PIX/ASA: مجموعات خوادم مصادقة Kerberos وتفويض LDAP لمستخدمي عميل VPN عبر ASDM/CLI مثال تكوين

المحتويات

المقدمة

يصف هذا المستند كيفية إستخدام مدير أجهزة الأمان المعدلة (ASDM) من Cisco لتكوين مصادقة Kerberos ومجموعات خادم تفويض LDAP على جهاز الأمان Cisco PIX 500 Series Security Appliance. في هذا المثال، يتم إستخدام مجموعات الخوادم بواسطة نهج مجموعة أنفاق VPN لمصادقة المستخدمين الواردين وتخويلهم.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن PIX قيد التشغيل الكامل وتم تكوينه للسماح ل ASDM بإجراء تغييرات التكوين.

ملاحظة: راجع السماح بوصول HTTPS ل ASDM للسماح بتكوين PIX بواسطة ASDM.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج جهاز أمان PIX من Cisco الإصدار x.7 والإصدارات الأحدث
- Cisco ASDM، الإصدار x.5 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان القابل للتكيف (ASA) من Cisco، الإصدار x.7.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

لا يتم دعم جميع طرق المصادقة والتفويض الممكنة المتوفرة في برنامج PIX/ASA 7.x عند التعامل مع مستخدمي VPN. يوضح هذا الجدول الطرق المتوفرة لمستخدمي الشبكة الخاصة الظاهرية (VPN):

	محلي	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
المصادقة	نعم	نعم	نعم	نعم	نعم	نعم	لا
الاعتماد	نعم	نعم	لا	لا	لا	لا	نعم

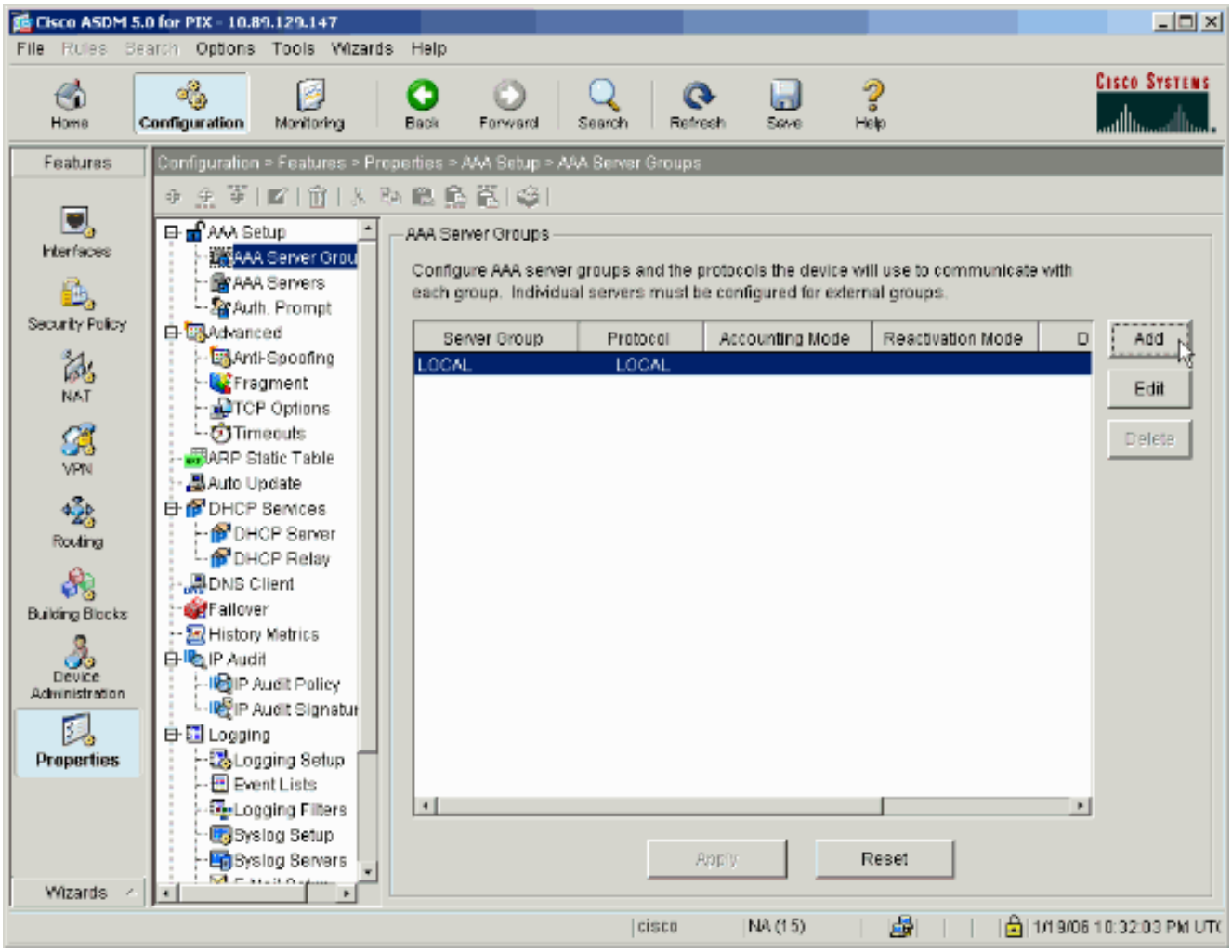
ملاحظة: يتم إستخدام Kerberos للمصادقة ويستخدم LDAP لتفويض مستخدمي VPN في هذا المثال.

تكوين المصادقة والتفويض لمستخدمي VPN باستخدام ASDM

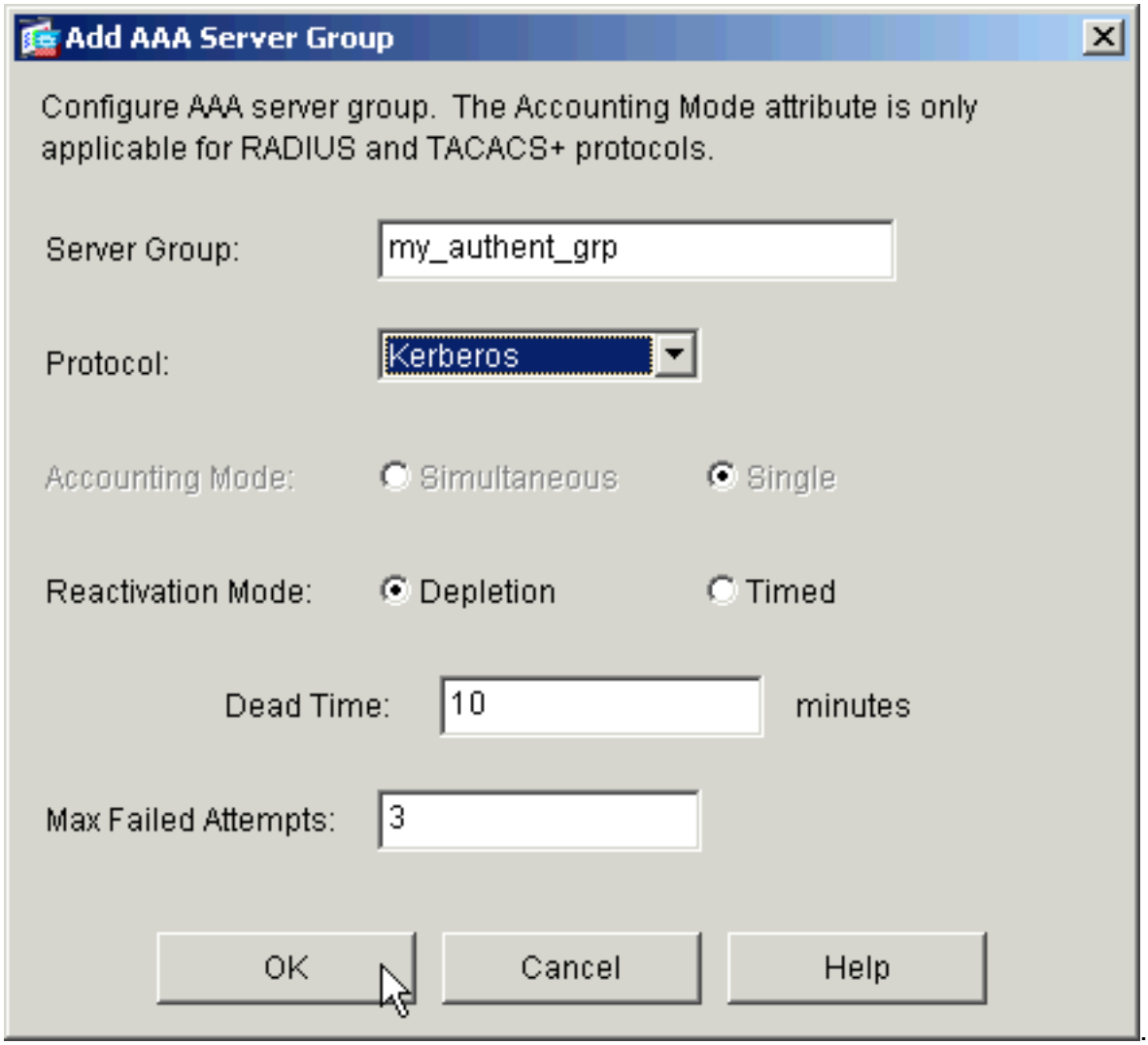
تكوين خوادم المصادقة والتفويض

أكمل هذه الخطوات لتكوين مجموعات خوادم المصادقة والتفويض لمستخدمي VPN من خلال ASDM.

1. أختر **تكوين > خصائص > إعداد AAA > مجموعات خوادم AAA**، وانقر **إضافة**.

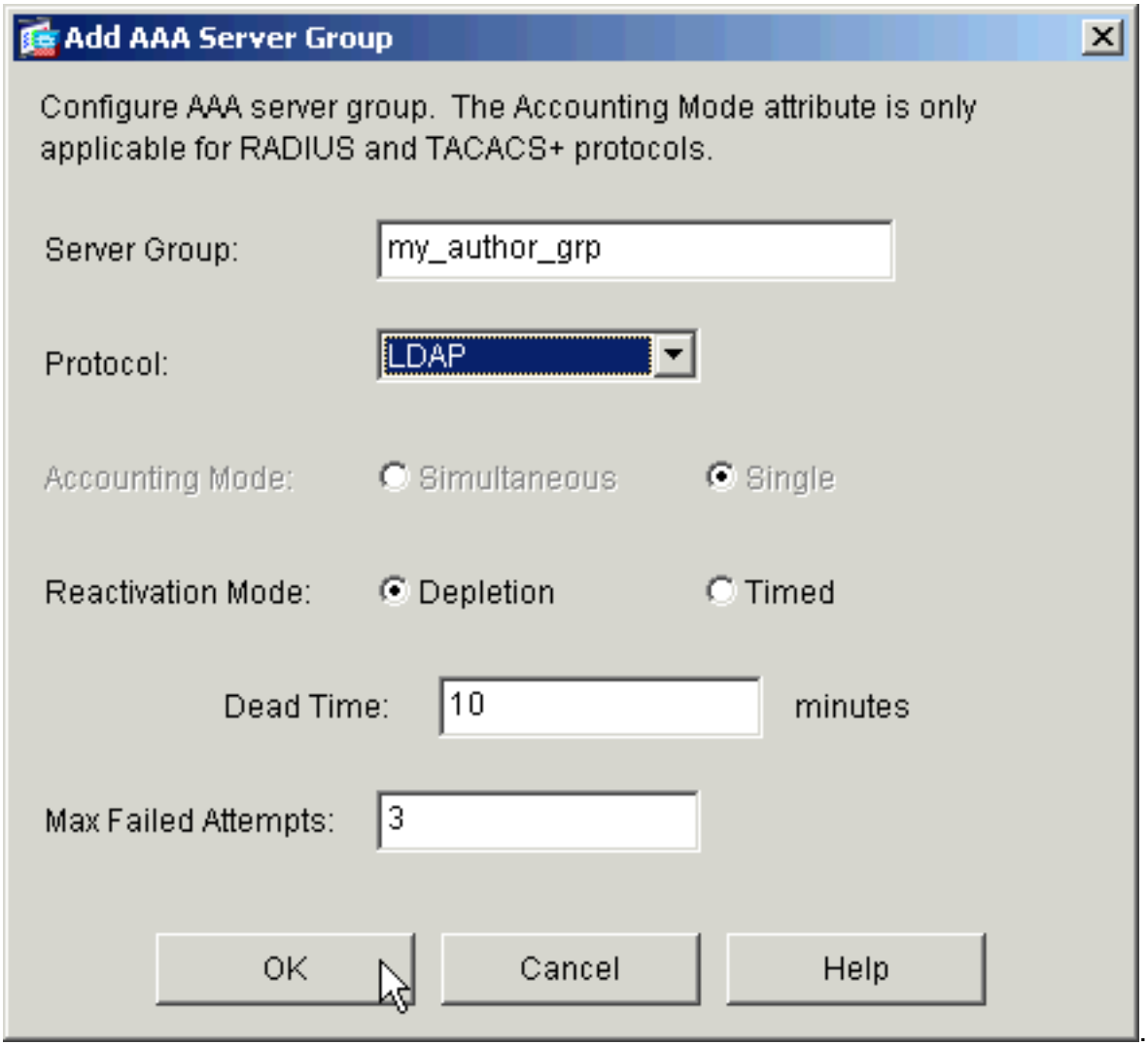


2. قم بتحديد اسم لمجموعة خوادم المصادقة الجديدة، واختر بروتوكولا.يكون خيار وضع المحاسبة ل RADIUS و TACACS+ فقط. انقر فوق موافق عند



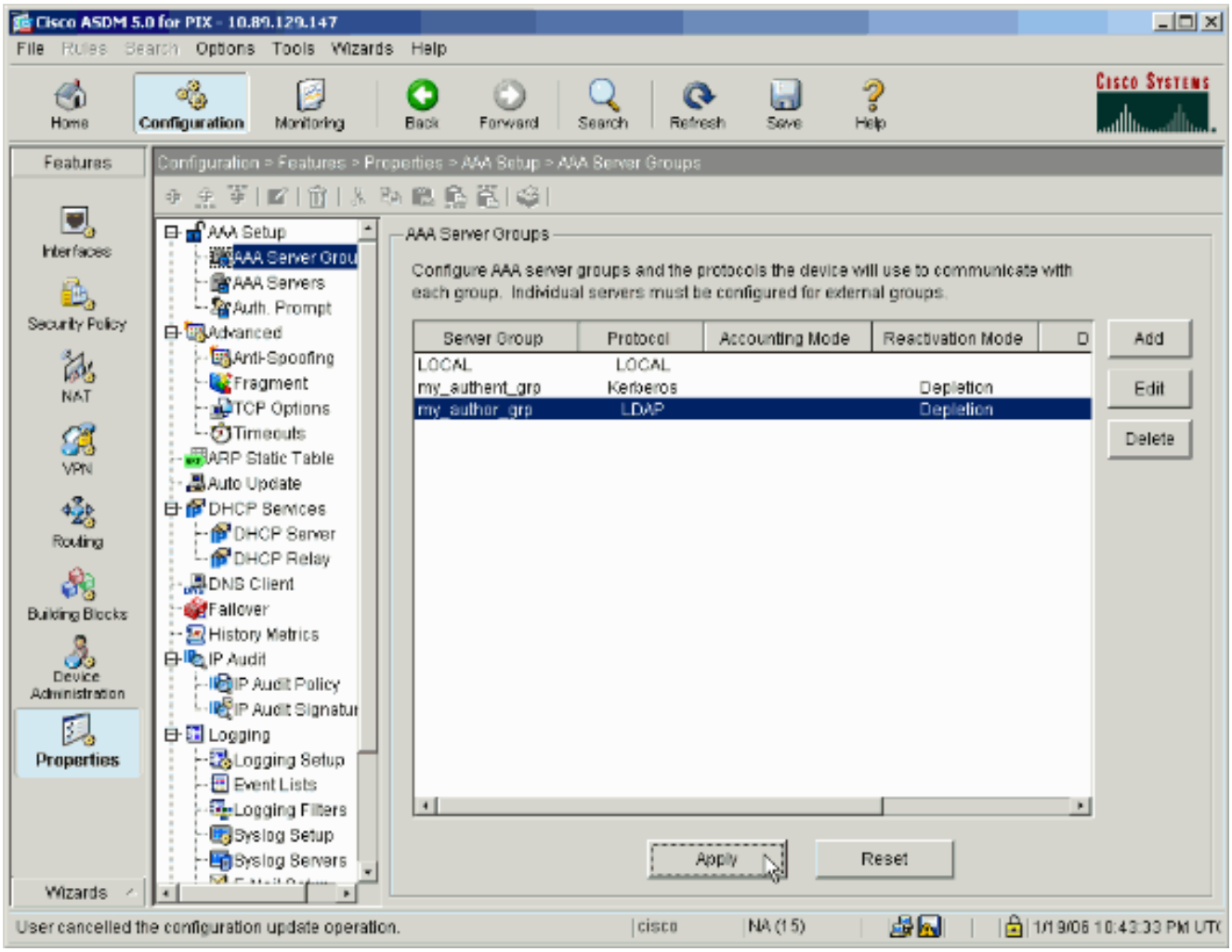
الانتهاء.

3. كرر الخطوات 1 و 2 لإنشاء مجموعة خوادم تخويل



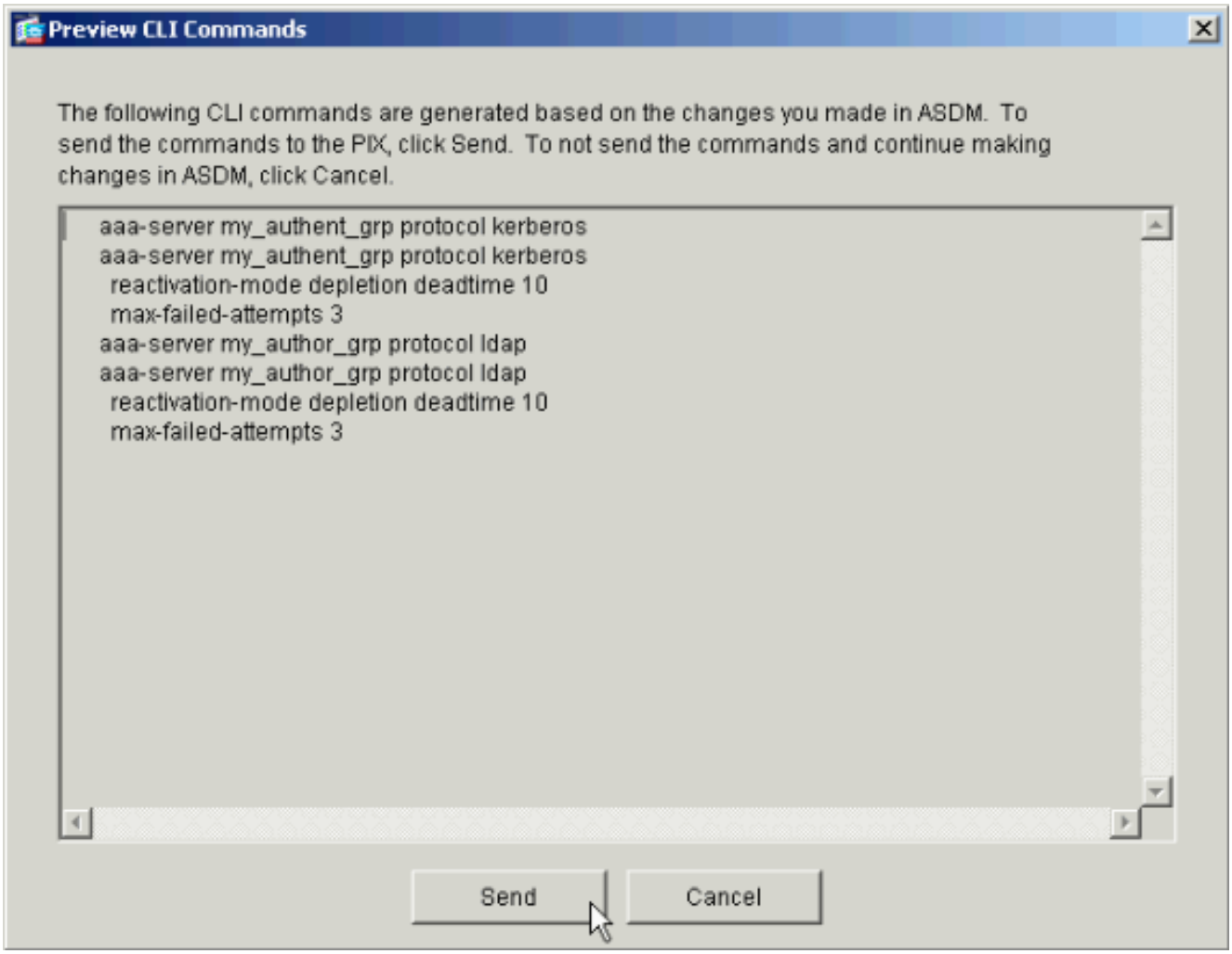
جديدة.

4. انقر فوق **تطبيق** لإرسال التغييرات إلى الجهاز.



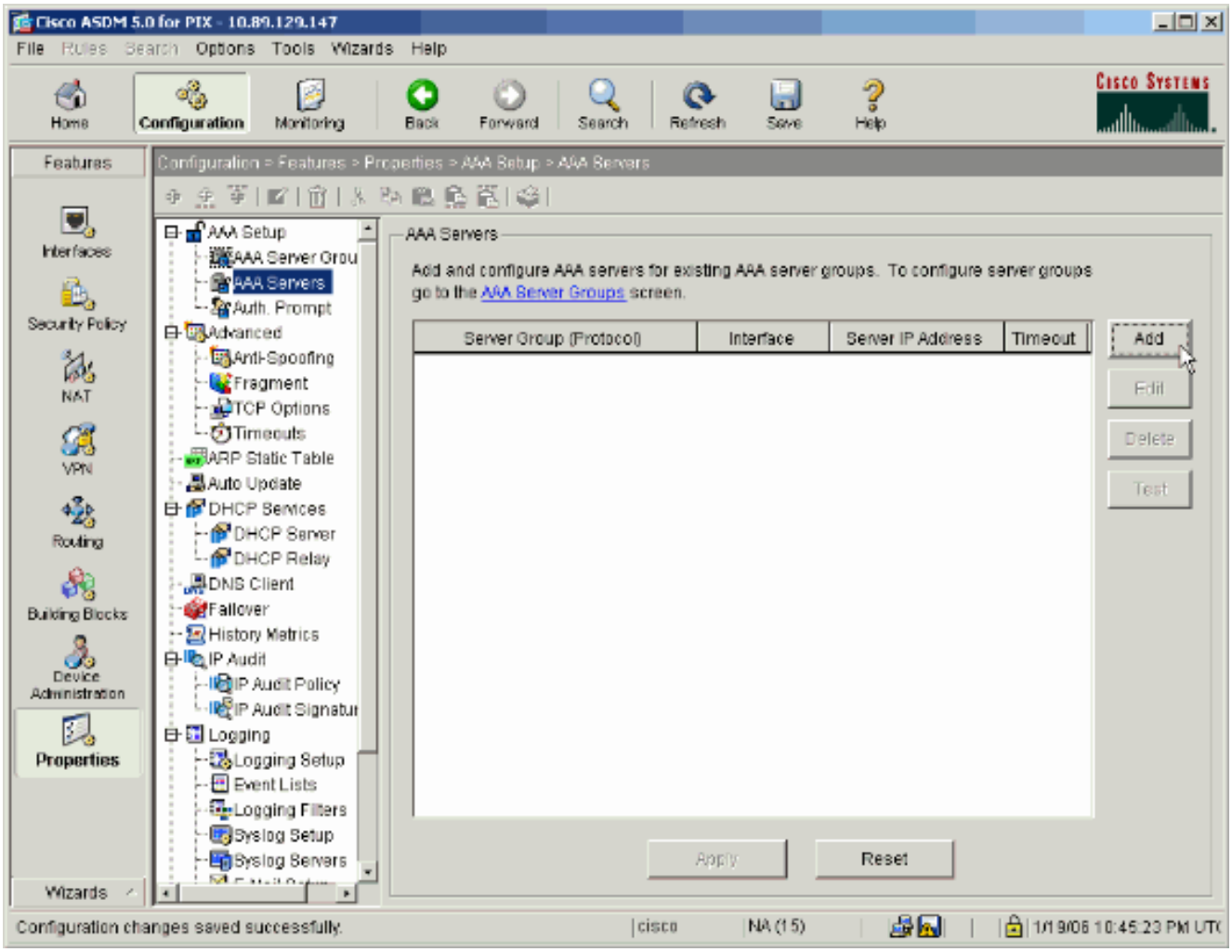
إذا قمت بتكوينه للقيام بذلك، فإن الجهاز يقوم الآن بمعاينة الأوامر التي يتم إضافتها إلى التكوين الجاري تشغيله.

5. طقطقة **يرسل** in order to أرسلت الأمر إلى الأداة.

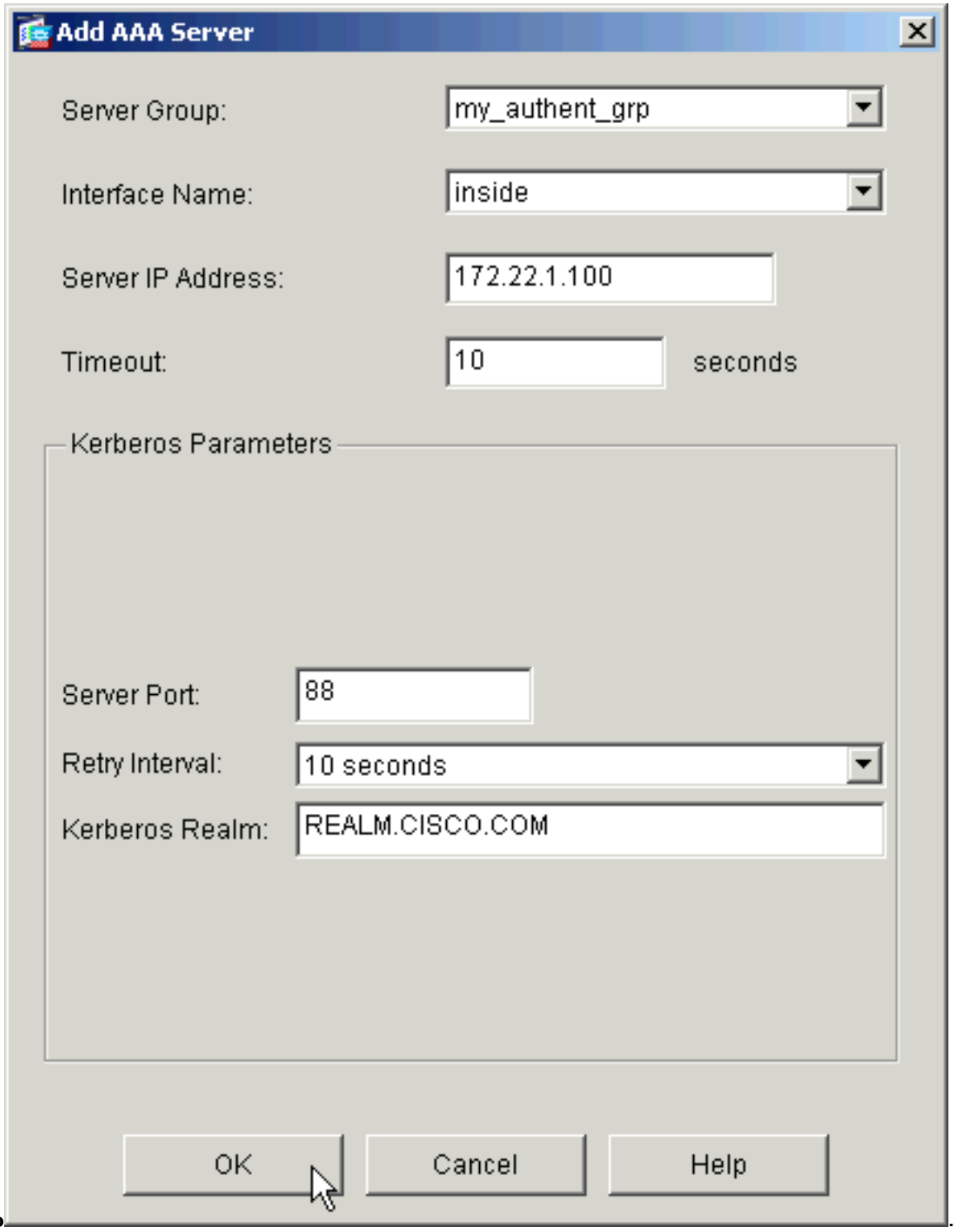


يجب ملء مجموعات الخوادم التي تم إنشاؤها حديثا الآن بخوادم المصادقة والتخويل.

6. أختر **تكوين > خصائص > إعداد AAA > خوادم AAA**، وانقر **إضافة**.

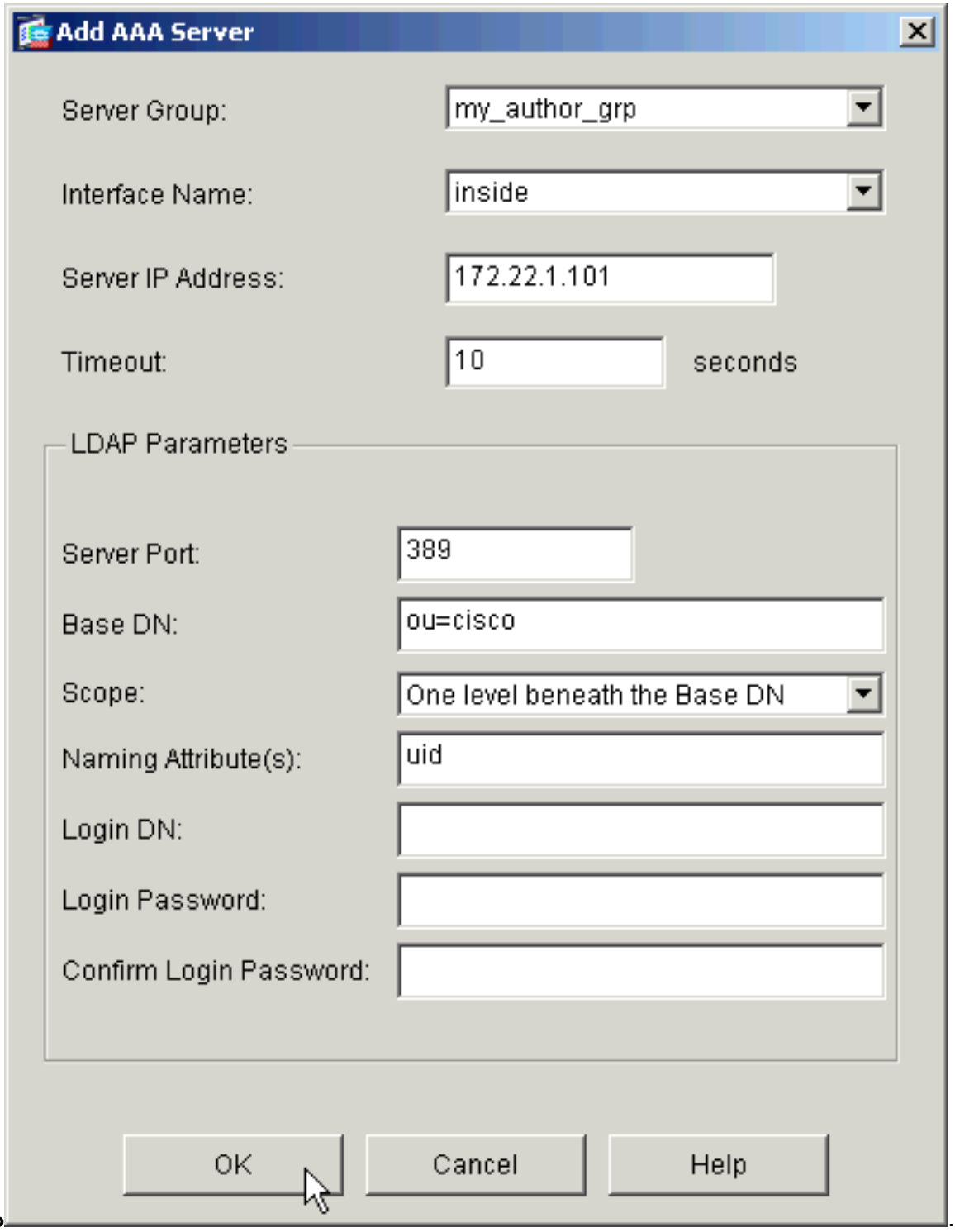


7. قم بتكوين خادم مصادقة. انقر فوق موافق عند



الانتهاء.**مجموعة الخوادم**—أختر مجموعة خوادم المصادقة التي تم تكوينها في الخطوة 2.**اسم الواجهة**— أختر الواجهة التي يتواجد عليها الخادم.**عنوان IP للخادم**—حدد عنوان IP الخاص بخادم المصادقة.**المهلة**— حدد الحد الأقصى للوقت، بالثواني، للانتظار إستجابة من الخادم.**معلمات Kerberos:منفذ الخادم**—88 هو المنفذ القياسي ل Kerberos.**الفاصل الزمني لإعادة المحاولة**— أختر الفاصل الزمني لإعادة المحاولة المطلوب.**عالم Kerberos**—أدخل اسم عالم Kerberos. غالبا ما يكون هذا هو اسم مجال Windows في كافة الأحرف الكبيرة.

8. قم بتكوين خادم تفويض. طقطقة **ok** عندما



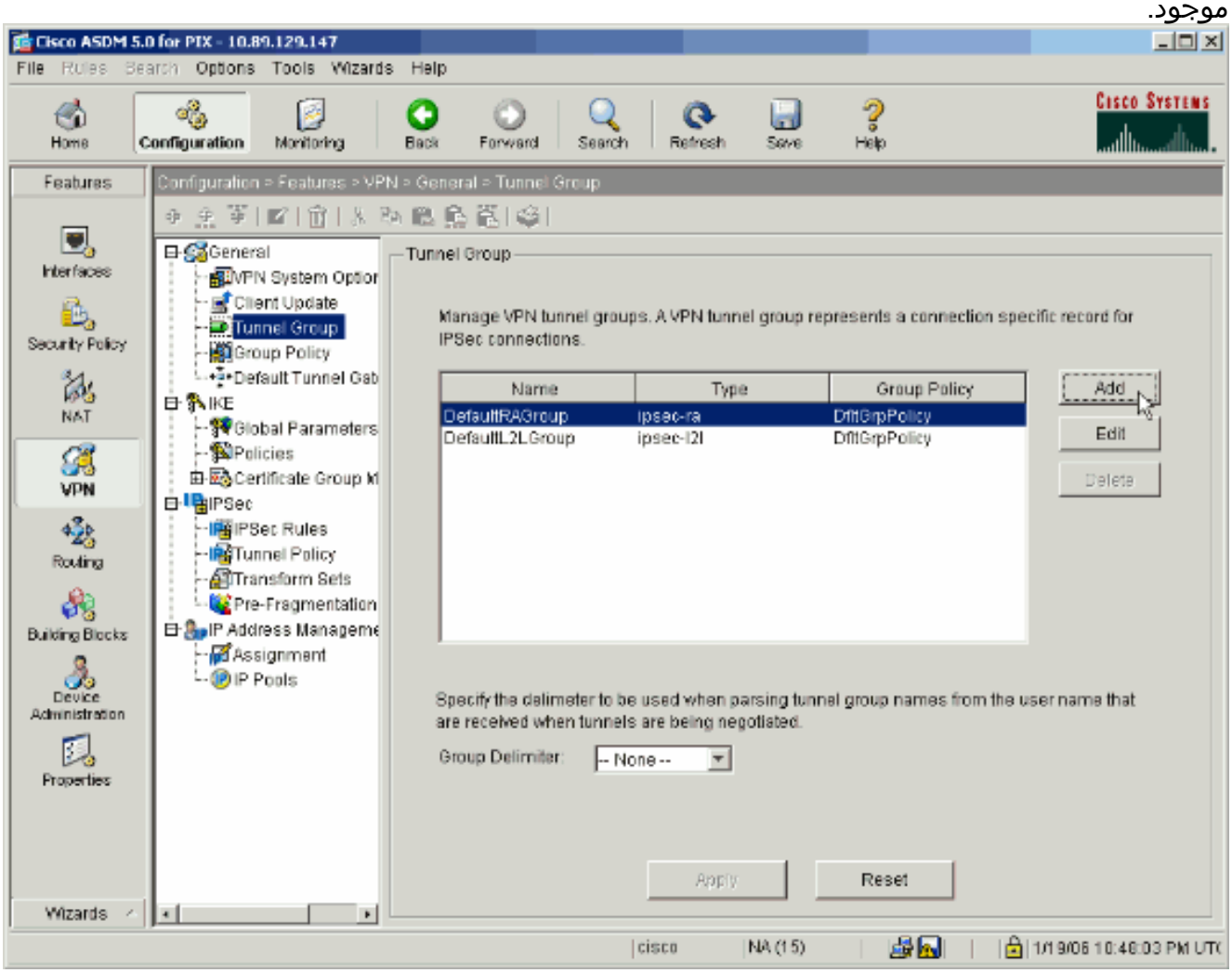
إنتهيت.**مجموع ة الخوادم**—أختر مجموعة خوادم التخويل التي تم تكوينها في الخطوة 3.**اسم الواجهة**— أختر الواجهة التي يتواجد عليها الخادم.**عنوان IP للخادم**—حدد عنوان IP الخاص بخادم التخويل.**المهلة**— حدد الحد الأقصى للوقت، بالثواني، للانتظار إستجابة من الخادم.**معلمات LDAP:منفذ الخادم**—389 هو المنفذ الافتراضي ل LDAP.**Base DN**—أدخل الموقع في التدرج الهرمي ل LDAP حيث يجب أن يبدأ الخادم في البحث بمجرد أن يستلم طلب تخويل.**النطاق**—أختر المدى الذي يجب أن يبحث فيه الخادم في التدرج الهرمي ل LDAP بمجرد أن يستلم طلب تفويض.**سمة (سمات) التسمية**- أدخل سمة (سمات) الأسماء المميزة ذات الصلة التي يتم من خلالها تعريف الإدخالات الموجودة على خادم LDAP بشكل فريد. سمات التسمية الشائعة هي الاسم الشائع (cn) ومعرف المستخدم (uid).**تسجيل الدخول DN**—تتطلب بعض خوادم LDAP، بما في ذلك خادم Microsoft Active Directory، أن يقوم الجهاز بإنشاء مصافحة عبر ربط مصدق قبل أن تقبل طلبات لأية عمليات LDAP أخرى. يحدد حقل DN الخاص بتسجيل الدخول خصائص مصادقة الجهاز، والتي يجب أن تتطابق مع خصائص مستخدم لديه امتيازات إدارية. على سبيل المثال، cn=administrator. للوصول المجهول، أترك هذا الحقل فارغا.**كلمة مرور تسجيل الدخول**- أدخل كلمة المرور ل DN تسجيل الدخول.**قم بتأكيد كلمة مرور تسجيل الدخول**— قم بتأكيد كلمة المرور ل DN الخاص بتسجيل الدخول.

9. انقر فوق **تطبيق** لإرسال التغييرات إلى الجهاز بعد إضافة جميع خوادم المصادقة والتخويل.إذا قمت بتكوينه للقيام بذلك، فإن PIX يقوم الآن بمعاينة الأوامر التي يتم إضافتها إلى التكوين الجاري تشغيله.
10. طقطقة **يرسل** in order to أرسلت الأمر إلى الأداة.

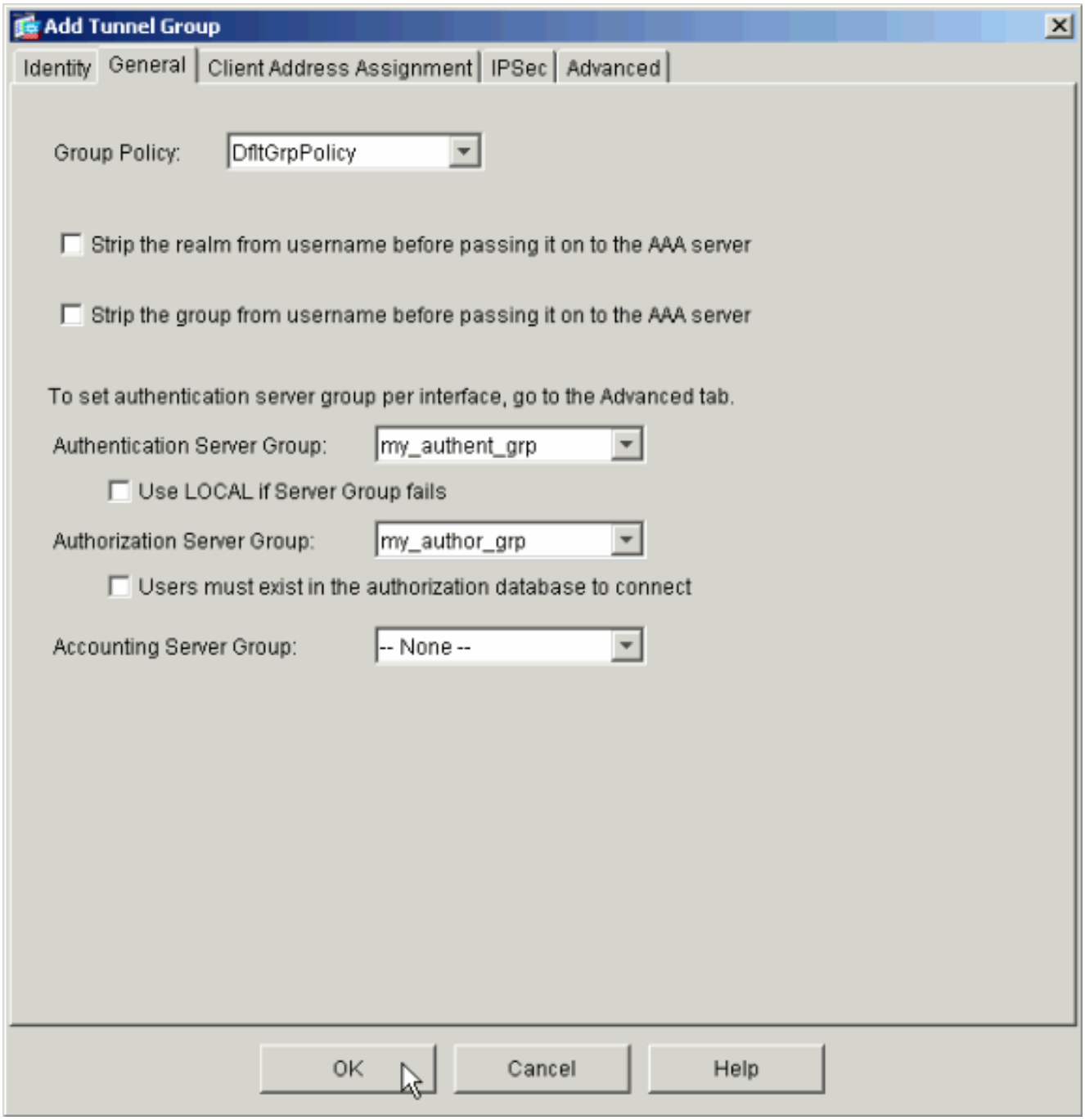
تكوين مجموعة نفق VPN للمصادقة والتفويض

أتمت هذا steps in order to أضفت النادل مجموعة أنت فقط شكلت إلى VPN نفق مجموعة.

1. أخترت **تشكيل** > **VPN** > **مجموعة نفق**، وطقطقة **يضيف** in order to خلقت جديد نفق مجموعة، أو **يحرر** in order to عدلت مجموعة موجود.



2. في علامة التبويب "عام" للنافذة التي تظهر، حدد مجموعات الخوادم التي تم تكوينها مسبقا.



3. *إختياري:* قم بتكوين المعلمات المتبقية في علامات التبويب الأخرى إذا قمت بإضافة مجموعة نفق جديدة.
4. انقر فوق موافق عند الانتهاء.
5. انقر فوق **تطبيق** لإرسال التغييرات إلى الجهاز بعد اكتمال تكوين مجموعة النفق.إذا قمت بتكوينه للقيام بذلك، فإن PIX يقوم الآن بمعاينة الأوامر التي يتم إضافتها إلى التكوين الجاري تشغيله.
6. طقطقة **يرسل** in order to أرسلت الأمر إلى الأداة.

تكوين المصادقة والتفويض لمستخدمي VPN باستخدام CLI

هذا هو تكوين CLI المكافئ لمجموعات خوادم المصادقة والتفويض الخاصة بمستخدمي VPN.

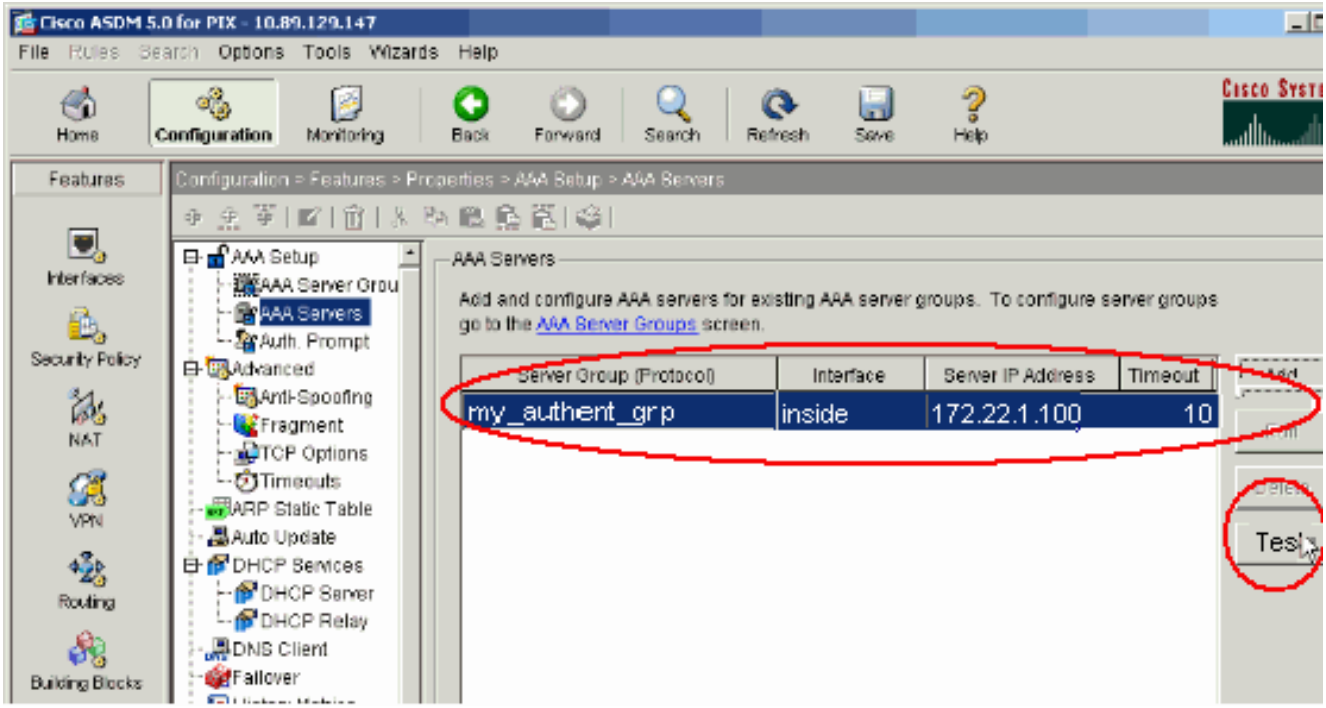
تكوين واجهة سطر الأوامر (CLI) عبر جهاز الأمان
pixfirewall#**show run** Saved : : (PIX Version 7.2(2

```
!
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 ---!
```

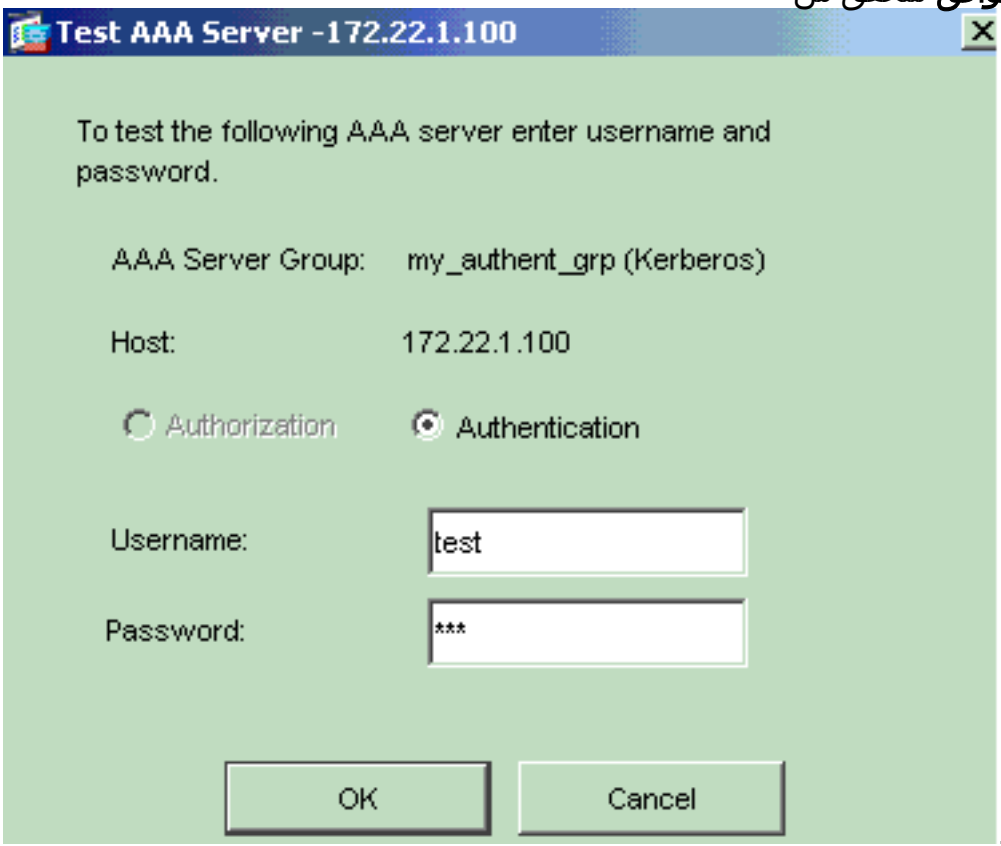
التحقق من الصحة

أكمل هذه الخطوات للتحقق من مصادقة المستخدم بين خادم PIX/ASA و AAA:

1. أختر **تكوين > خصائص > إعداد AAA > خوادم AAA**، وحدد مجموعة الخوادم (my_authent_grp). ثم انقر على **إختبار** للتحقق من مسوغات المستخدم.

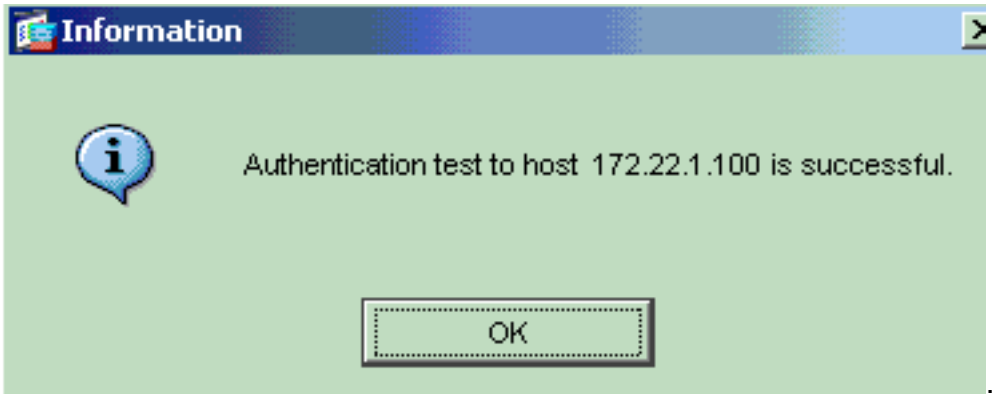


2. قم بتوفير اسم المستخدم وكلمة المرور (على سبيل المثال، اسم المستخدم: الاختبار وكلمة المرور: الاختبار)، وانقر **موافق** للتحقق من



الصحة.

3. يمكنك أن ترى أن المصادقة



ناجحة.

استكشاف الأخطاء وإصلاحها

1. أحد الأسباب المتكررة لفشل المصادقة هو انحراف الساعة. تأكد من مزامنة الساعات الموجودة على PIX أو ASA وخادم المصادقة الخاص بك.عندما تفشل المصادقة بسبب انحراف الساعة، يمكنك تلقي رسالة الخطأ هذه: `- : : 300 .. تظهر أيضا رسالة السجل هذه:PIX|ASA-3-113020 :Kerberos :ip_address` `300 ip_address`— عنوان IP الخاص بخادم Kerberos.يتم عرض هذه الرسالة عند فشل مصادقة مستخدم IPSec أو WebVPN من خلال خادم Kerberos لأن الساعات الموجودة على جهاز الأمان والخادم تبعد أكثر من خمس دقائق (300 ثانية). وعند حدوث ذلك، يتم رفض محاولة الاتصال.لحل هذه المشكلة، قم بمزامنة الساعات على جهاز الأمان وخادم Kerberos.
2. يجب تعطيل المصادقة المسبقة في Active Directory (AD)، أو قد يؤدي ذلك إلى فشل مصادقة المستخدم.
3. يتعذر على مستخدمي عميل شبكة VPN المصادقة مقابل خادم شهادات Microsoft. تظهر رسالة الخطأ هذه:" `(14 )` " لحل هذه المشكلة، قم بإلغاء تحديد خانة الاختيار **لا تتطلب** مصادقة **مسبقة ل kerberose** على خادم المصادقة.

معلومات ذات صلة

- تكوين خوادم AAA وقاعدة البيانات المحلية
- دعم منتجات أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).