PIX/ASA: Autenticación de Kerberos y grupos de servidor de autorización LDAP para los usuarios de cliente VPN vía el ejemplo de configuración ASDM/CLI

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Productos Relacionados
Convenciones
Antecedentes
Autenticación y autorización de la configuración para los usuarios de VPN que usan el ASDM
Servidores de la autenticación y autorización de la configuración
Configure a un grupo de túnel VPN para la autenticación y autorización
Configure la autenticación y autorización para los usuarios de VPN que usan el CLI
Verificación
Troubleshooting
Información Relacionada

Introducción

Este documento describe cómo utilizar al Cisco Adaptive Security Device Manager (ASDM) para configurar la autenticación de Kerberos y a los grupos de servidor de autorización LDAP en el dispositivo de seguridad de la serie del Cisco PIX 500. En este ejemplo, la directiva de un grupo de túnel VPN utilizan a los grupos de servidores para autenticar y para autorizar a los usuarios entrantes.

prerrequisitos

Requisitos

Este documento asume el PIX está completamente - operativo y configurado para permitir que el ASDM realice los cambios de configuración.

Nota: Refiera a permitir el acceso HTTPS para el ASDM para permitir que el PIX sea configurado por el ASDM.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de software 7.x del dispositivo de seguridad del Cisco PIX y posterior
- Cisco ASDM versión 5.x y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con la versión 7.x adaptante del dispositivo de seguridad de Cisco (ASA).

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

No todos los métodos de autenticación y autorización posibles disponibles en el software del PIX/ASA 7.x se soportan cuando usted trata de los usuarios de VPN. Esta tabla detalla qué métodos están disponibles para los usuarios de VPN:

	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
Autenticación	Sí	Sí	Sí	Sí	Sí	Sí	No
Autorización	Sí	Sí	No	No	No	No	Sí

Nota: El Kerberos se utiliza para la autenticación y el LDAP se utiliza para la autorización de los usuarios de VPN en este ejemplo.

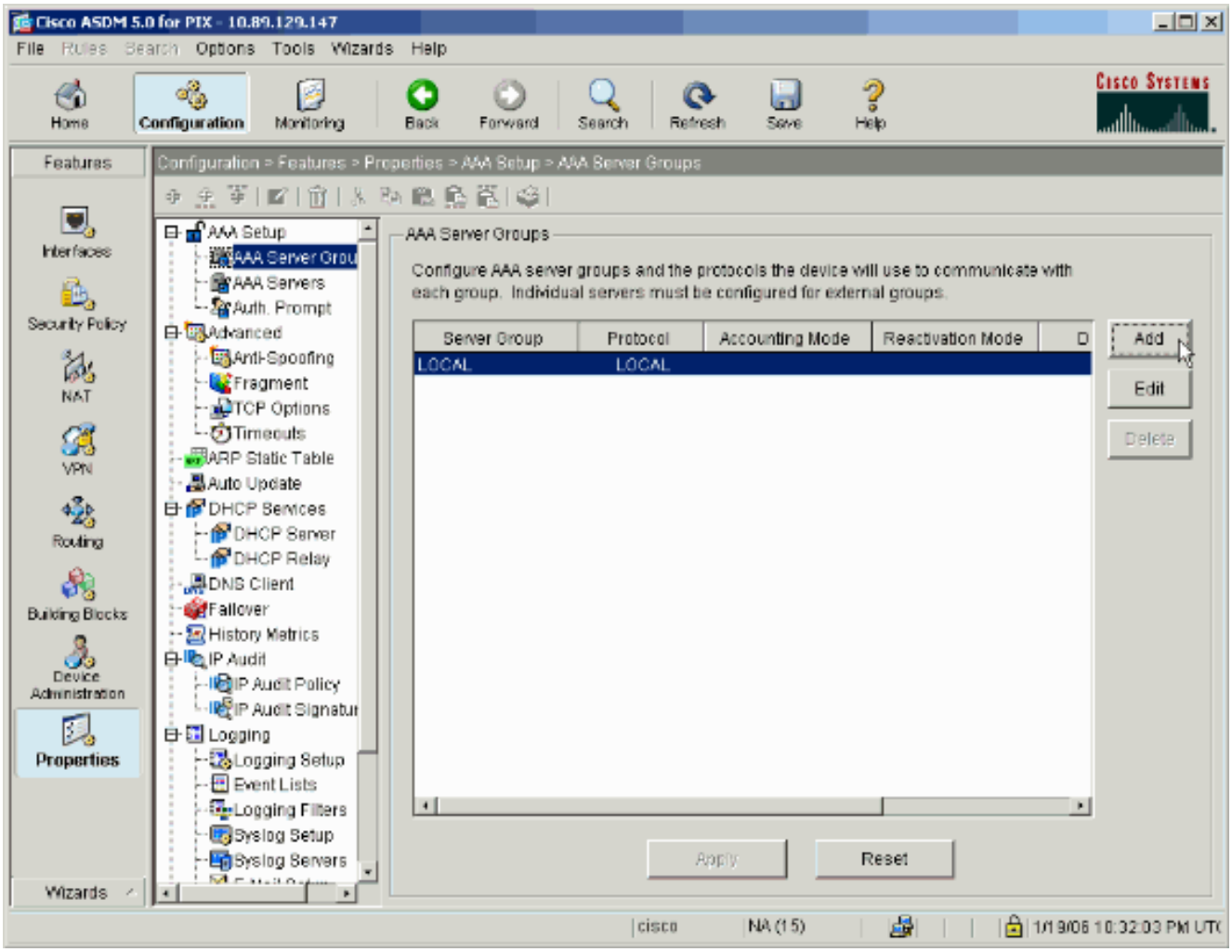
Autenticación y autorización de la configuración para los usuarios de VPN que usan el ASDM

Servidores de la autenticación y autorización de la configuración

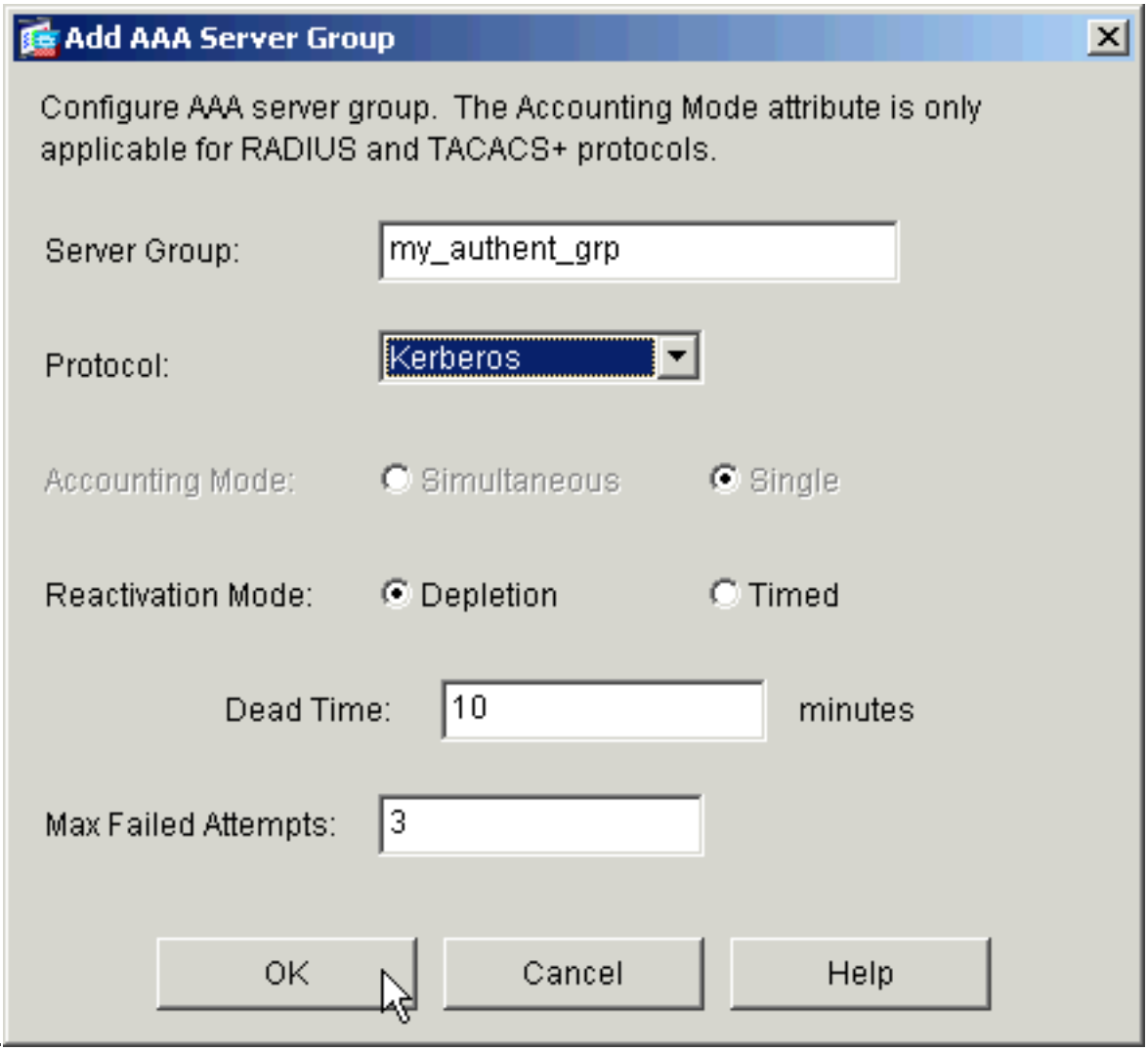
Complete estos pasos para configurar a los grupos de servidores de la autenticación y autorización para los usuarios de VPN con el ASDM.

1. Elija la **configuración > las propiedades >AAA ponen >AAA los grupos de servidores**, y el

haga click en
Add

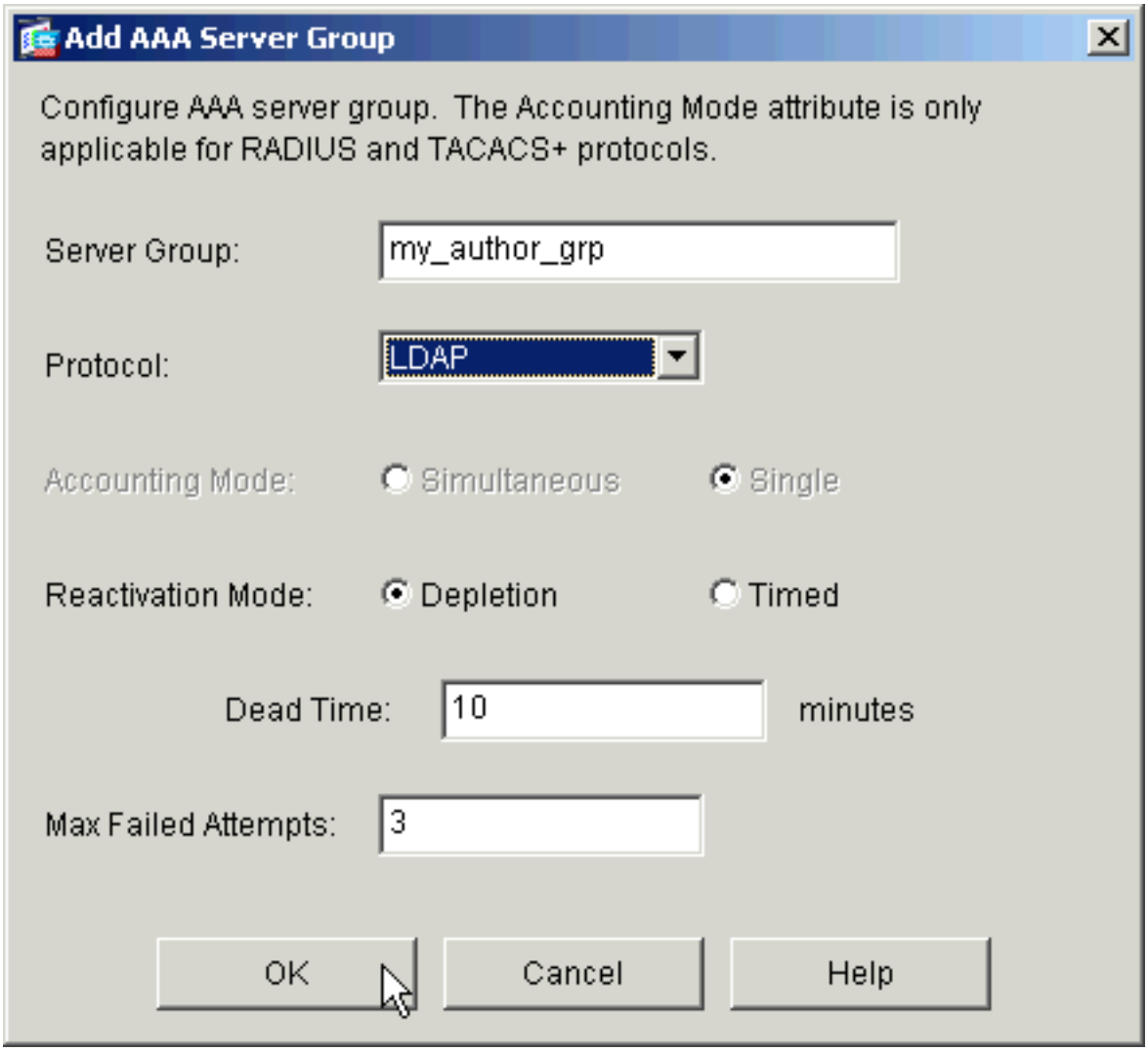


2. Defina un nombre para el nuevo grupo de servidor de autenticación, y elija un protocolo.La opción de modo de las estadísticas está para el RADIUS y el TACACS+ solamente. Haga Click en OK cuando le

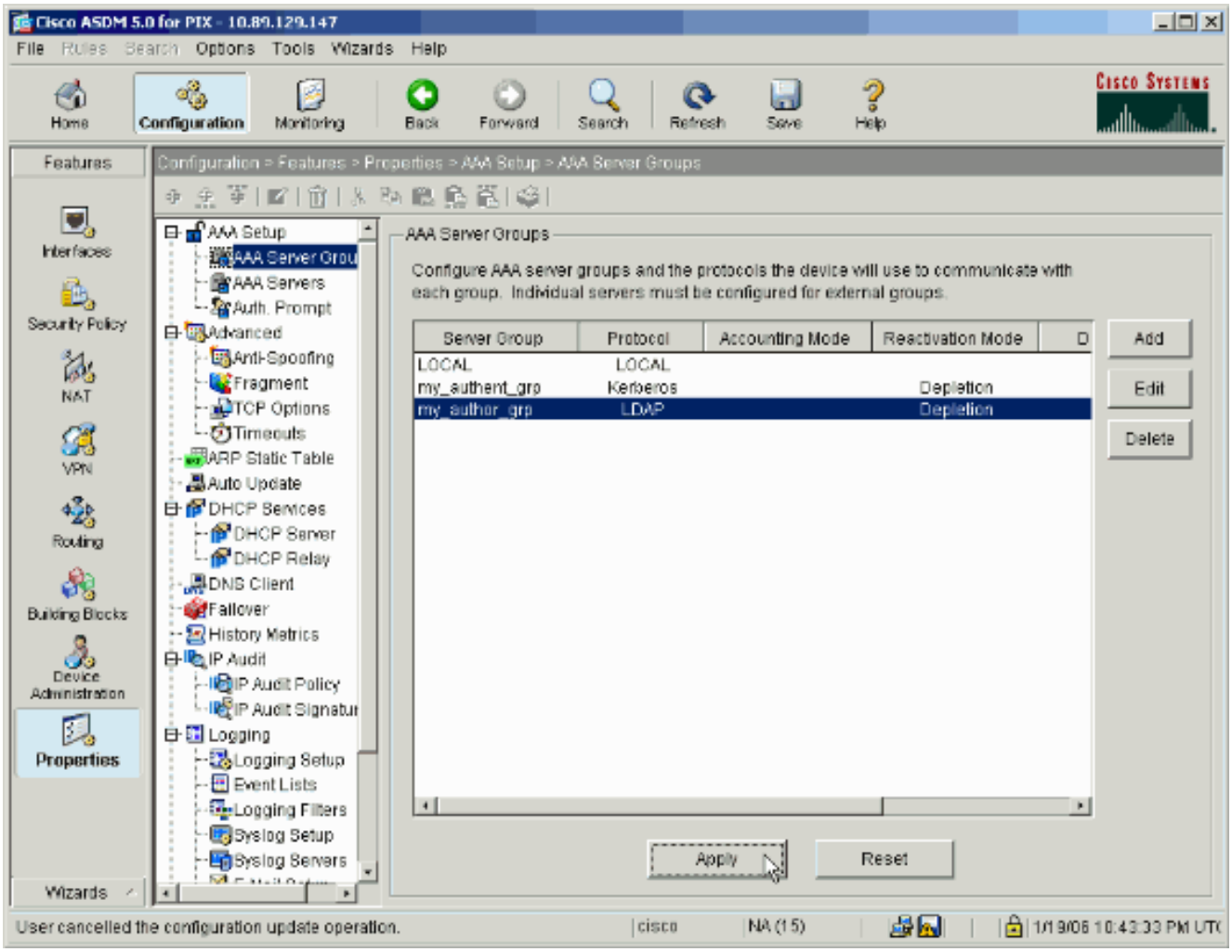


hacen.

3. Relance los pasos 1 y 2 para crear a un nuevo grupo de servidor de autorización.

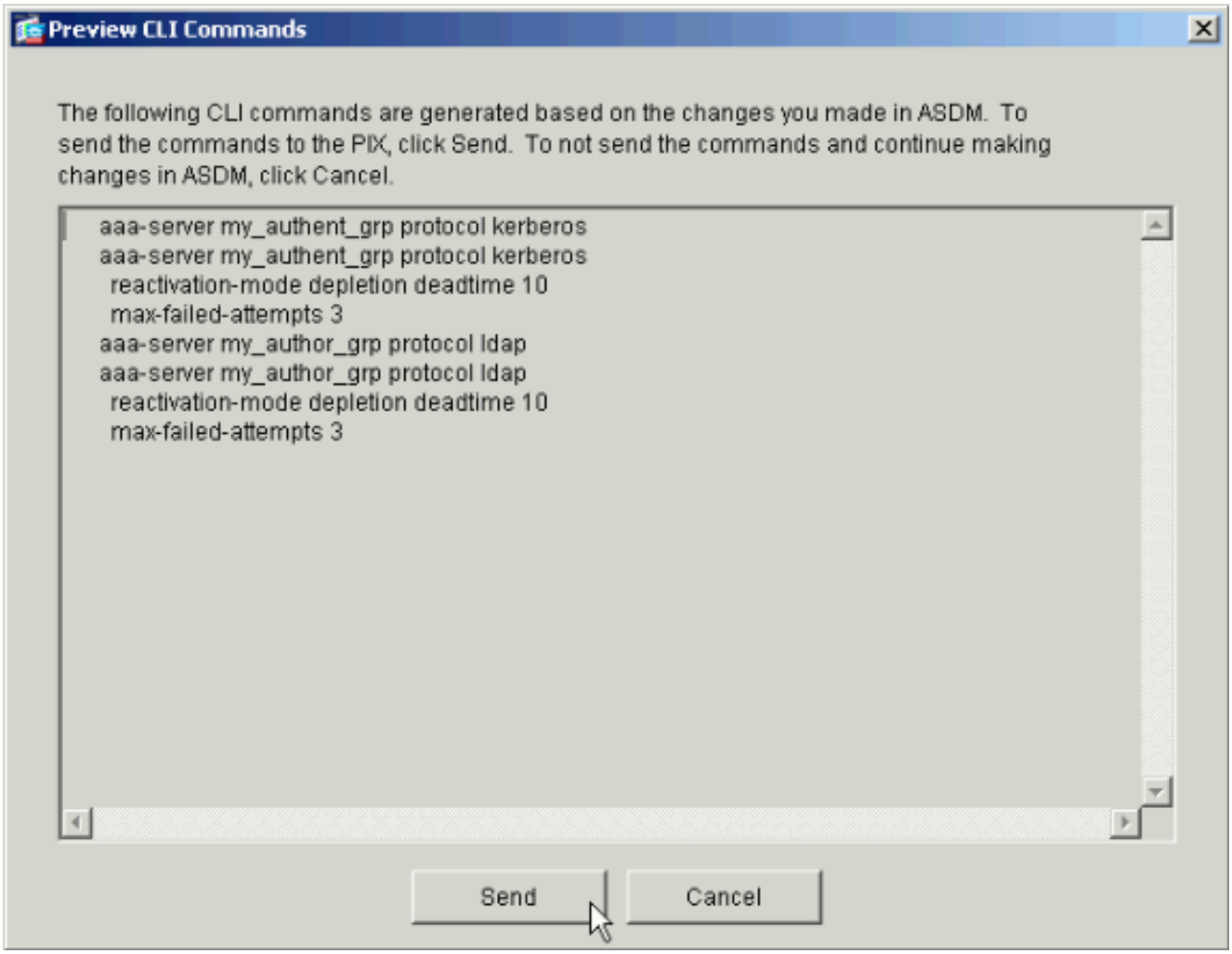


4. El tecleo **se aplica** para enviar los cambios al dispositivo.



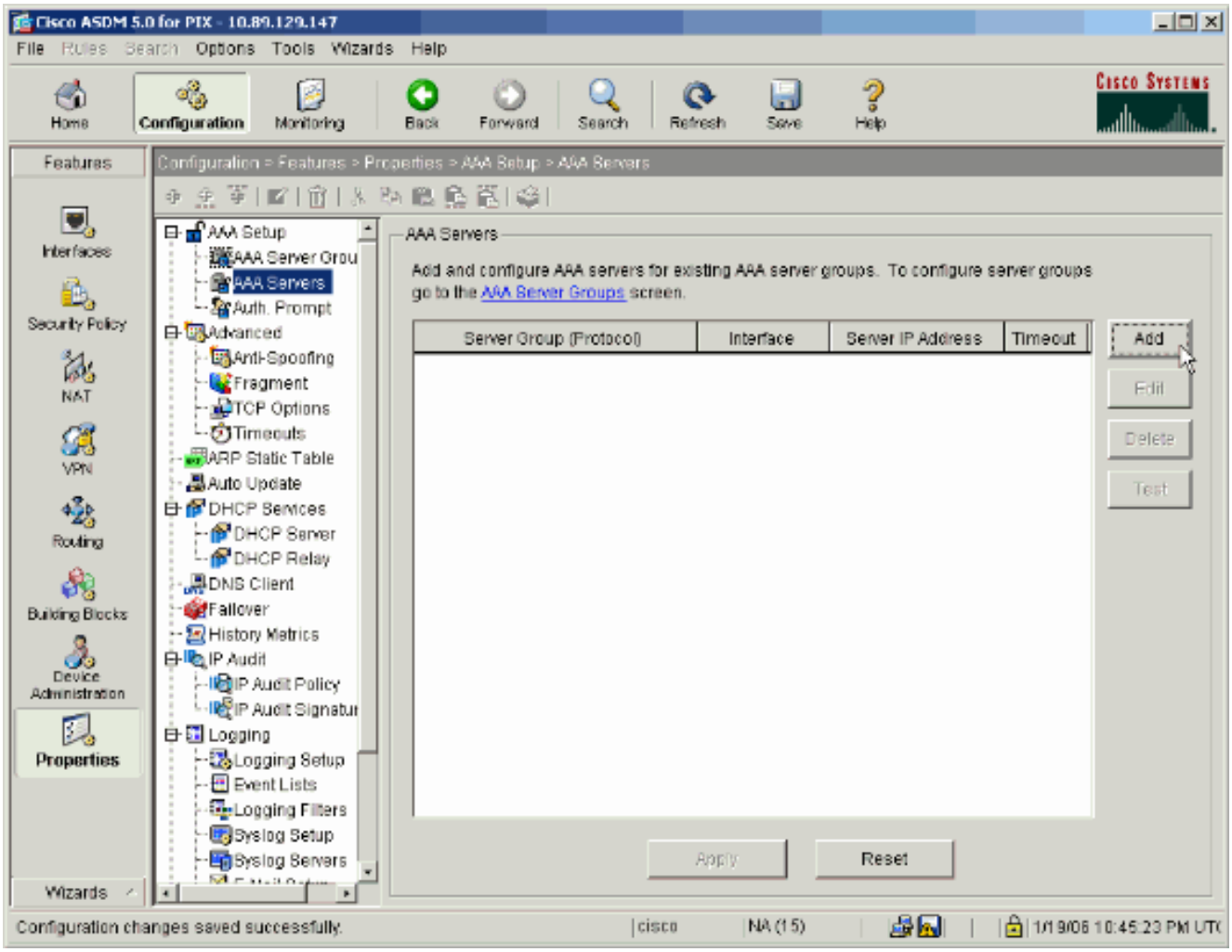
Si usted lo hace configurar para hacer así pues, el dispositivo ahora ve los comandos de antemano que se agregan a la configuración corriente.

5. El tecleo **envía** para enviar los comandos al dispositivo.

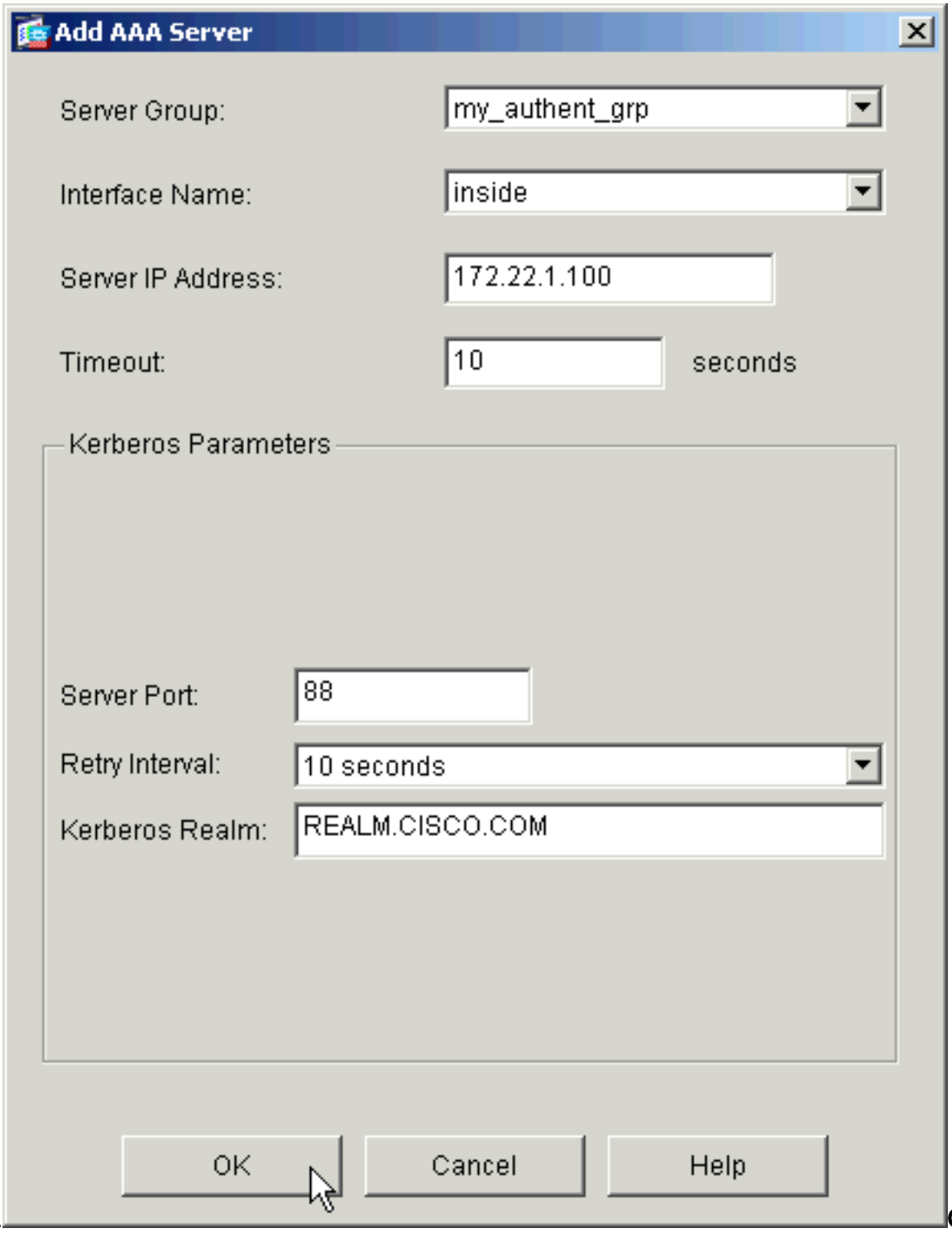


Los grupos de servidores creados recientemente deben ahora ser poblados con los servidores de la autenticación y autorización.

6. Elija la **configuración > las propiedades >AAA ponen >AAA los servidores**, y el haga click en Add

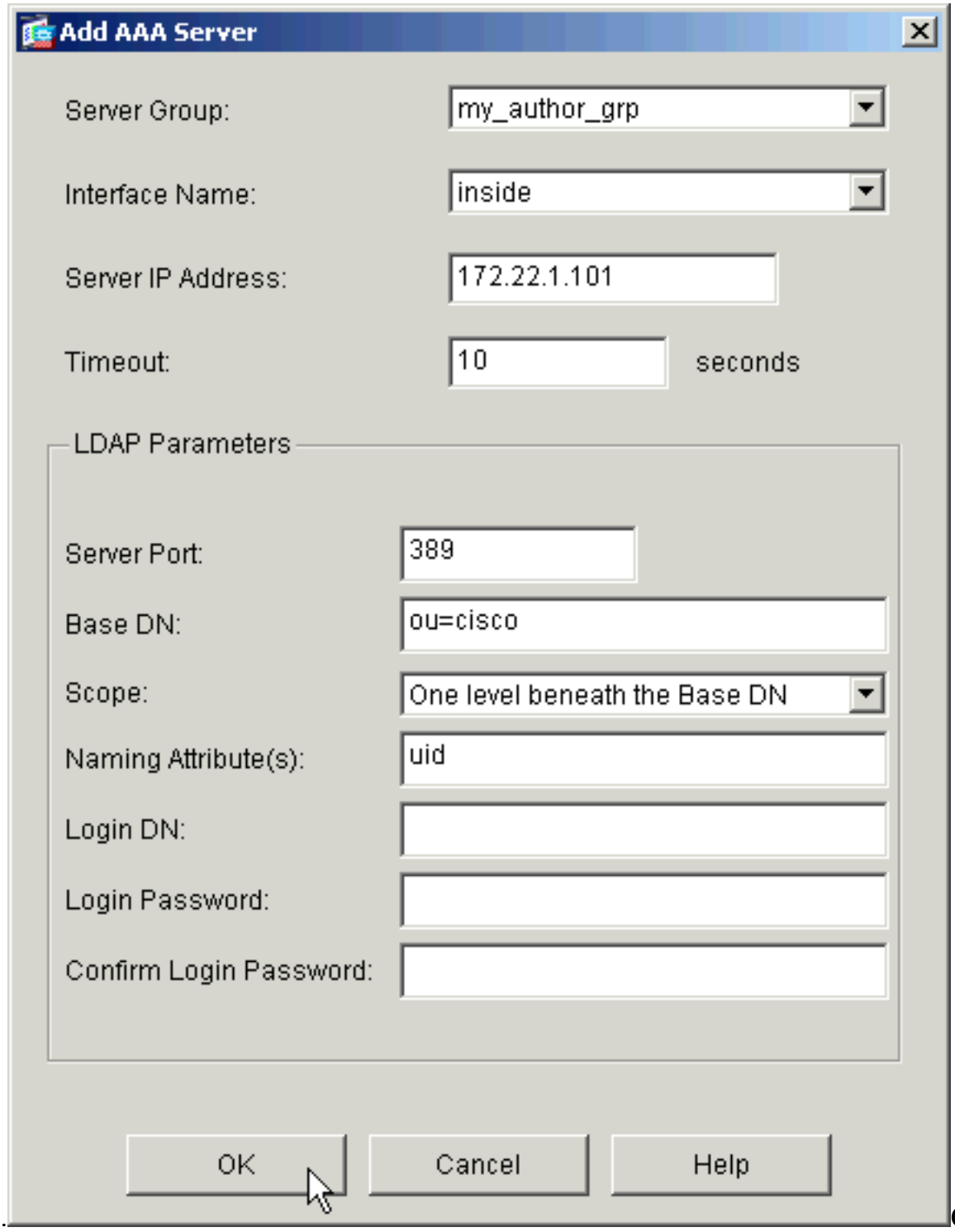


7. Configure a un servidor de autenticación. Haga Click en OK cuando le



hacen.**Grupo de servidores** — Elija al grupo de servidor de autenticación configurado en el paso 2.**Nombre de la interfaz** — Elija la interfaz en la cual el servidor reside.**Dirección IP del servidor** — Especifique la dirección IP del servidor de autenticación.**Descanso** — Especifique el tiempo máximo, en los segundos, para esperar una respuesta del servidor.**Parámetros Kerberos:Puerto de servidor** — 88 es el puerto estándar para el Kerberos.**Intervalo entre reintentos** — Elija el intervalo entre reintentos deseado.**Terreno de Kerberos** — Ingrese el nombre de su terreno de Kerberos. Éste es con frecuencia el Domain Name de Windows en todas las letras mayúsculas.

8. Configure a un servidor de autorización. Haga Click en OK cuando está



acabado.**Grupo de servidores** — Elija al grupo de servidor de autorización configurado en el paso 3.**Nombre de la interfaz** — Elija la interfaz en la cual el servidor reside.**Dirección IP del servidor** — Especifique la dirección IP del servidor de autorización.**Descanso** — Especifique el tiempo máximo, en los segundos, para esperar una respuesta del servidor.**Parámetros de LDAP:Puerto de servidor** — 389 es el puerto predeterminado para el LDAP.**Base DN** — Ingrese la ubicación en la jerarquía LDAP en donde el servidor debe comenzar a buscarla una vez recibe un pedido de autorización.**Alcance** — Elija el fragmento al cual el servidor debe buscar la jerarquía LDAP que recibe una vez un pedido de autorización.**Atributos de nombramiento** — Ingrese los atributos de nombre distintivo relativos por los cuales las entradas en el servidor LDAP son definidas únicamente. Los atributos de nombramiento comunes son Common Name (CN) y identificación del usuario (uid).**Login DN** — Algunos servidores LDAP, incluyendo el servidor del Microsoft Active Directory, requieren el dispositivo para establecer un apretón de manos vía el atascamiento autenticado antes de

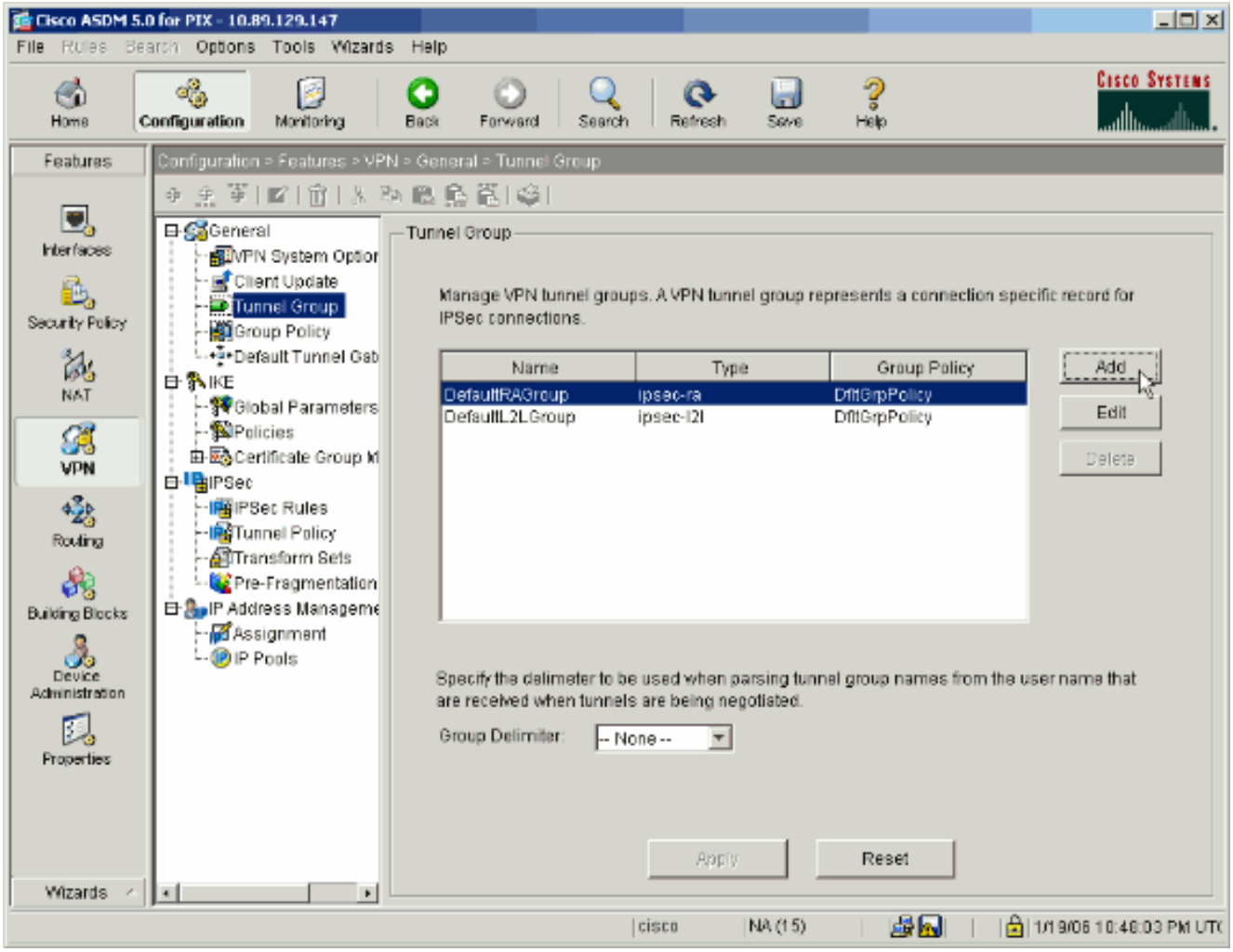
que validen los pedidos cualquier otra operaciones LDAP. El campo del login DN define las características de autenticación del dispositivo, que debe corresponder a los de un usuario con los privilegios de la administración. Por ejemplo, cn=administrator. Para el acceso anónimo, deje este espacio en blanco del campo.**Contraseña de inicio de sesión** — Ingrese la contraseña para el login DN.**Confirme la contraseña de inicio de sesión** — Confirme la contraseña para el login DN.

9. El tecleo **se aplica** para enviar los cambios a los servidores de la autenticación y autorización del dispositivo después de todo se agrega.Si usted lo hace configurar para hacer así pues, el PIX ahora ve los comandos de antemano que se agregan a la configuración corriente.
10. El tecleo **envía** para enviar los comandos al dispositivo.

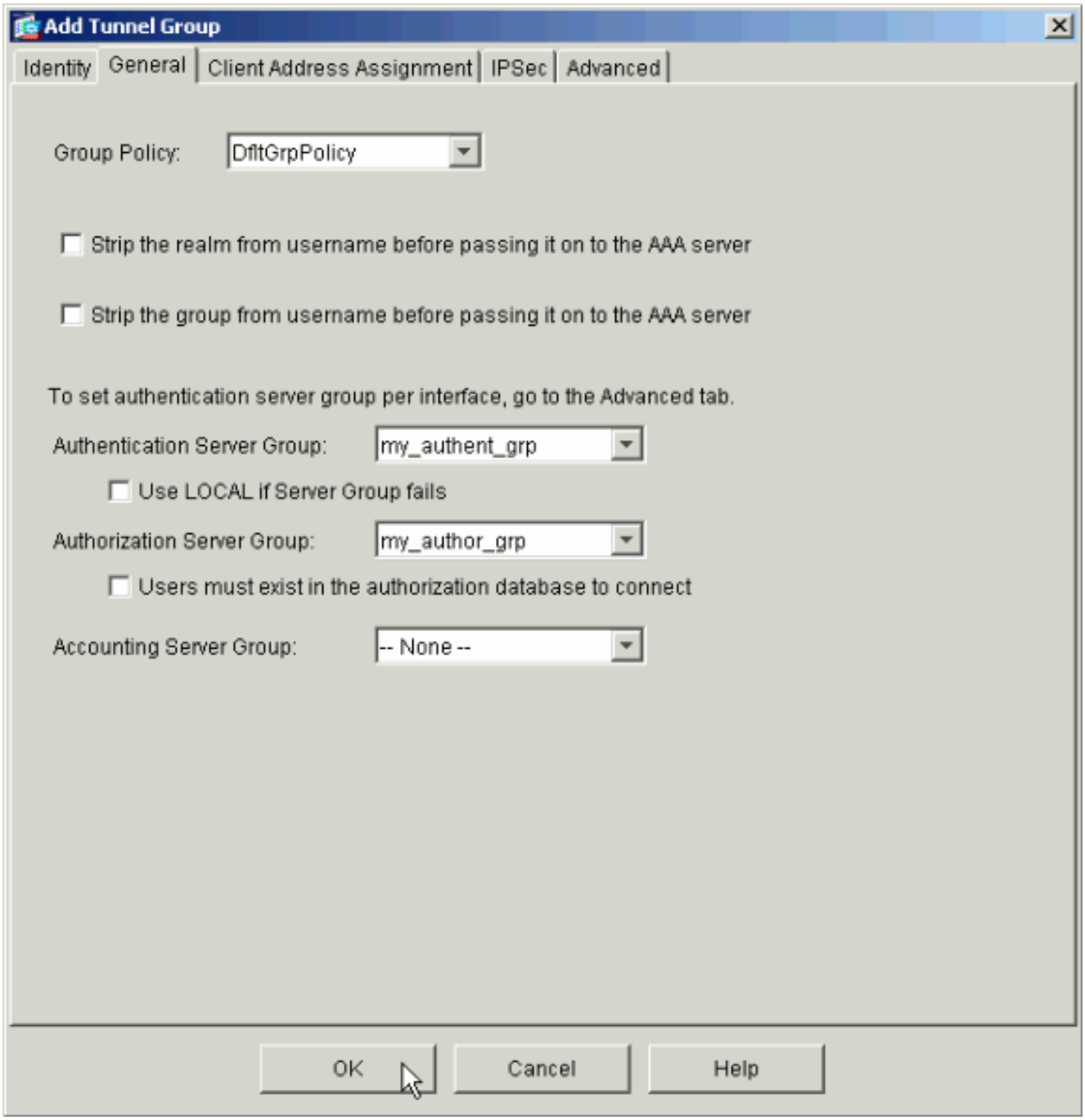
Configure a un grupo de túnel VPN para la autenticación y autorización

Complete estos pasos para agregar a los grupos de servidores que usted acaba de configurar a un grupo de túnel VPN.

1. Elija la **configuración > el VPN > al grupo de túnel**, y el tecleo **agrega** para crear a un nuevo grupo de túnel, o **edita** para modificar un grupo existente.



2. En la ficha general de la ventana que aparece, seleccione a los grupos de servidores configurados anterior.



3. *Opcional:* Configure los parámetros restantes en las otras lenguetas si usted agrega a un nuevo grupo de túnel.
4. Haga Click en OK cuando le hacen.
5. El tecleo **se aplica** para enviar los cambios al dispositivo después de que la configuración del grupo de túnel sea completa.Si usted lo hace configurar para hacer así pues, el PIX ahora ve los comandos de antemano que se agregan a la configuración corriente.
6. El tecleo **envía** para enviar los comandos al dispositivo.

Autenticación y autorización de la configuración para los usuarios de VPN que usan el CLI

Ésta es la configuración CLI equivalente para los grupos de servidores de la autenticación y autorización para los usuarios de VPN.

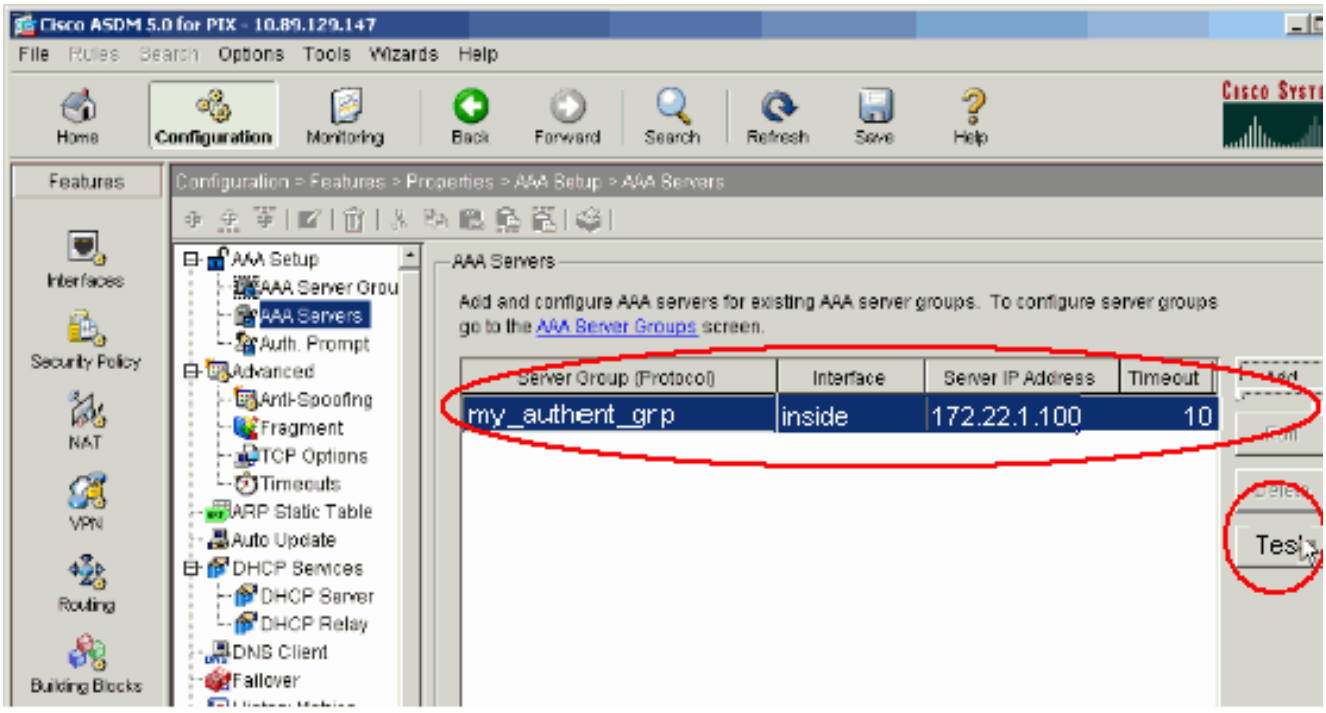
Configuración CLI del dispositivo de seguridad

```
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.
```

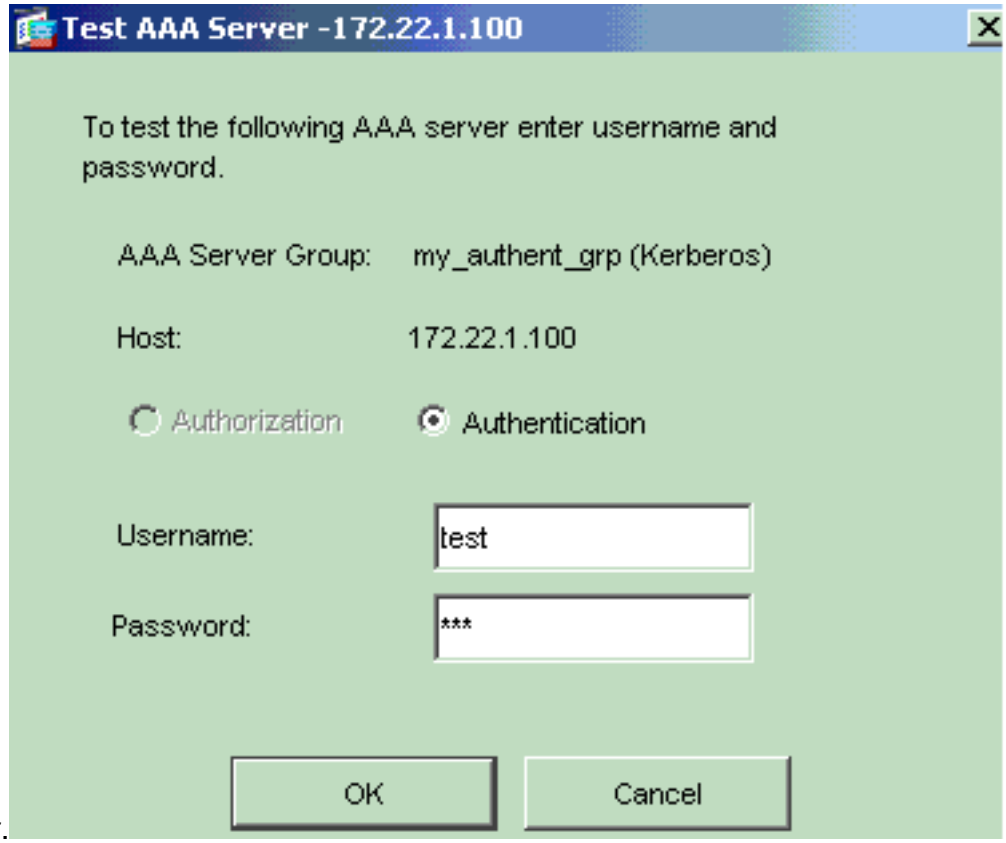
Verificación

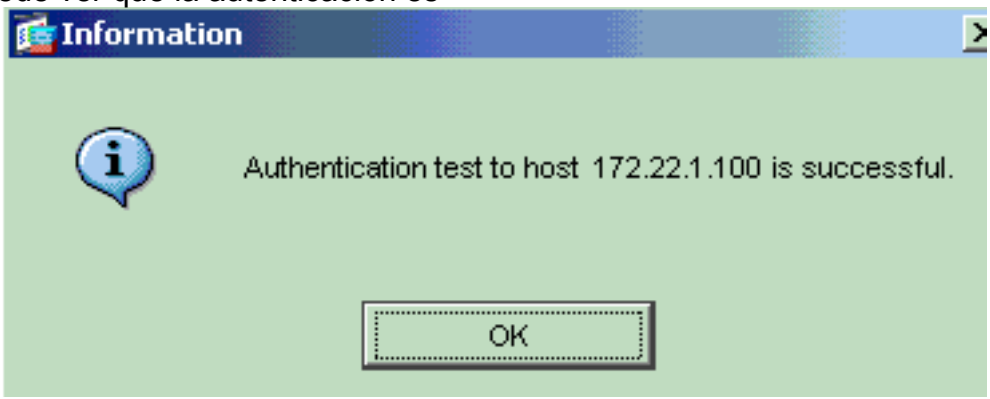
Complete estos pasos para verificar la autenticación de usuario entre el PIX/ASA y el servidor de AAA:

1. Elija la **configuración > las propiedades >AAA ponen >AAA los servidores**, y seleccionan el grupo de servidores (my_authent_grp). Entonces haga clic la **prueba** para validar los credenciales de
usuario.



2. Proporcione el nombre de usuario y contraseña (por ejemplo, nombre de usuario: prueba y contraseña: la prueba), y hace clic la **AUTORIZACIÓN** para

validar. 

3. Usted puede ver que la autenticación es acertada. 

Troubleshooting

1. Una causa frecuente de la falla de autenticación es posición oblicua del reloj. Esté seguro que sincronizan los relojes en el PIX o el ASA y a su servidor de autenticación.Cuando la autenticación falla debido cronometrar la posición oblicua, usted puede recibir este mensaje de error: `:- ERROR: Autenticación rechazada: Segundos oblicuos del reloj mayor de 300.` También, este mensaje del registro aparece:`%PIX|ASA-3-113020: Error del Kerberos: Posición oblicua del reloj con segundos de los ip_address del servidor mayores de 300 ip_address` — La dirección IP del servidor de Kerberos.Se visualiza este mensaje cuando la autenticación para un IPSec o un usuario de WebVPN a través de un servidor de Kerberos falla porque los relojes en el dispositivo de seguridad y el servidor son más de cinco minutos (300 segundos) aparte. Cuando ocurre esto, se rechaza el intento de conexión.Para resolver este problema, sincronice los relojes en el dispositivo de seguridad y el servidor de Kerberos.
2. la PRE-autenticación en el Active Directory (AD) se debe inhabilitar, o él puede llevar al error de la autenticación de usuario.
3. Los usuarios de cliente VPN no pueden autenticar contra el Microsoft certificate server. Este

mensaje de error aparece:`“Error que procesa el payload” (error 14)` Para resolver este problema, desmarque **no requieren el** checkbox de la **Autenticación previa del kerberose** en el servidor de autenticación.

Información Relacionada

- Configurar los servidores de AAA y la base de datos local
- Soporte de producto para dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems