PIX/ASA : Authentification Kerberos et groupes de serveurs d'autorisation de LDAP pour des utilisateurs de client vpn par l'intermédiaire d'exemple de configuration ASDM/CLI

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Produits connexes
Conventions
Informations générales
Configurez l'authentification et l'autorisation pour des utilisateurs VPN utilisant l'ASDM
Configurez les serveurs d'authentification et d'autorisation
Configurez un groupe de tunnel VPN pour l'authentification et l'autorisation
Configurez l'authentification et l'autorisation pour des utilisateurs VPN utilisant le CLI
Vérifiez
Dépannez
Informations connexes

Introduction

Ce document décrit comment utiliser le Cisco Adaptive Security Device Manager (ASDM) pour configurer des groupes de serveurs d'autorisation d'authentification Kerberos et de LDAP sur le Cisco PIX 500 Series Security Appliance. Dans cet exemple, les groupes de serveurs sont utilisés par la stratégie d'un groupe de tunnel VPN pour authentifier et autoriser des utilisateurs entrant.

Conditions préalables

Conditions requises

Ce document suppose que le PIX est complètement opérationnel et configuré pour permettre à l'ASDM pour apporter des modifications de configuration.

Remarque: Référez-vous à permettre à HTTPS Access pour l'ASDM afin de permettre le PIX à configurer par l'ASDM.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de logiciel 7.x d'appareils de Sécurité de Cisco PIX et plus tard
- Version 5.x et ultérieures de Cisco ASDM

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée avec la version 7.x de l'appliance de sécurité adaptable Cisco (ASA).

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Non toutes les authentification et authorizations method possibles disponibles en logiciel PIX/ASA 7.x sont prises en charge quand vous avez affaire avec des utilisateurs VPN. Cette table détaille quelles méthodes sont disponibles pour des utilisateurs VPN :

	Gens du pays	RAYON	TACACS+	SDI	NT	Kerberos	LDAP
Authentification	Oui	Oui	Oui	Oui	Oui	Oui	Non
Autorisation	Oui	Oui	Non	Non	Non	Non	Oui

Remarque: Le Kerberos est utilisé pour l'authentification et le LDAP est utilisé pour l'autorisation des utilisateurs VPN dans cet exemple.

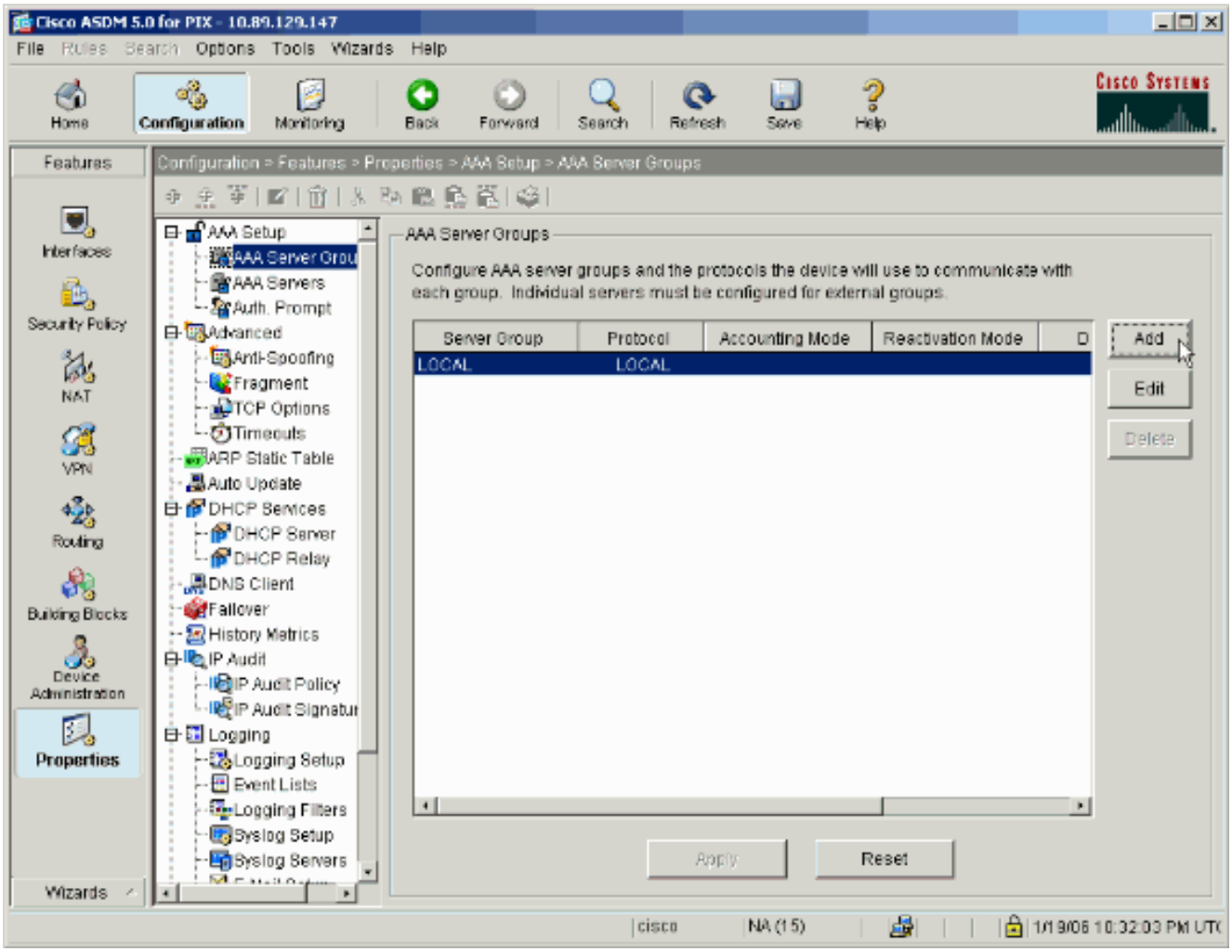
Configurez l'authentification et l'autorisation pour des utilisateurs VPN utilisant l'ASDM

Configurez les serveurs d'authentification et d'autorisation

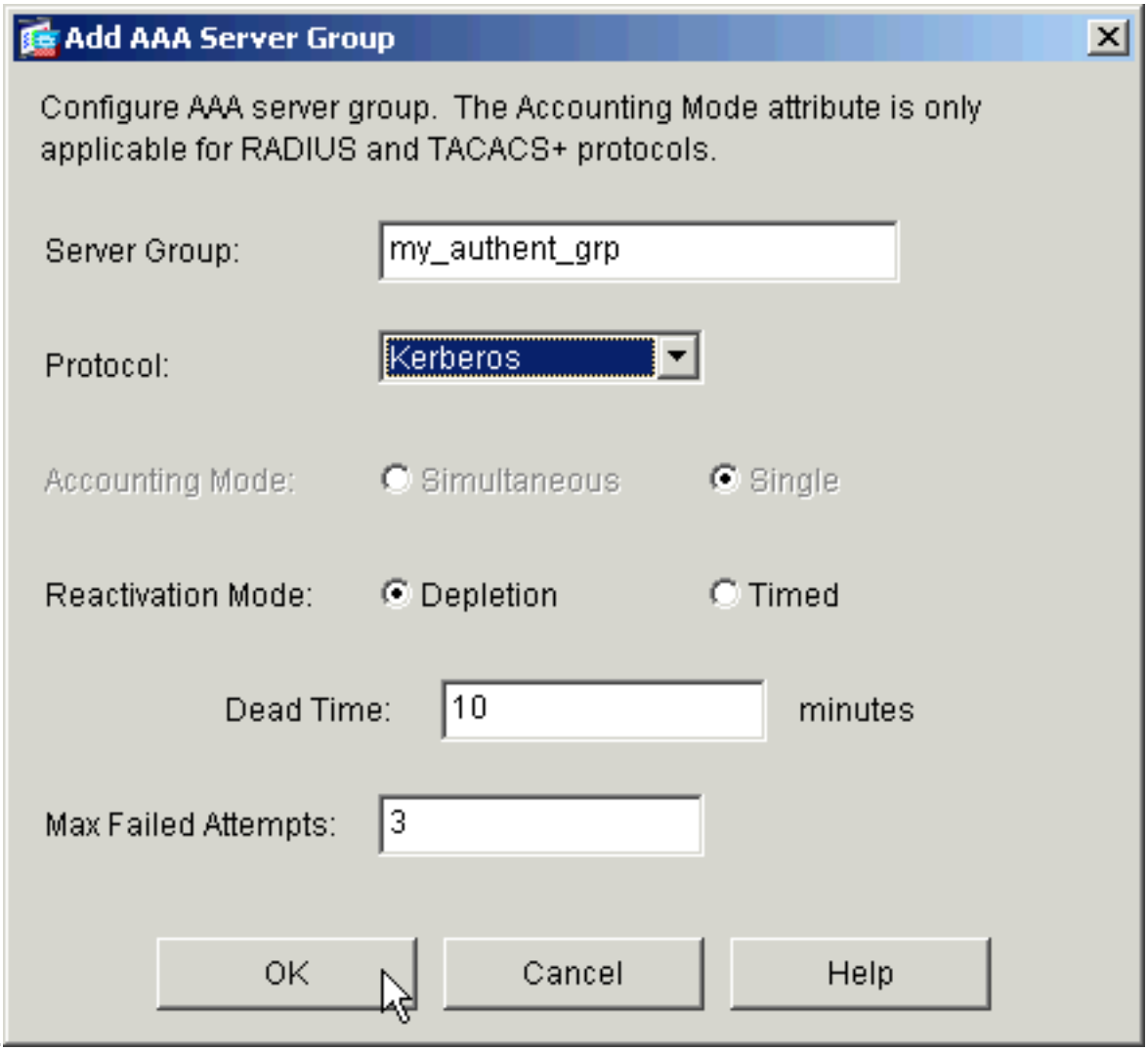
Terminez-vous ces étapes afin de configurer des groupes de serveurs d'authentification et d'autorisation pour des utilisateurs VPN par l'ASDM.

1. Choisissez la **configuration > le Properties > l'AAA installé > des Groupes de serveurs AAA**,

et cliquez sur
Add.

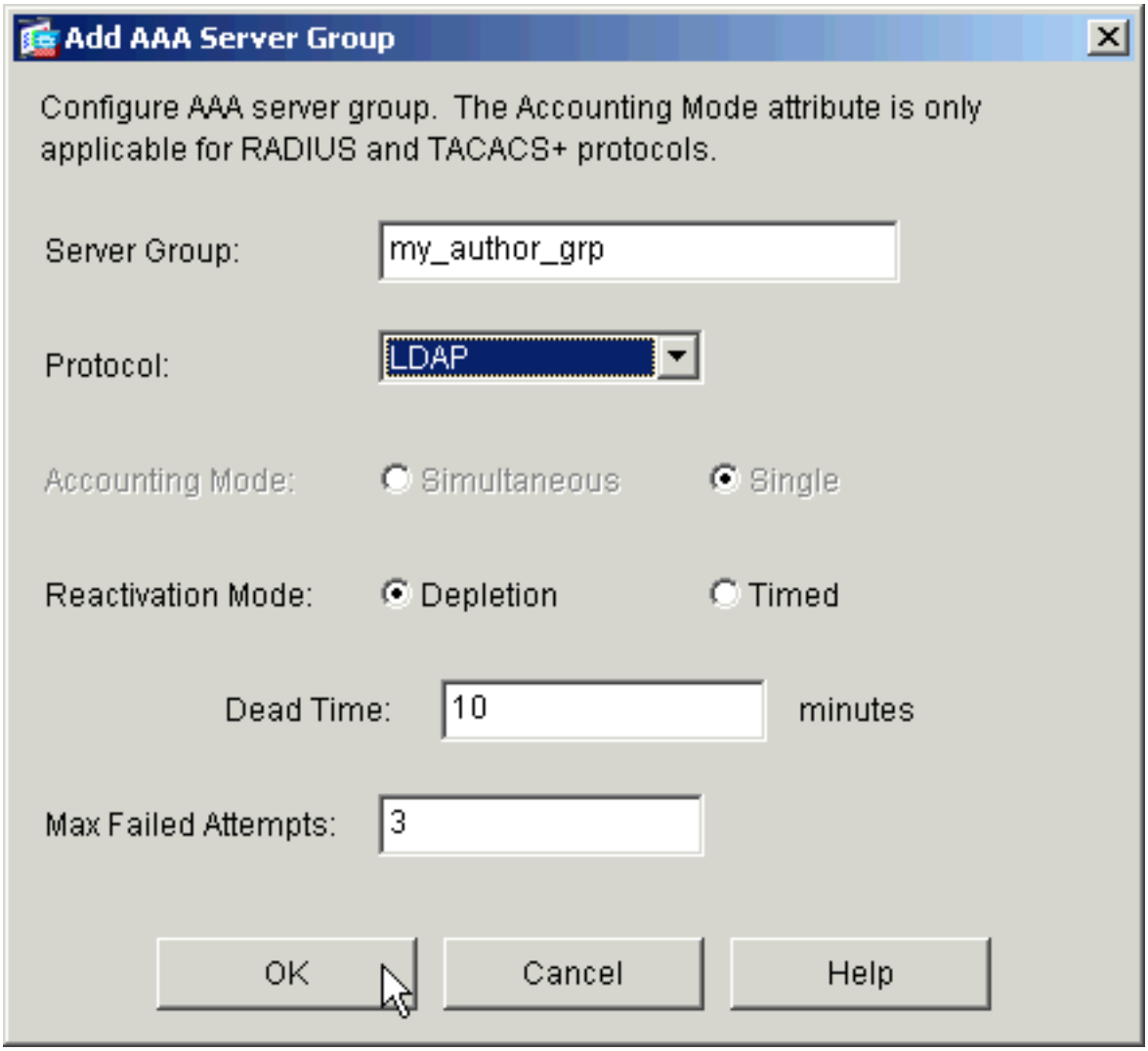


2. Définissez un nom pour le nouveau groupe de serveurs d'authentification, et choisissez un protocole.L'option de mode comptable est pour le RAYON et le TACACS+ seulement. Cliquez sur **OK** quand vous avez

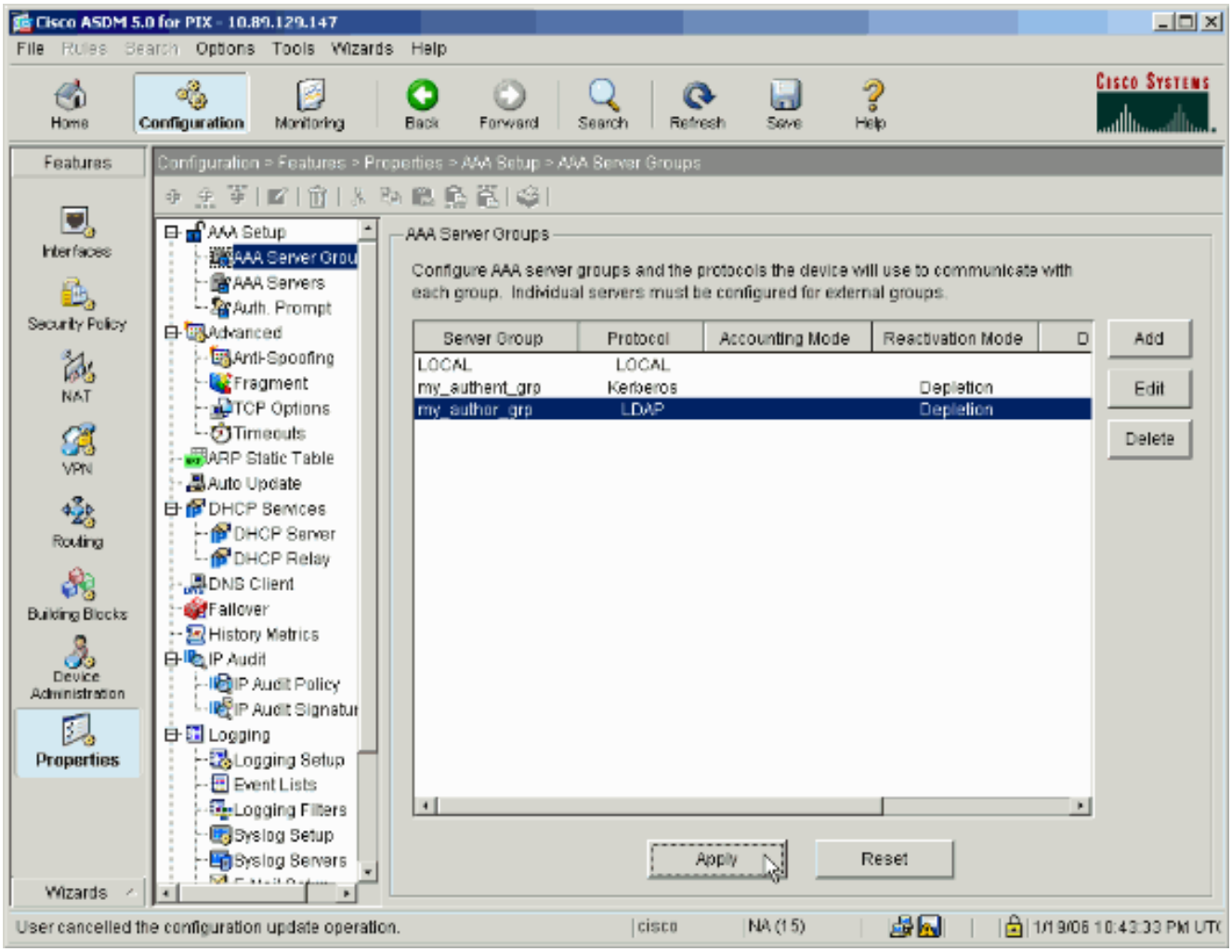


terminé.

3. Répétez les étapes 1 et 2 afin de créer un nouveau groupe de serveurs d'autorisation.

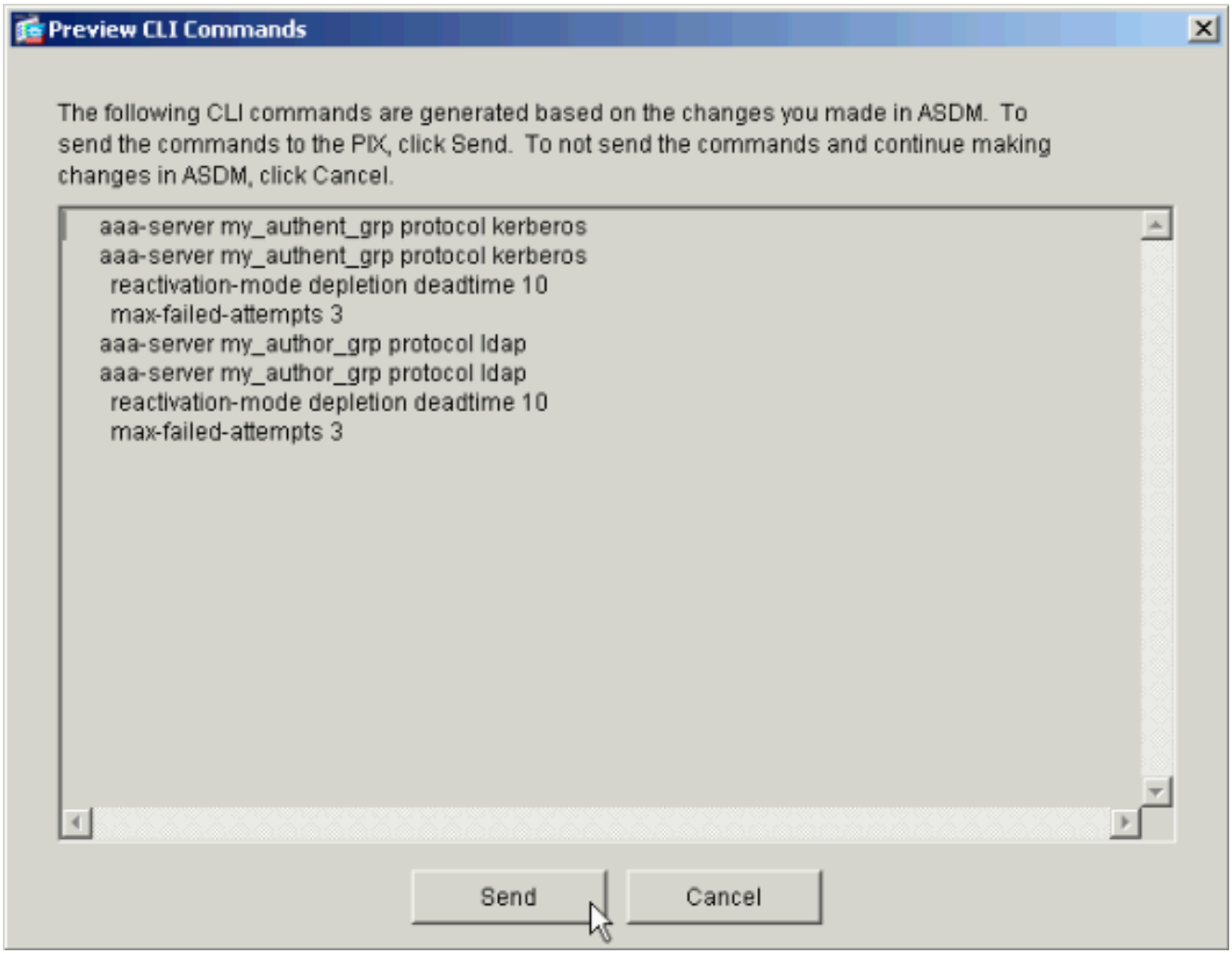


4. Cliquez sur Apply afin d'envoyer les modifications au périphérique.



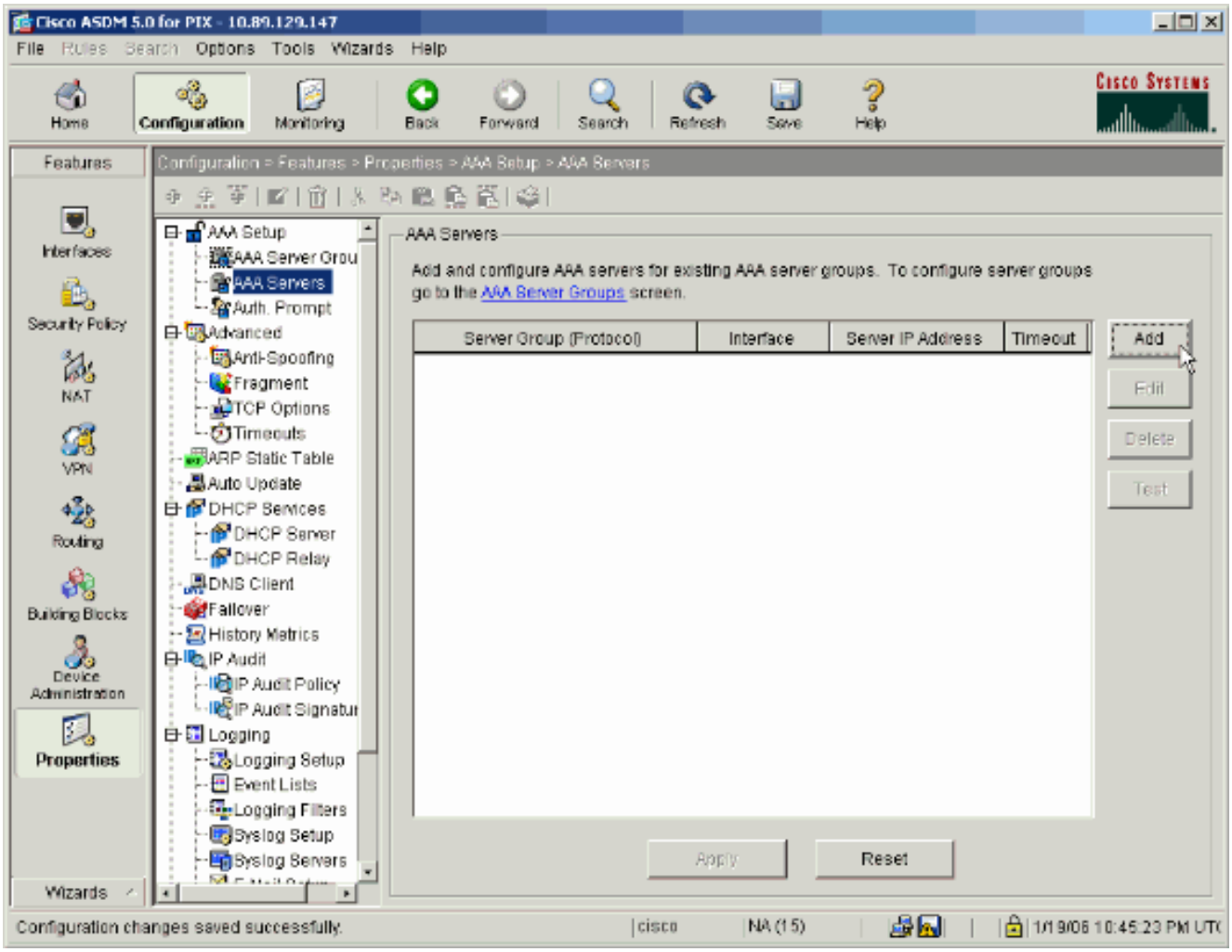
Si vous le faites configurer pour faire ainsi, le périphérique visionne maintenant les commandes préalablement qui sont ajoutées à la configuration en cours.

5. Le clic **envoient** afin d'envoyer les commandes au périphérique.

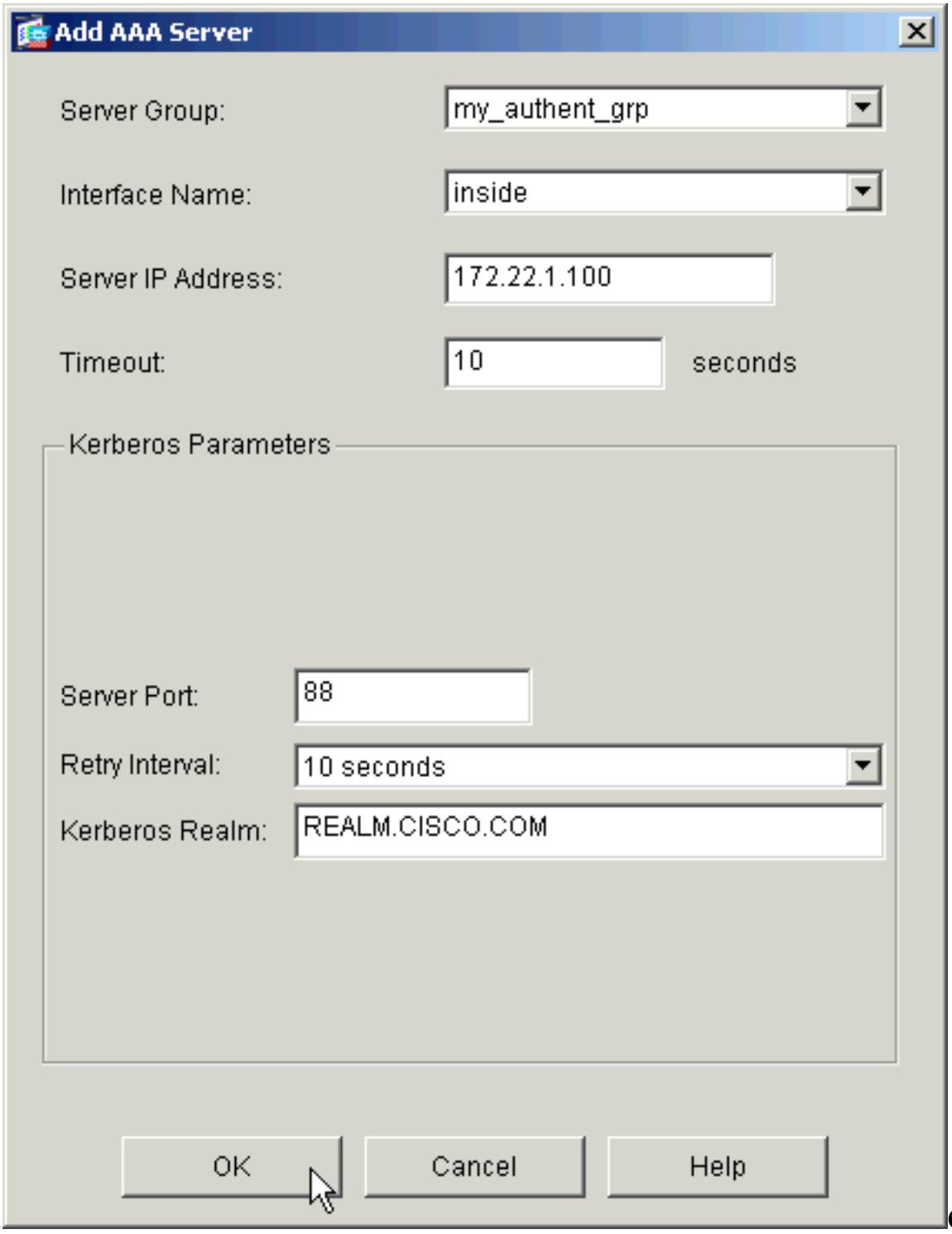


Les groupes de serveurs de création récente doivent maintenant être remplis avec des serveurs d'authentification et d'autorisation.

6. Choisissez la **configuration > le Properties > l'AAA installé > des serveurs d'AAA**, et cliquez sur
Add.

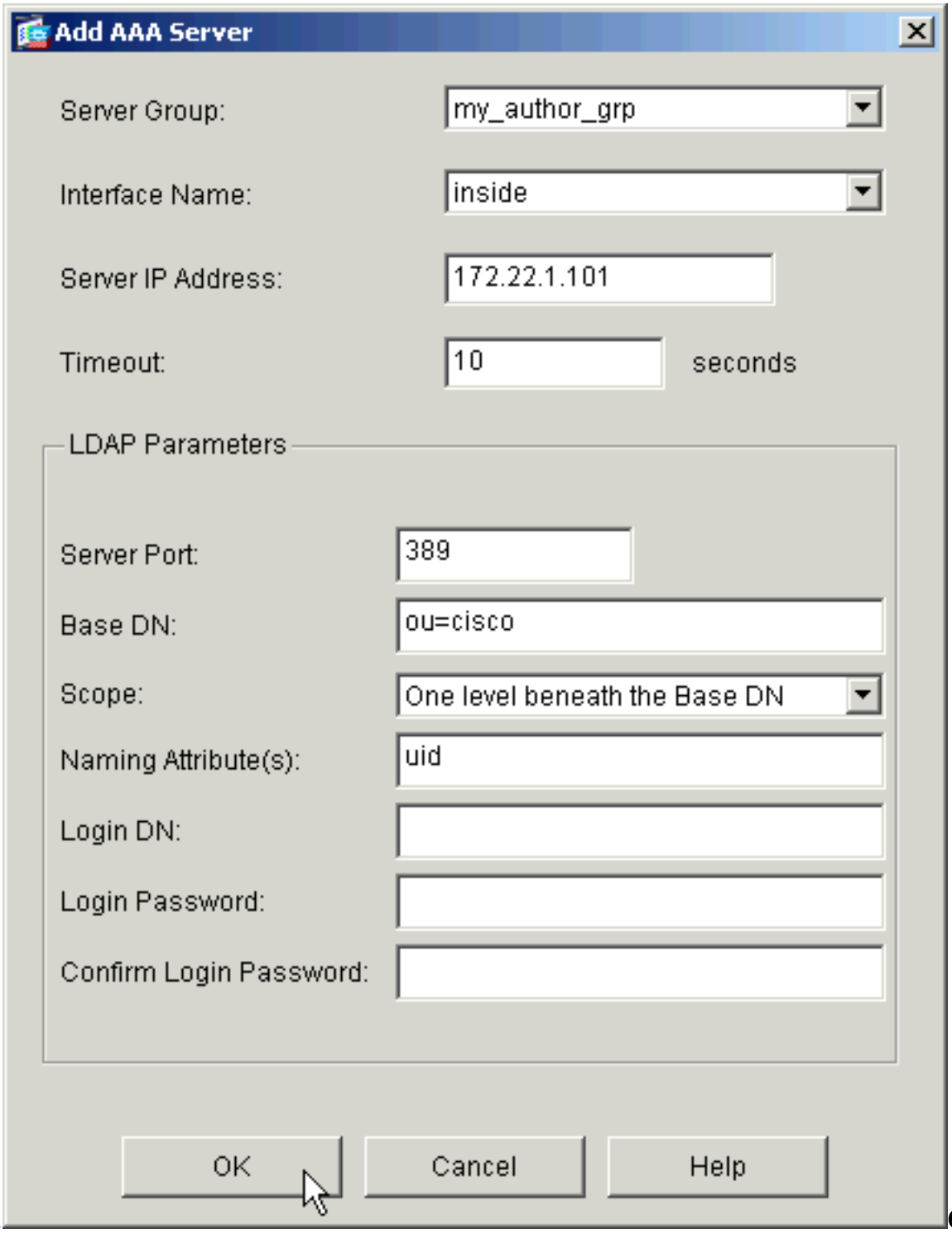


7. Configurez un serveur d'authentification. Cliquez sur **OK** quand vous avez



terminé.**Groupe de serveurs** — Choisissez le groupe de serveurs d'authentification configuré dans l'étape 2.**Nom d'interface** — Choisissez l'interface sur laquelle le serveur réside.**Adresse IP du serveur** — Spécifiez l'adresse IP du serveur d'authentification.**Délai d'attente** — Spécifiez l'heure maximum, en quelques secondes, d'attendre une réponse du serveur.**Paramètres de Kerberos :Port de serveur** — 88 est le port standard pour le Kerberos.**Retry interval** — Choisissez le retry interval désiré.**Royaume de Kerberos** — Écrivez le nom de votre royaume de Kerberos. C'est fréquemment le nom de domaine de Windows dans toutes les lettres majuscules.

8. Configurez un serveur d'autorisation. Cliquez sur OK une fois



terminé.**Groupe de serveurs** — Choisissez le groupe de serveurs d'autorisation configuré dans l'étape 3.**Nom d'interface** — Choisissez l'interface sur laquelle le serveur réside.**Adresse IP du serveur** — Spécifiez l'adresse IP du serveur d'autorisation.**Délai d'attente** — Spécifiez l'heure maximum, en quelques secondes, d'attendre une réponse du serveur.**Paramètres de LDAP :Port de serveur** — 389 est le port par défaut pour le LDAP.**DN de base** — Entrez l'emplacement dans la hiérarchie de LDAP où le serveur devrait commencer au rechercher une fois reçoit une demande d'autorisation.**Portée** — Choisissez le point auquel le serveur devrait rechercher la hiérarchie de LDAP une fois qu'elle reçoit une demande d'autorisation.**Nommant des attributs** — Écrivez les attributs de nom unique relatifs par lesquels des entrées sur le serveur LDAP sont seulement définies. Les attributs nommants communs sont le nom commun (NC) et l'user-id (uid).**DN de procédure de connexion** — Quelques serveurs LDAP, y compris le serveur de Microsoft Active Directory, exigent du périphérique pour établir une prise de contact par l'intermédiaire de l'attache authentifiée

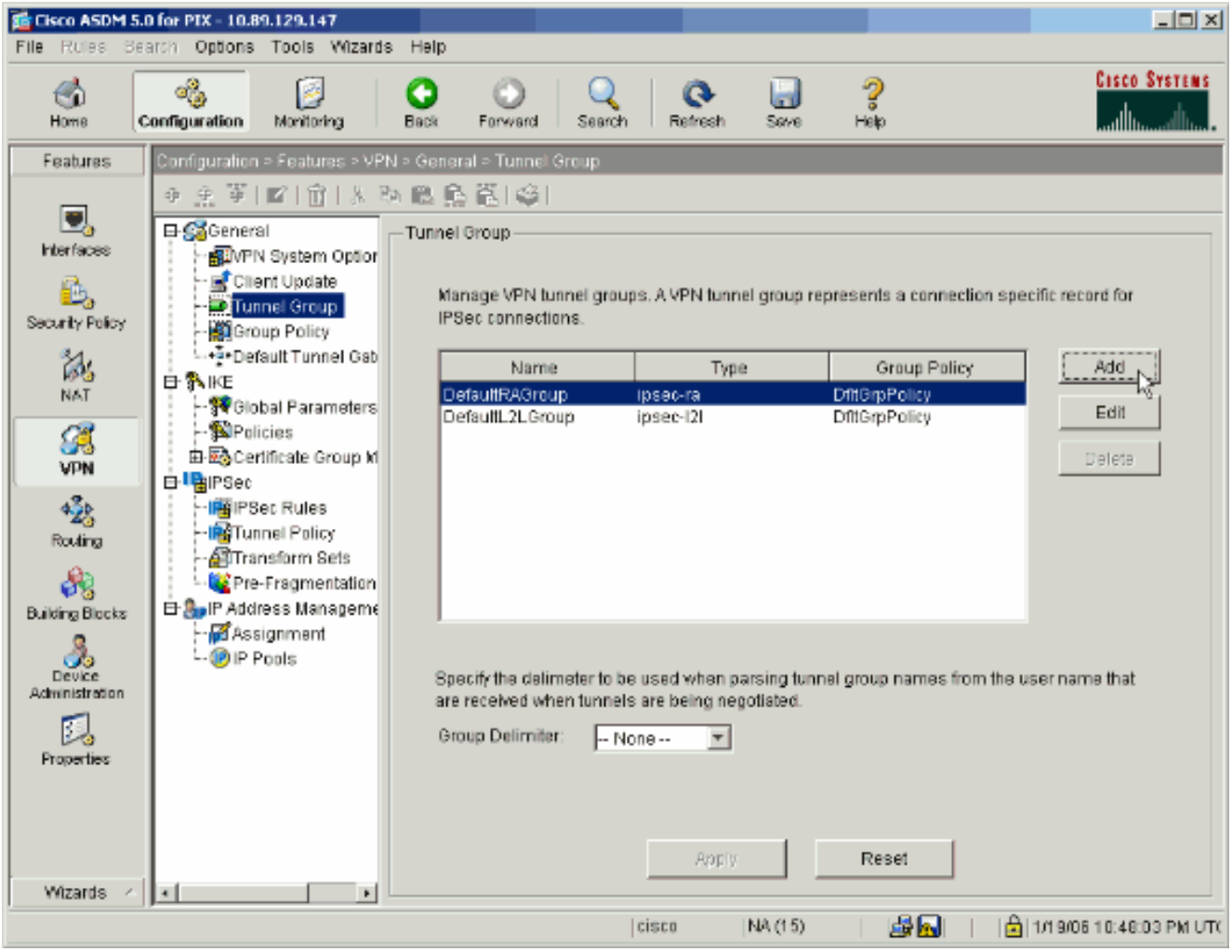
avant qu'ils reçoivent des demandes de toutes les autres exécutions de LDAP. Le gisement de DN de procédure de connexion définit les caractéristiques d'authentification du périphérique, qui devrait correspondre à ceux d'un utilisateur aux privilèges de gestion. Par exemple, cn=administrator. Pour l'accès anonyme, laissez ce champ vide.**Mot de passe de connexion** — Entrez le mot de passe pour le DN de procédure de connexion.**Confirmez le mot de passe de connexion** — Confirmez le mot de passe pour le DN de procédure de connexion.

9. Cliquez sur Apply afin d'envoyer les modifications à l'authentification de périphérique après tout et des serveurs d'autorisation sont ajoutés.Si vous le faites configurer pour faire ainsi, le PIX visionne maintenant les commandes préalablement qui sont ajoutées à la configuration en cours.
10. Le clic **envoient** afin d'envoyer les commandes au périphérique.

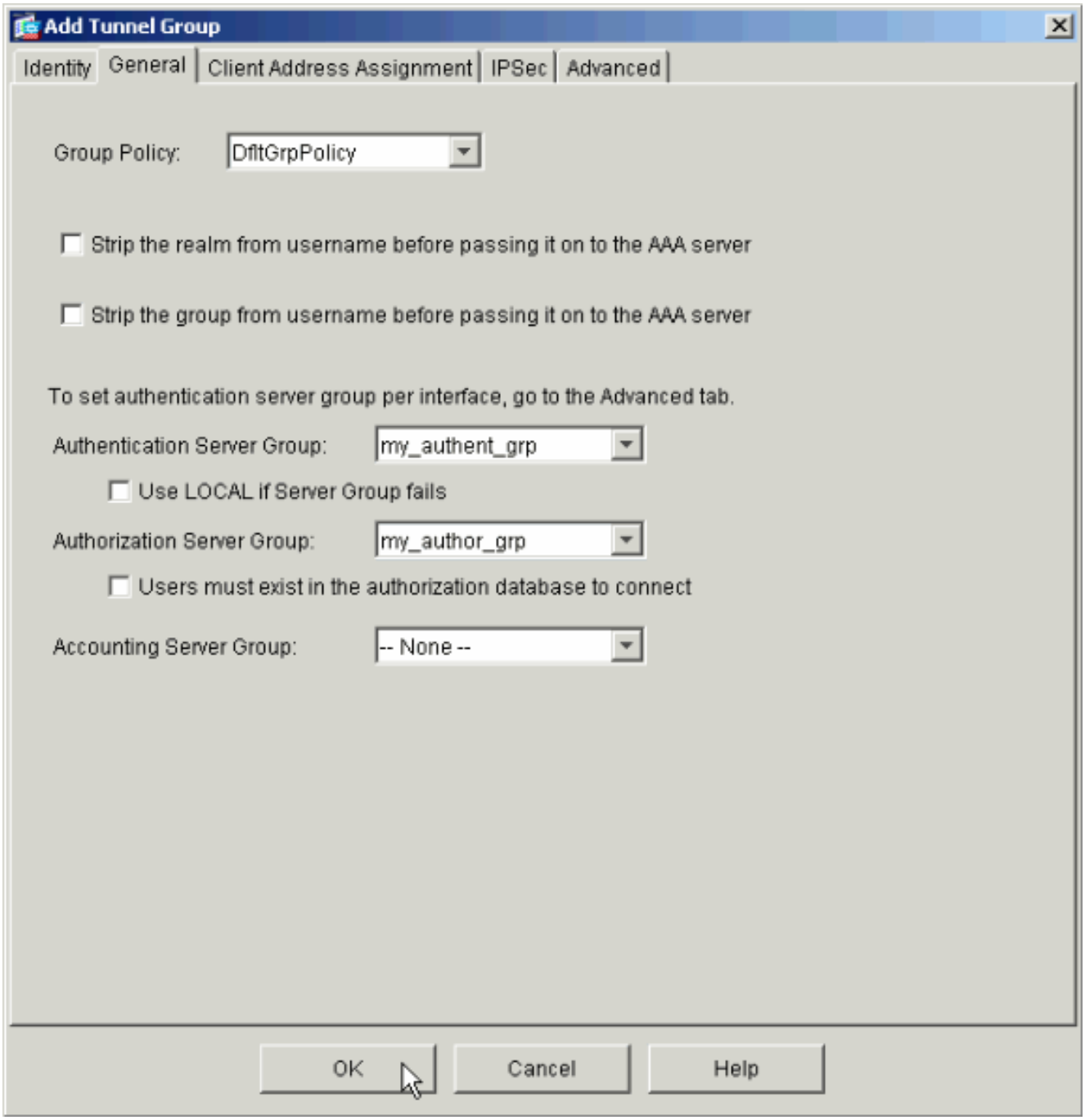
Configurez un groupe de tunnel VPN pour l'authentification et l'autorisation

Terminez-vous ces étapes afin d'ajouter les groupes de serveurs que vous avez juste configurés à un groupe de tunnel VPN.

1. Choisissez la **configuration > le VPN > le groupe de tunnel**, et cliquez sur Add afin de créer un nouveau groupe de tunnel, ou **les éditez** afin de modifier un groupe existant.



2. Sur l'onglet Général de la fenêtre qui apparaît, sélectionnez les groupes de serveurs configurés plus tôt.



3. *Facultatif :* Configurez les paramètres restants sur les autres onglets si vous ajoutez un nouveau groupe de tunnel.
4. Cliquez sur **OK** quand vous avez terminé.
5. Cliquez sur Apply afin d'envoyer les modifications au périphérique après que la configuration de groupe de tunnel soit complète.Si vous le faites configurer pour faire ainsi, le PIX visionne maintenant les commandes préalablement qui sont ajoutées à la configuration en cours.
6. Le clic **envoient** afin d'envoyer les commandes au périphérique.

Configurez l'authentification et l'autorisation pour des utilisateurs VPN utilisant le CLI

C'est la configuration équivalente CLI pour les groupes de serveurs d'authentification et d'autorisation pour des utilisateurs VPN.

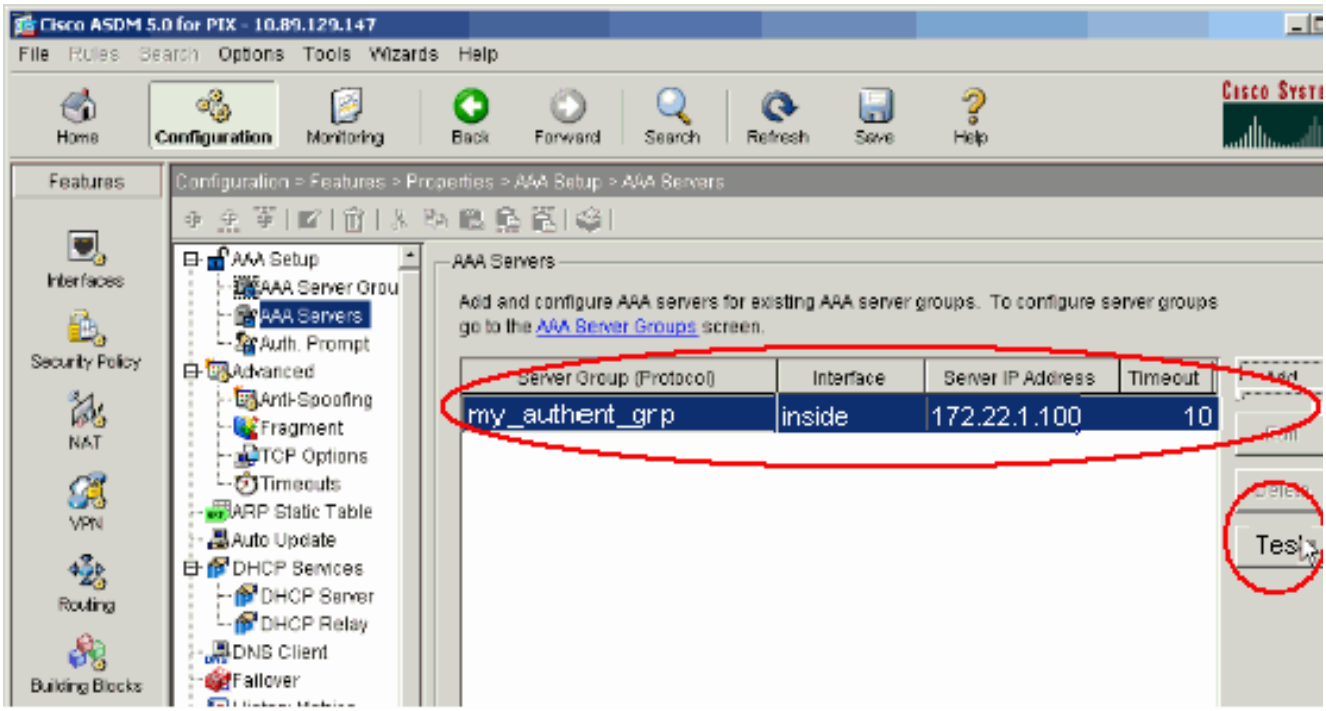
Configuration CLI de dispositifs de sécurité

```
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.
```

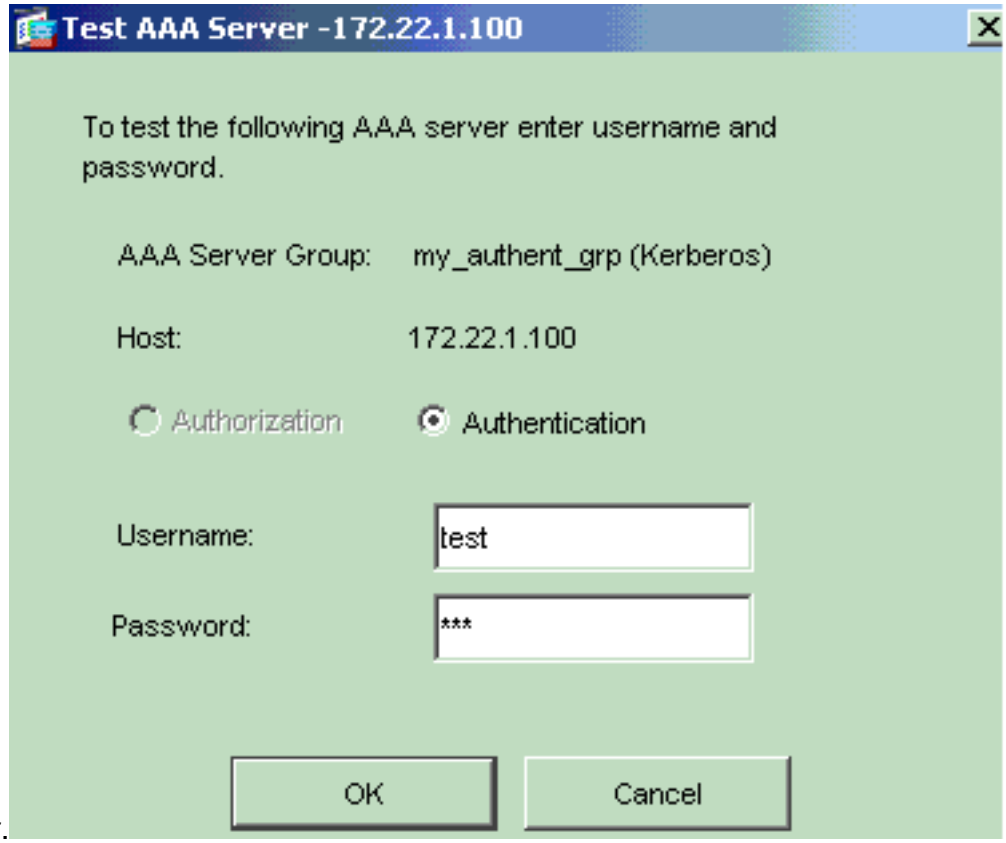
Vérifiez

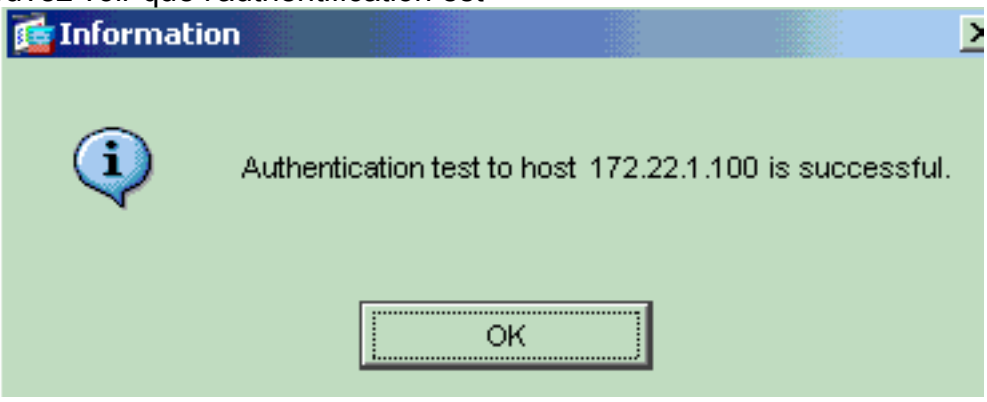
Terminez-vous ces étapes afin de vérifier l'authentification de l'utilisateur entre le serveur PIX/ASA et d'AAA :

1. Choisissez la **configuration > le Properties > l'AAA installé > des serveurs d'AAA**, et sélectionnez le groupe de serveurs (my_authent_grp). Cliquez sur alors le **test** afin de valider les identifiants
utilisateurs.



2. Fournissez le nom d'utilisateur et mot de passe (par exemple, nom d'utilisateur : test et mot de passe : le test), et cliquent sur OK afin de

valider. 

3. Vous pouvez voir que l'authentification est réussie. 

Dépannez

1. Une cause fréquente d'échec d'authentification est distorsion d'horloge. Soyez sûr que les horloges sur le PIX ou l'ASA et votre serveur d'authentification sont synchronisés.Quand l'authentification échoue dû pour synchroniser la distorsion, vous pouvez recevoir ce message d'erreur : `: - ERREUR : Authentification rejetée : Secondes obliques d'horloge plus considérablement que 300`. En outre, ce message de log apparaît :`%PIX|ASA-3-113020 : Erreur de Kerberos : Synchronisez la distorsion avec secondes d'ip_address de serveur de plus grandes que 300 ip_address` — L'adresse IP du serveur de Kerberos.Ce message est affiché quand l'authentification pour un IPSec ou un utilisateur WebVPN par un serveur de Kerberos échoue parce que les horloges sur les dispositifs de sécurité et le serveur sont plus de cinq minutes (300 secondes) à part. Quand ceci se produit, la tentative de connexion est rejetée.Afin de résoudre ce problème, synchronisez les horloges sur les dispositifs de sécurité et le serveur de Kerberos.
2. la Pré-authentification sur le Répertoire actif (AD) doit être désactivée, ou il peut mener à la panne d'authentification de l'utilisateur.

3. Les utilisateurs de client vpn ne peuvent pas authentifier contre le Microsoft Certificate Server. Ce message d'erreur apparaît :`« Erreur traitant la charge utile » (erreur 14)` Afin de résoudre ce problème, décochez **n'exigent pas la** case à cocher de **Préauthentification de kerberose** sur le serveur d'authentification.

Informations connexes

- Configurer les serveurs d'AAA et la base de données locale
- Assistance produit des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems