Este é frequentemente o Domain Name de Windows em todas as letras maiúsculas.

8. Configurar um servidor de autorização. Clique a **APROVAÇÃO** quando



terminado.**Grupo de servidor** — Escolha o grupo de servidor de autorização configurado em etapa 3.**Nome da relação** — Escolha a relação em que o server reside.**Endereço IP do servidor** — Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de autorização.**Intervalo** — Especifique o tempo máximo, nos segundos, esperar uma resposta do server.**Parâmetros LDAP:Porta de servidor** — 389 são a porta padrão para o LDAP.**Base DN** — Entre no lugar na hierarquia LDAP onde o server deve começar ao procurar uma vez recebe um pedido de autorização.**Espaço** — Escolha a extensão a que o server deve procurar a hierarquia LDAP uma vez que recebe um pedido de autorização.**Atributos de nomeação** — Incorpore os atributos de nome destacado relativos por que as entradas no servidor ldap são definidas excepcionalmente. Os atributos de nomeação comuns são Common Name (CN) e usuário - identificação (uid).**Início de uma sessão DN** — Alguns servidores ldap, incluindo o server do microsoft ative directory, exigem o dispositivo estabelecer um aperto de mão através do emperramento autenticado antes que aceitem

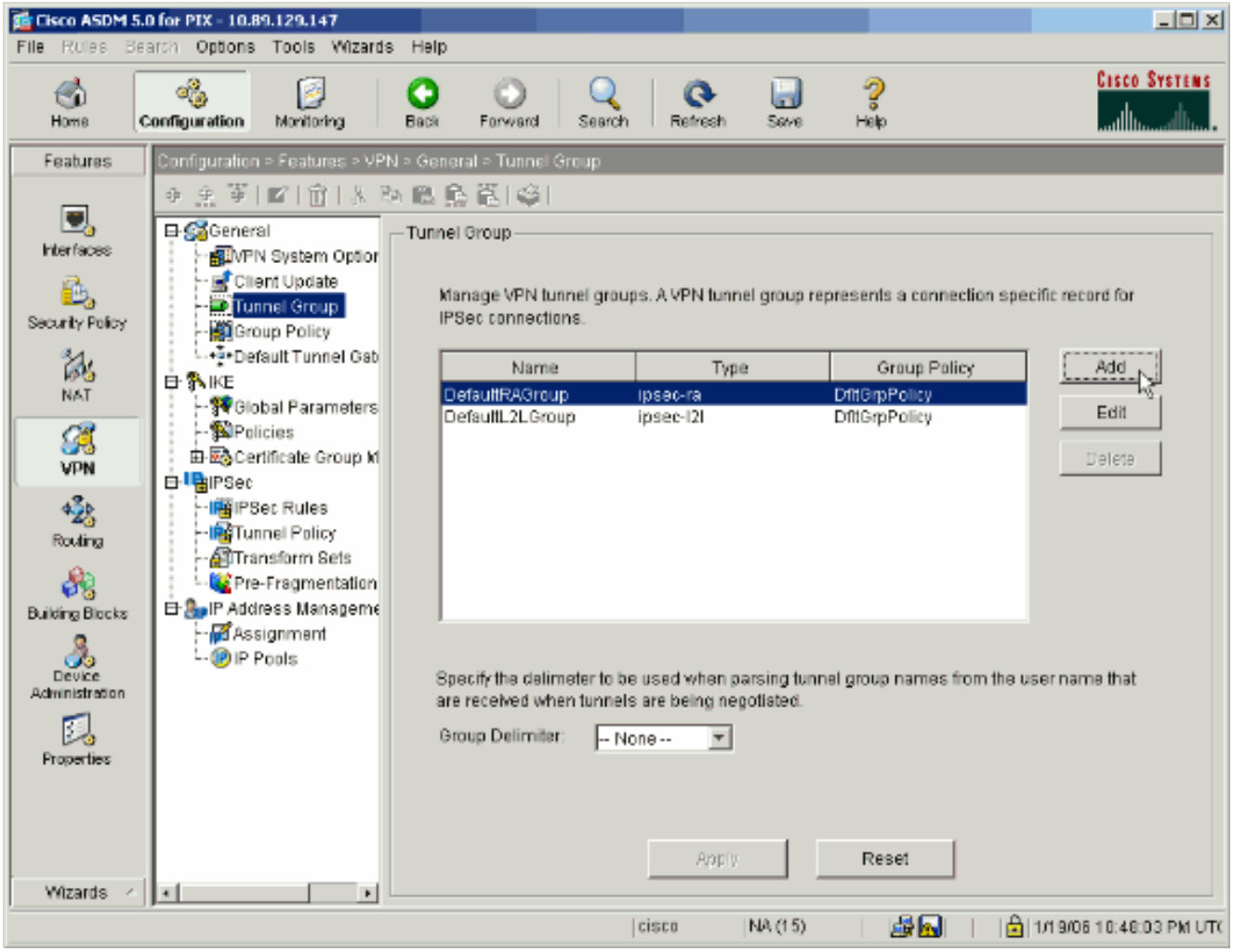
pedidos para todas as outras operações de LDAP. O campo do início de uma sessão DN define as características de autenticação do dispositivo, que deve corresponder àqueles de um usuário com os privilégios da administração. Por exemplo, cn=administrator. Para o acesso anônimo, deixe esta placa do campo.**Senha de login** — Incorpore a senha para o início de uma sessão DN.**Confirme a senha de login** — Confirme a senha para o início de uma sessão DN.

9. O clique **aplica-se** a fim enviar as mudanças aos server da authentication e autorização do dispositivo é adicionado afinal.Se você o tem configurado para fazer assim, o PIX inspeciona agora os comandos que são adicionados à configuração running.
10. O clique **envia** a fim enviar os comandos ao dispositivo.

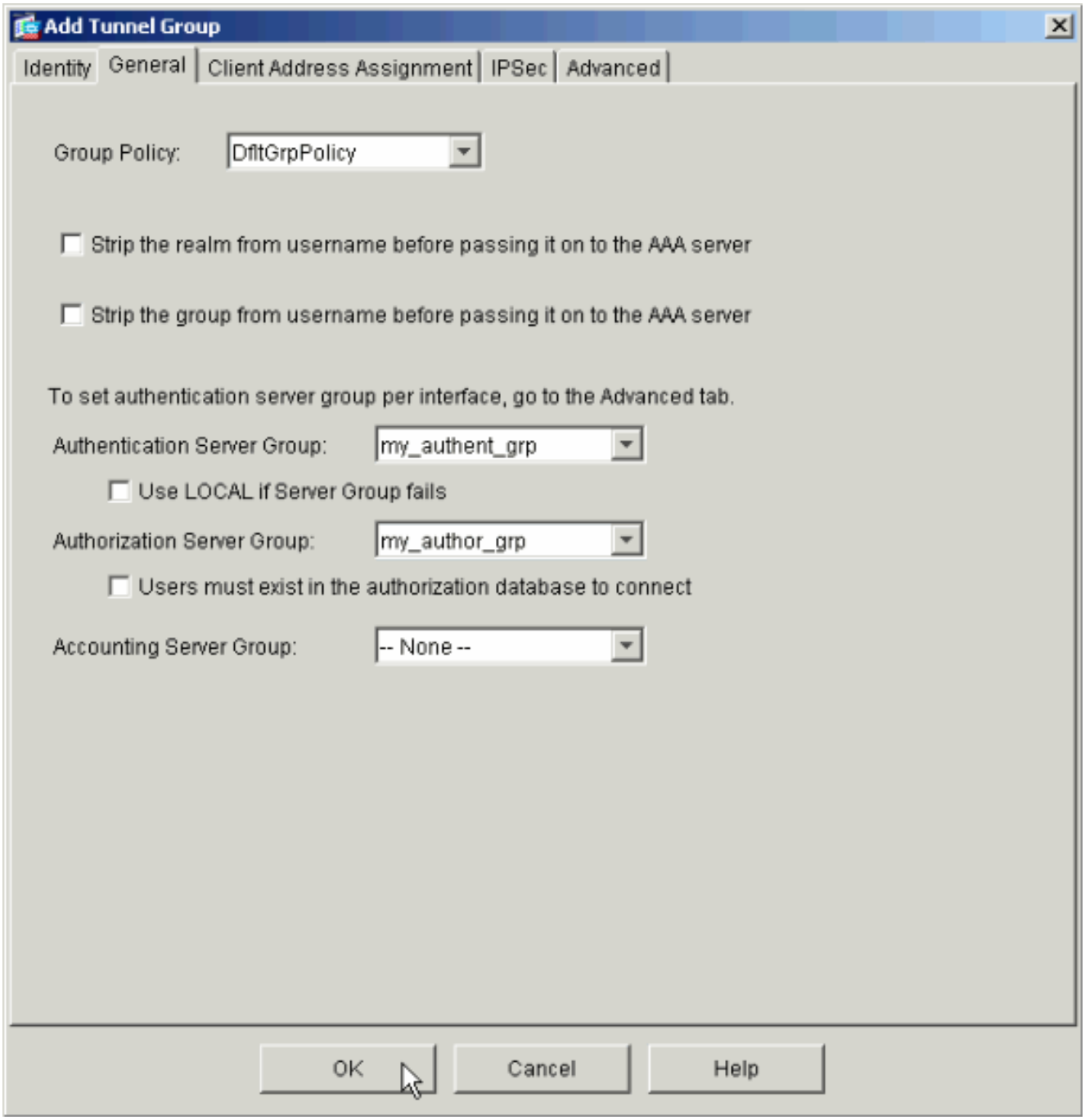
Configurar um grupo de túneis VPN para a authentication e autorização

Termine estas etapas a fim adicionar os grupos de servidor que você apenas configurou a um grupo de túneis VPN.

1. Escolha a **configuração > o VPN > o grupo de túneis**, e o clique **adiciona** a fim criar um grupo de túneis novo, ou **edita** a fim alterar um grupo existente.



2. No tab geral do indicador que aparece, selecione os grupos de servidor configurados mais cedo.



3. *Opcional:* Configurar os parâmetros remanescente nas outras abas se você adiciona um grupo de túneis novo.
4. Clique a **APROVAÇÃO** quando você é feito.
5. O clique **aplica-se** a fim enviar as mudanças ao dispositivo depois que a configuração do grupo de túneis está completa.Se você o tem configurado para fazer assim, o PIX inspeciona agora os comandos que são adicionados à configuração running.
6. O clique **envia** a fim enviar os comandos ao dispositivo.

Configurar a authentication e autorização para os usuários VPN que usam o CLI

Esta é a configuração de CLI equivalente para os grupos de servidor da authentication e autorização para usuários VPN.

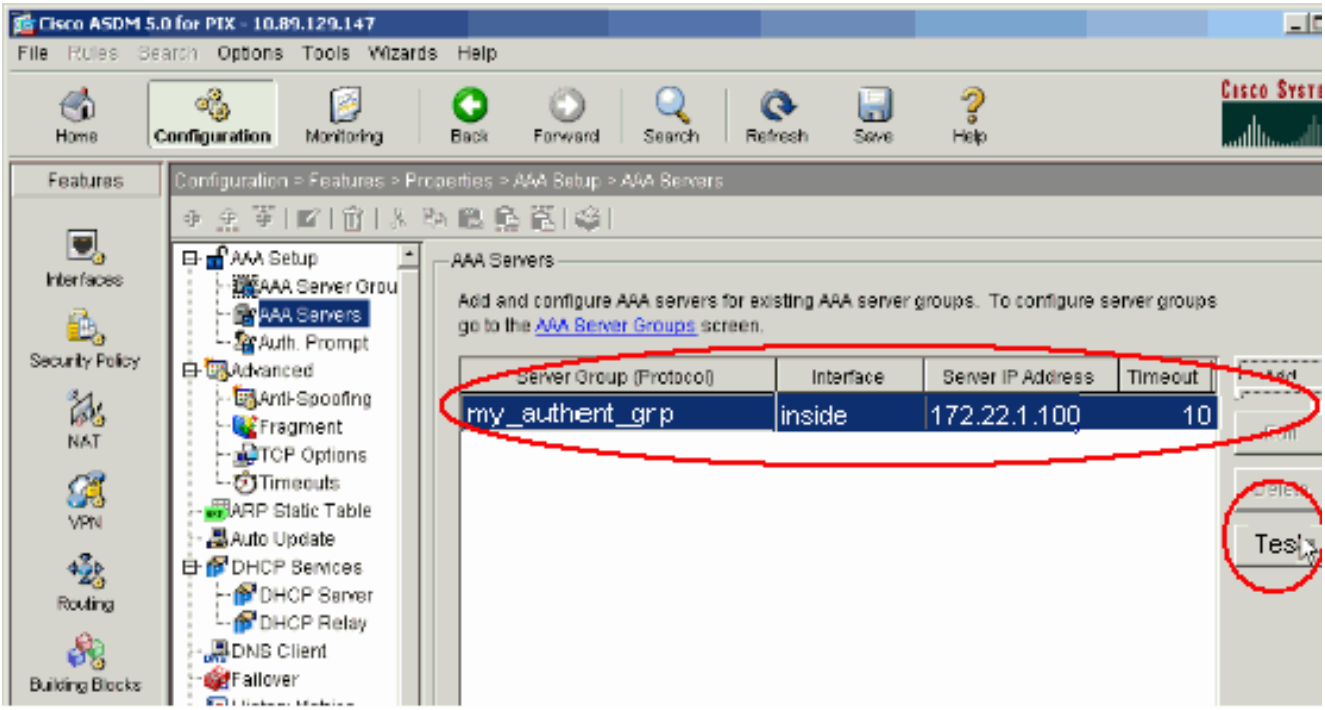
Configuração de CLI da ferramenta de segurança

```
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.
```

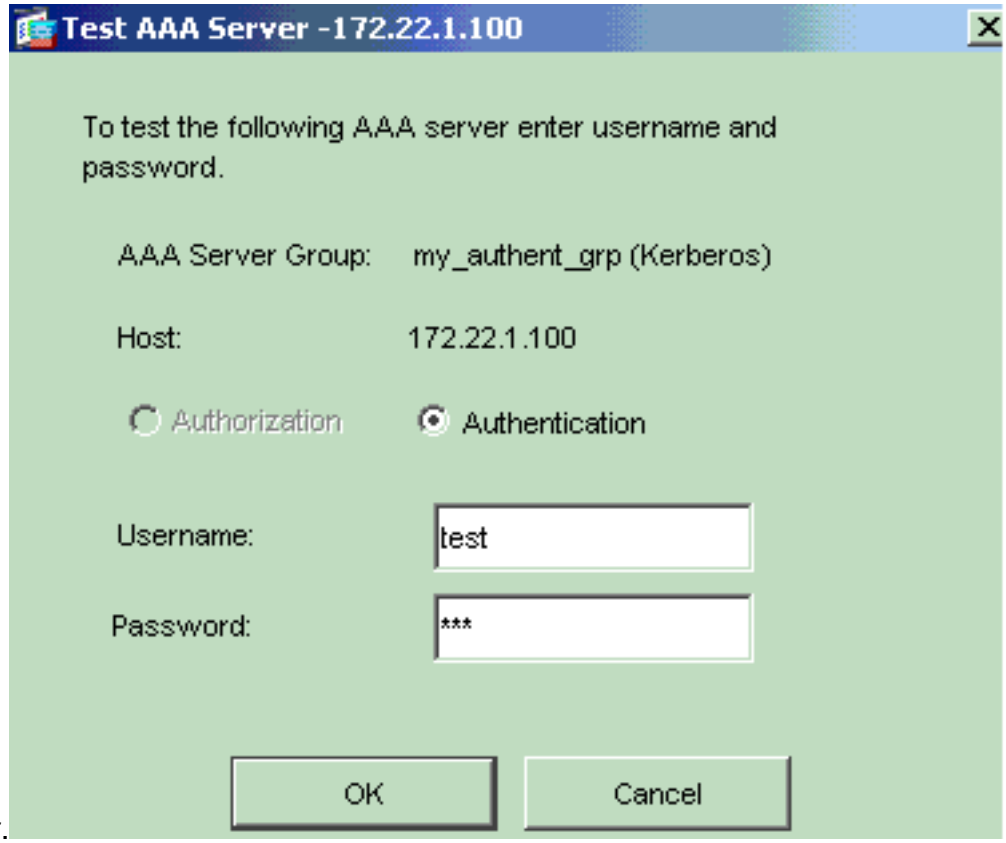
Verificar

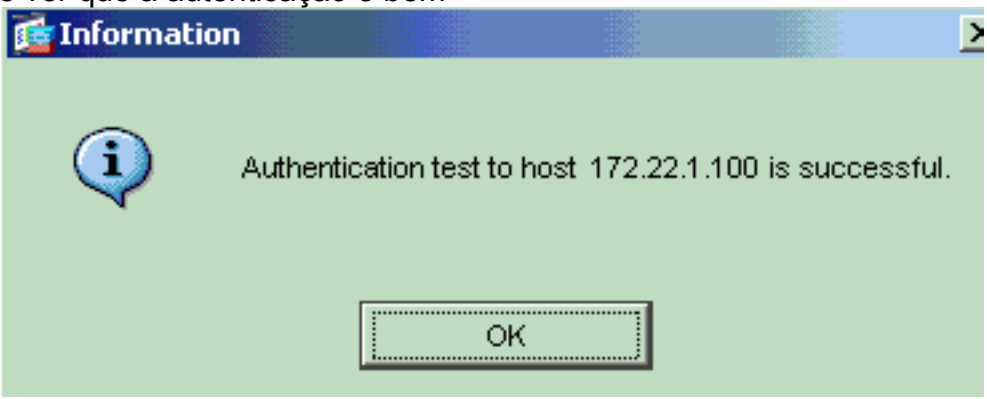
Termine estas etapas a fim verificar a autenticação de usuário entre o PIX/ASA e o servidor AAA:

1. Escolha a **configuração > as propriedades > o AAA Setup > servidores AAA**, e selecione o grupo de servidor (my_authent_grp). Clique então o **teste** a fim validar as credenciais do usuário.



2. Forneça o nome de usuário e senha (por exemplo, username: teste e senha: o teste), e clica a **APROVAÇÃO** a fim

validar. 

3. Você pode ver que a autenticação é bem sucedida. 

Troubleshooting

1. Uma causa frequente da falha de autenticação é enviesamento do pulso de disparo. Seja certo que os pulsos de disparo no PIX ou no ASA e seu Authentication Server estão sincronizados.Quando a autenticação falha devido cronometrar o enviesamento, você pode receber este Mensagem de Erro: `:- ERRO: Autenticação rejeitada: Segundos enviesados do pulso de disparo maior de 300`. Também, este mensagem de registro aparece:`%PIX|ASA-3-113020: Erro do Kerberos: Enviesamento do pulso de disparo com segundos dos ip_address do server maiores de 300 ip_address` — O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Kerberos.Esta mensagem é indicada quando a autenticação para um usuário do IPsec ou WebVPN através de um servidor Kerberos falha porque os pulsos de disparo na ferramenta de segurança e no server são mais de cinco minutos (300 segundos) distante. Quando isto ocorre, a tentativa de conexão está rejeitada.A fim resolver esta edição, sincronize os pulsos de disparo na ferramenta de segurança e no servidor Kerberos.
2. a PRE-autenticação no diretório ativo (AD) deve ser desabilitada, ou ele pode conduzir à falha da autenticação de usuário.

3. Os usuários de cliente VPN são incapazes de autenticar contra o Microsoft certificate server. Este Mensagem de Erro aparece:`"Erro que processa o payload" (erro 14)` A fim resolver esta edição, desmarcar **não exigem a** caixa de seleção **Pré-autenticação do kerberose no** Authentication Server.

Informações Relacionadas

- Configurando servidores AAA e o base de dados local
- Sustentação do produto do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems