PIX/ASA:通過ASDM/CLI配置VPN客戶端使用者的Kerberos身份驗證和LDAP授權伺服器組示例

目錄

簡介

本文檔介紹如何使用Cisco Adaptive Security Device Manager(ASDM)在Cisco PIX 500系列安全裝置上配置Kerberos身份驗證和LDAP授權伺服器組。在本示例中，VPN隧道組的策略使用伺服器組對傳入使用者進行身份驗證和授權。

必要條件

需求

本文檔假定PIX完全可以運行並且配置為允許ASDM更改配置。

注意：請參閱允許ASDM的HTTPS訪問，以便允許ASDM配置PIX。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco PIX安全裝置軟體版本7.x及更高版本
- Cisco ASDM版本5.x及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以與思科自適應安全裝置(ASA)版本7.x配合使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

處理VPN使用者時，並不支援PIX/ASA 7.x軟體中的所有可能的身份驗證和授權方法。下表詳細說明了哪些方法可用於VPN使用者：

	本地	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
驗證	是	是	是	是	是	是	否
Authorization	是	是	否	否	否	否	是

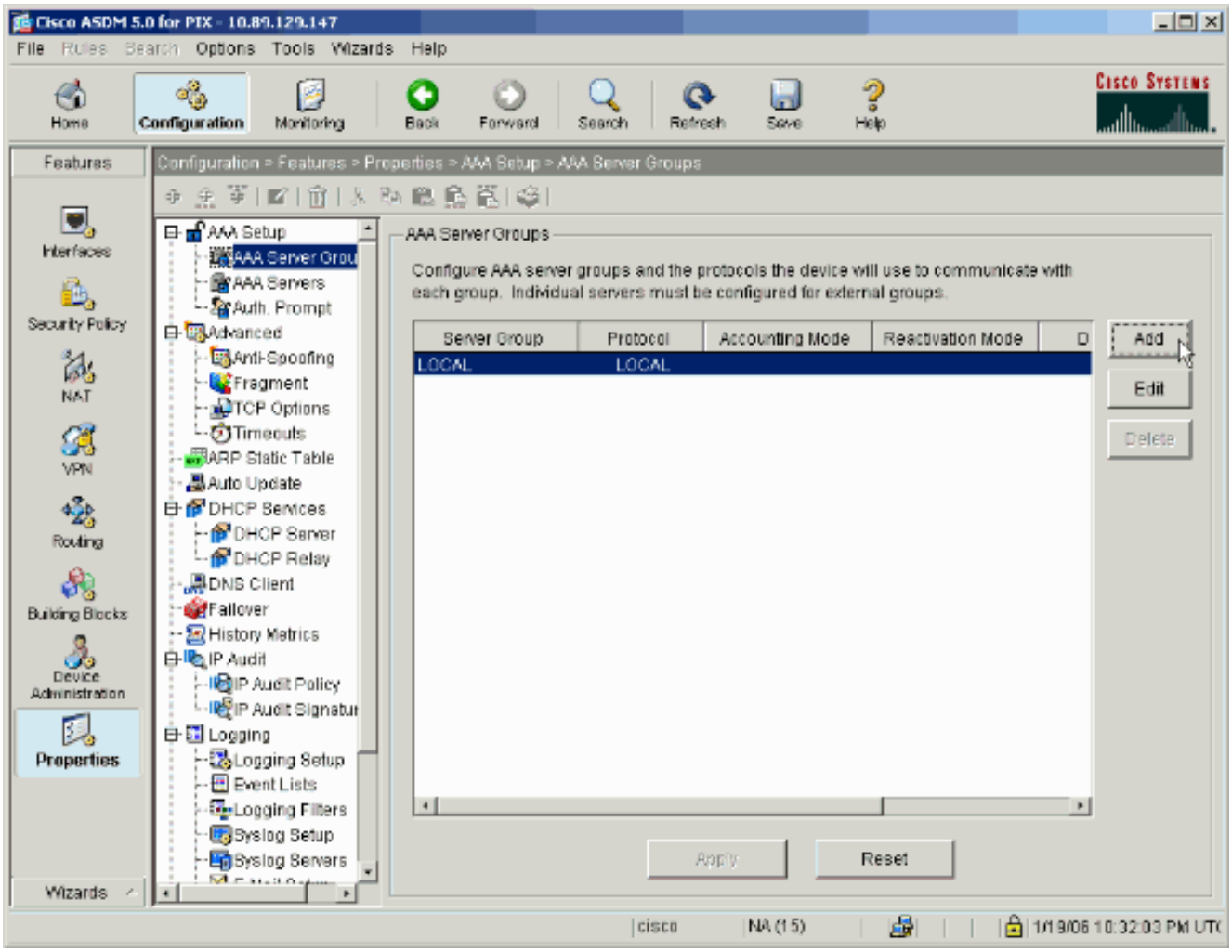
注意：在本示例中，Kerberos用於身份驗證，LDAP用於VPN使用者的授權。

使用ASDM為VPN使用者配置身份驗證和授權

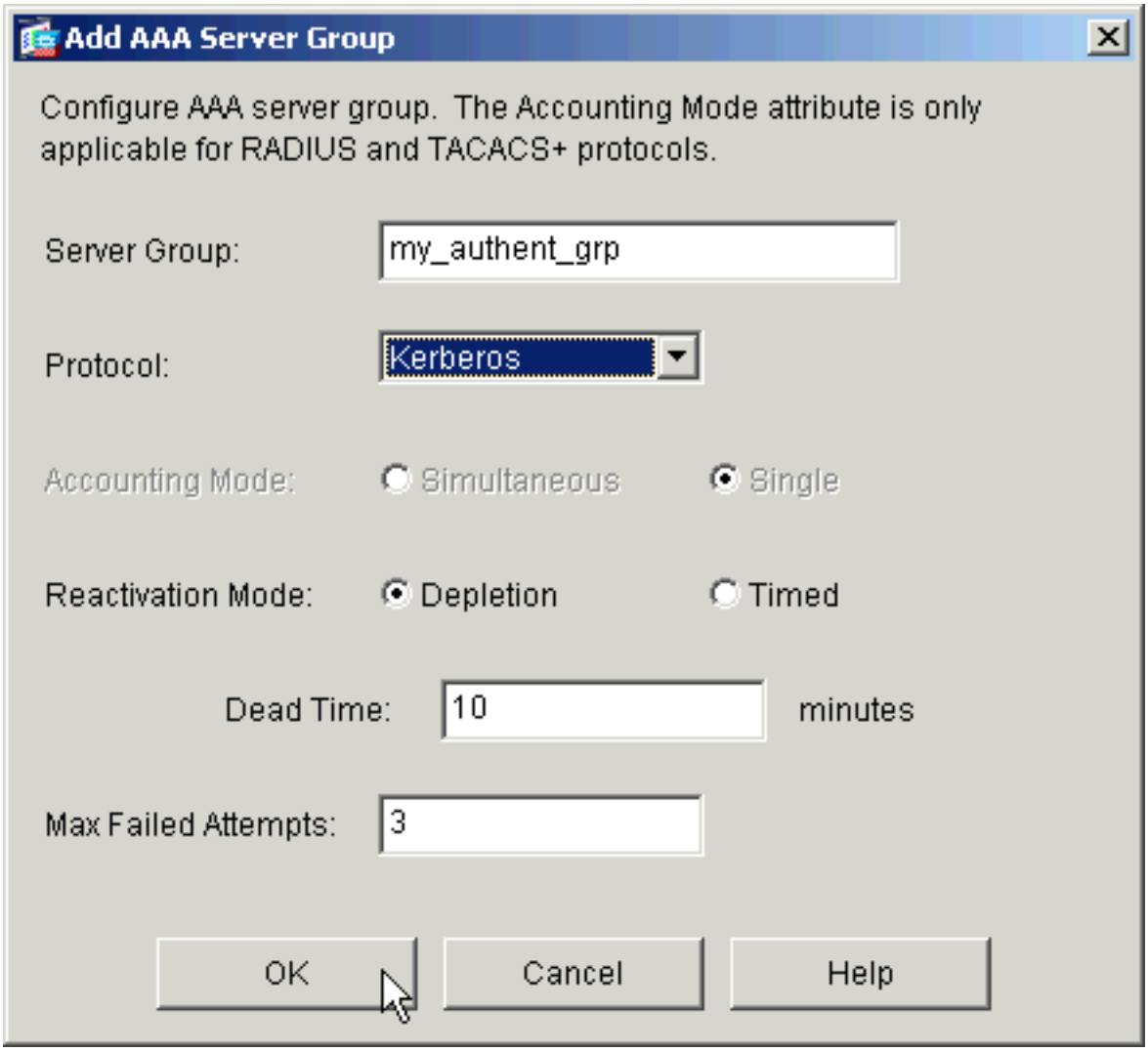
配置身份驗證和授權伺服器

完成以下步驟，以便通過ASDM為VPN使用者配置身份驗證和授權伺服器組。

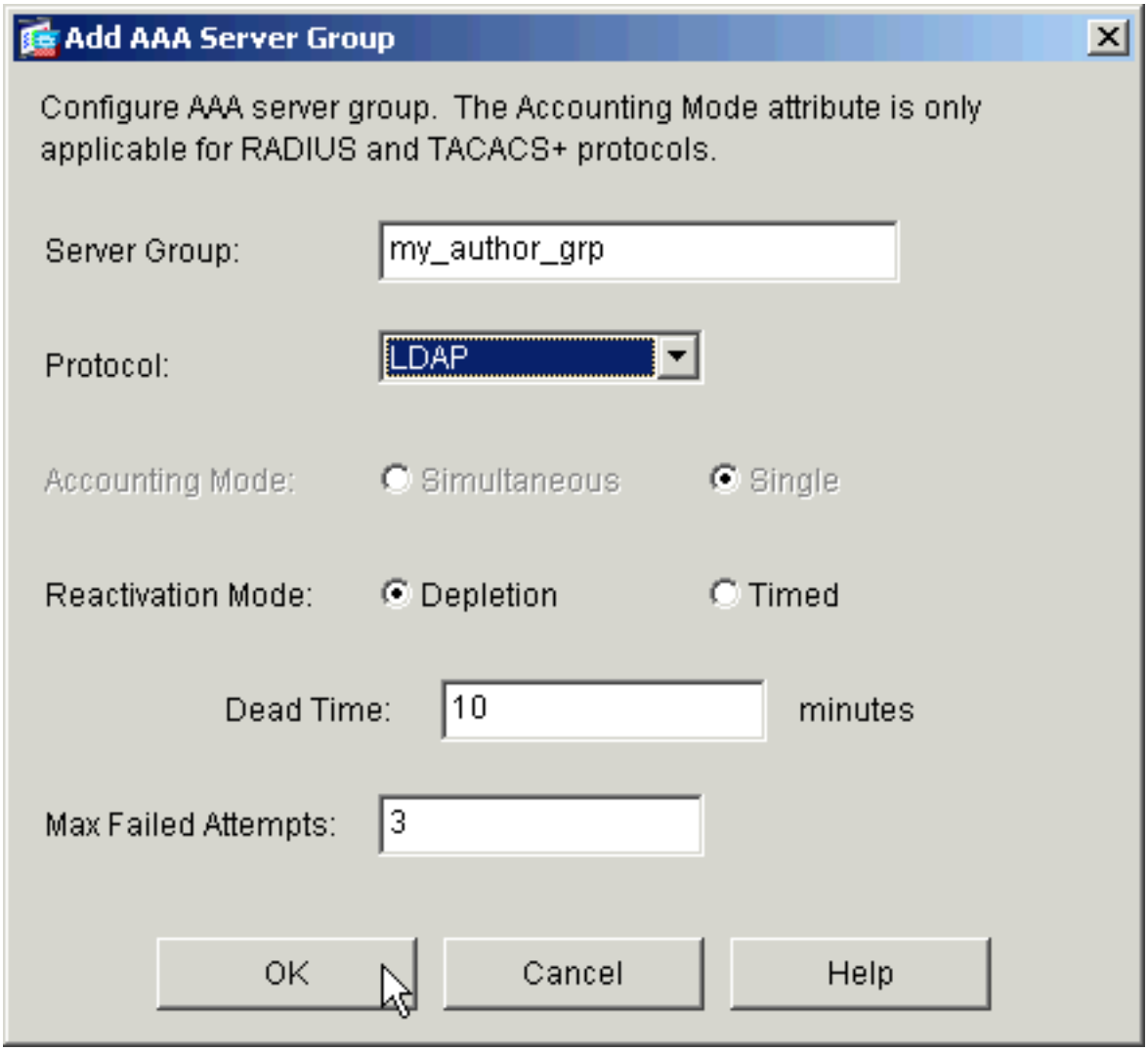
1. 選擇**Configuration > Properties > AAA Setup > AAA Server Groups**，然後按一下**Add**。



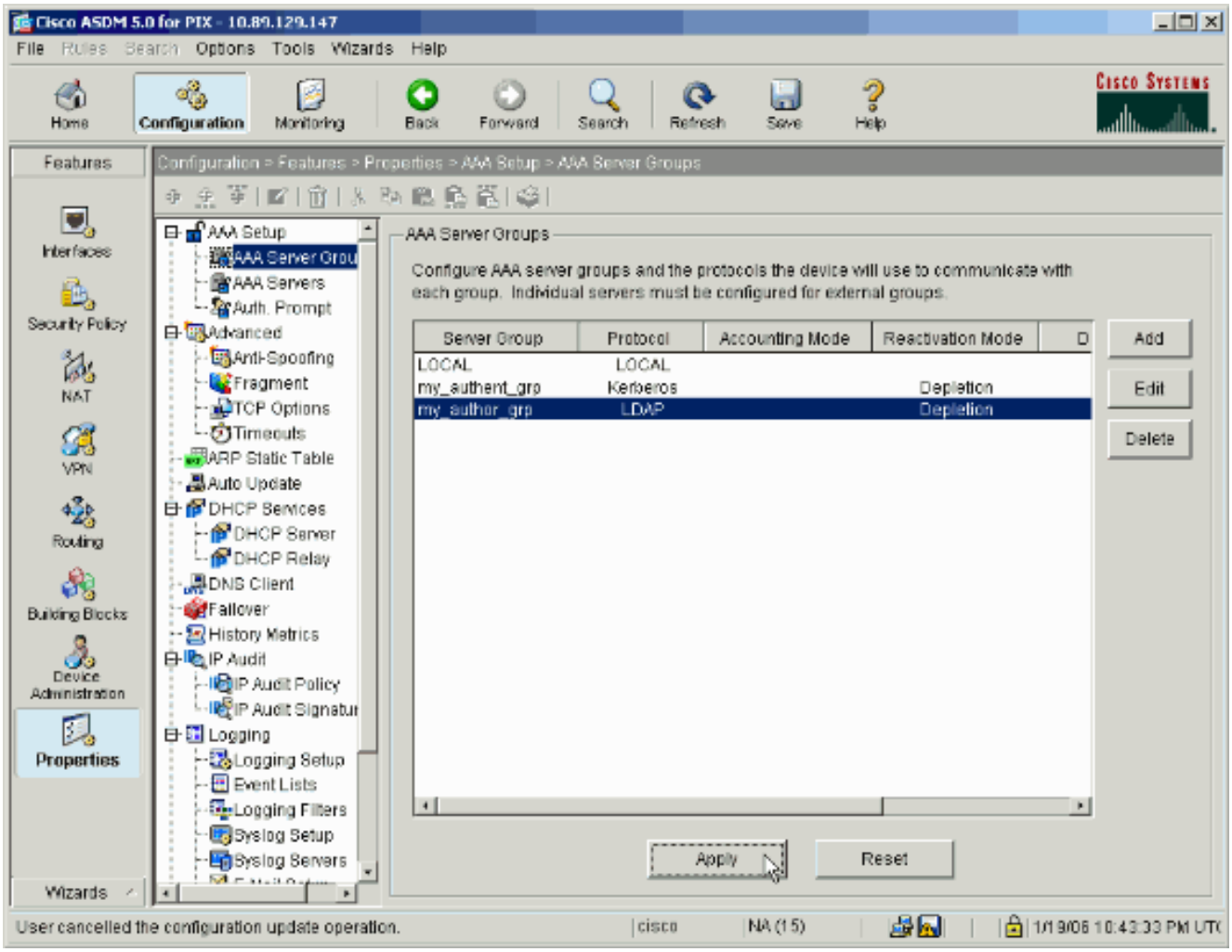
2. 定義新身份驗證伺服器組的名稱，並選擇協定。Accounting Mode選項僅適用於RADIUS和TACACS+。完成後按一下**OK**。



3. 重複步驟1和2以建立新的授權伺服器組。

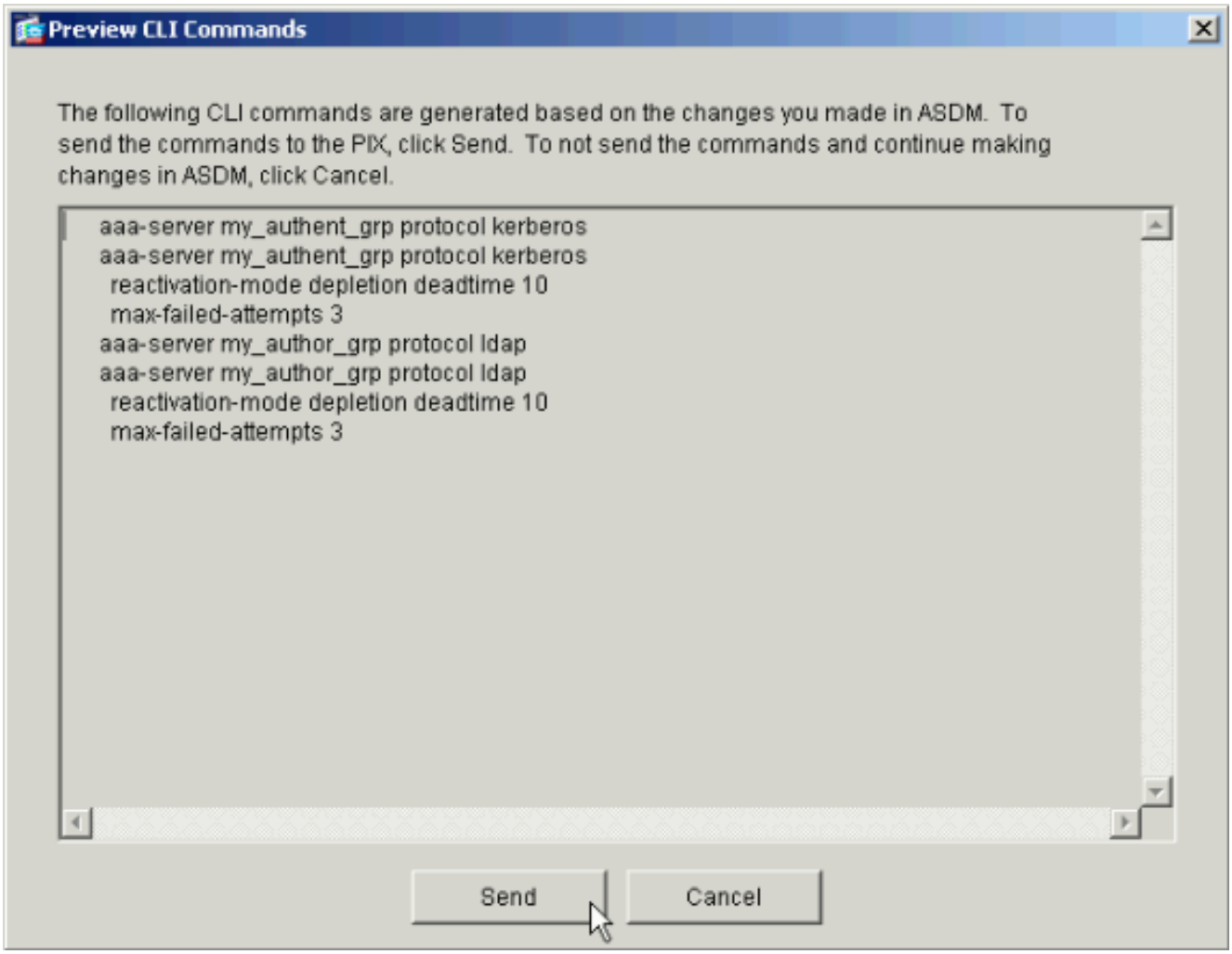


4. 按一下「**Apply**」將變更傳送到裝置。



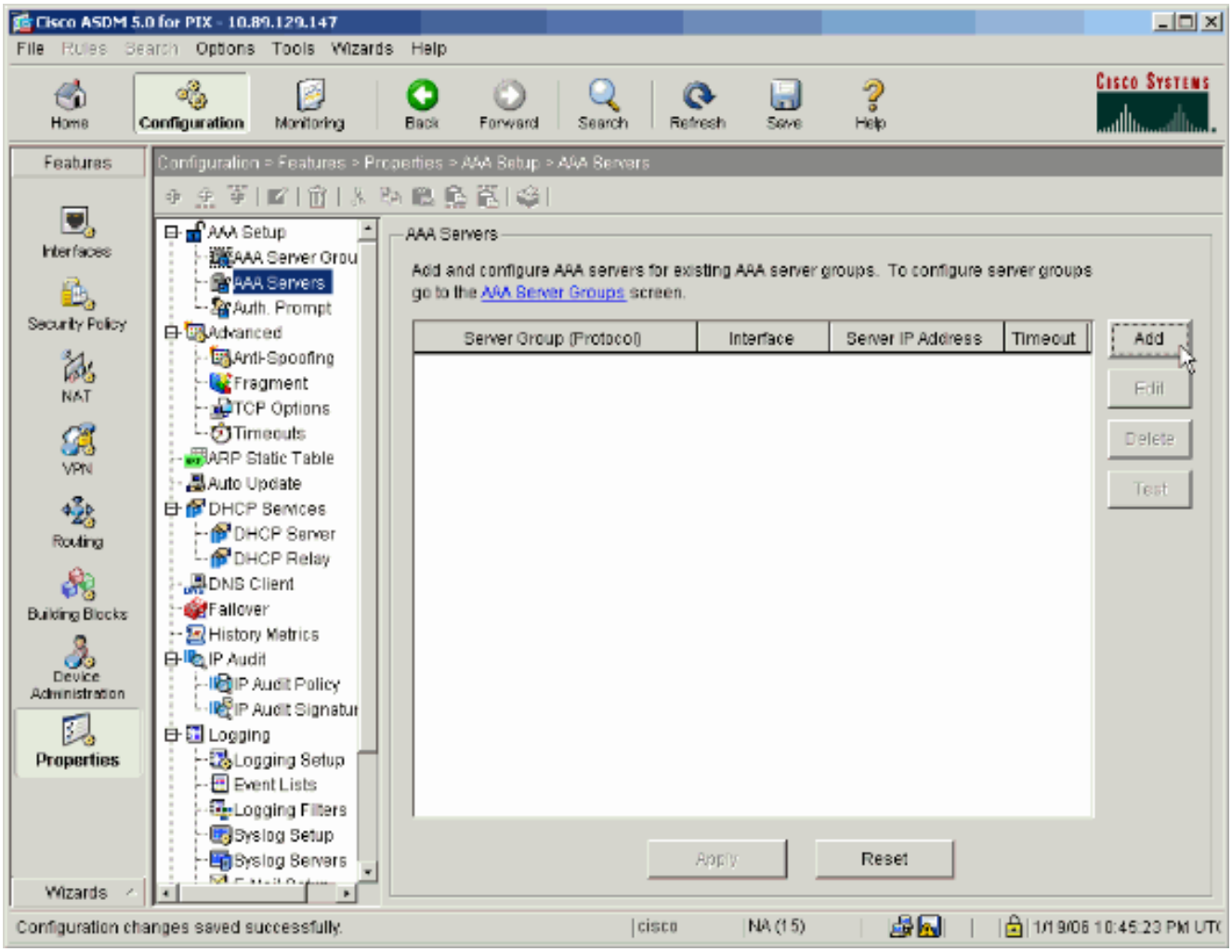
如果裝置已配置為這樣做，裝置現在會預覽新增到運行配置中的命令。

5. 按一下「**Send**」將命令傳送到裝置。

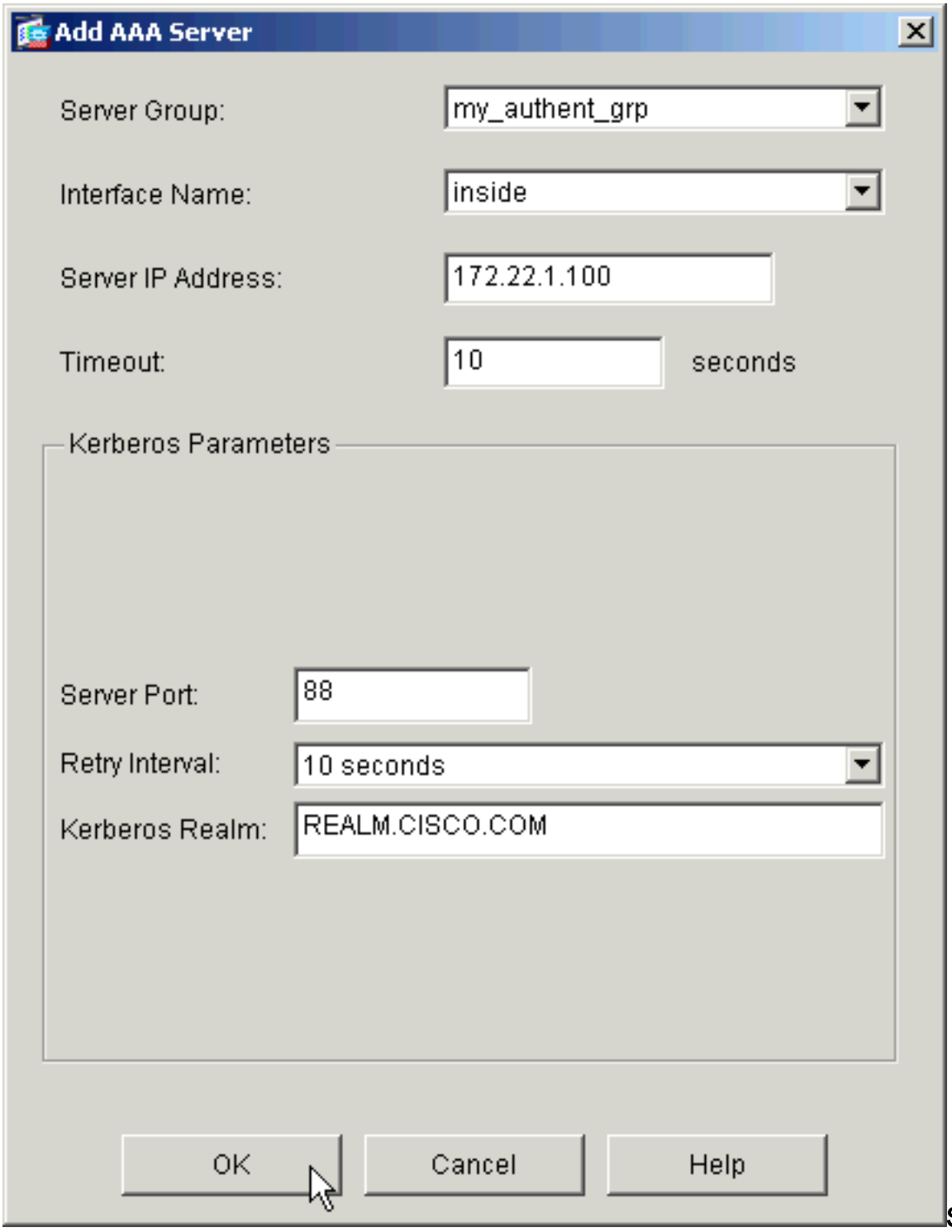


現在必須使用身份驗證和授權伺服器填充新建立的伺服器組。

6. 選擇**Configuration > Properties > AAA Setup > AAA Servers**，然後按一下**Add**。

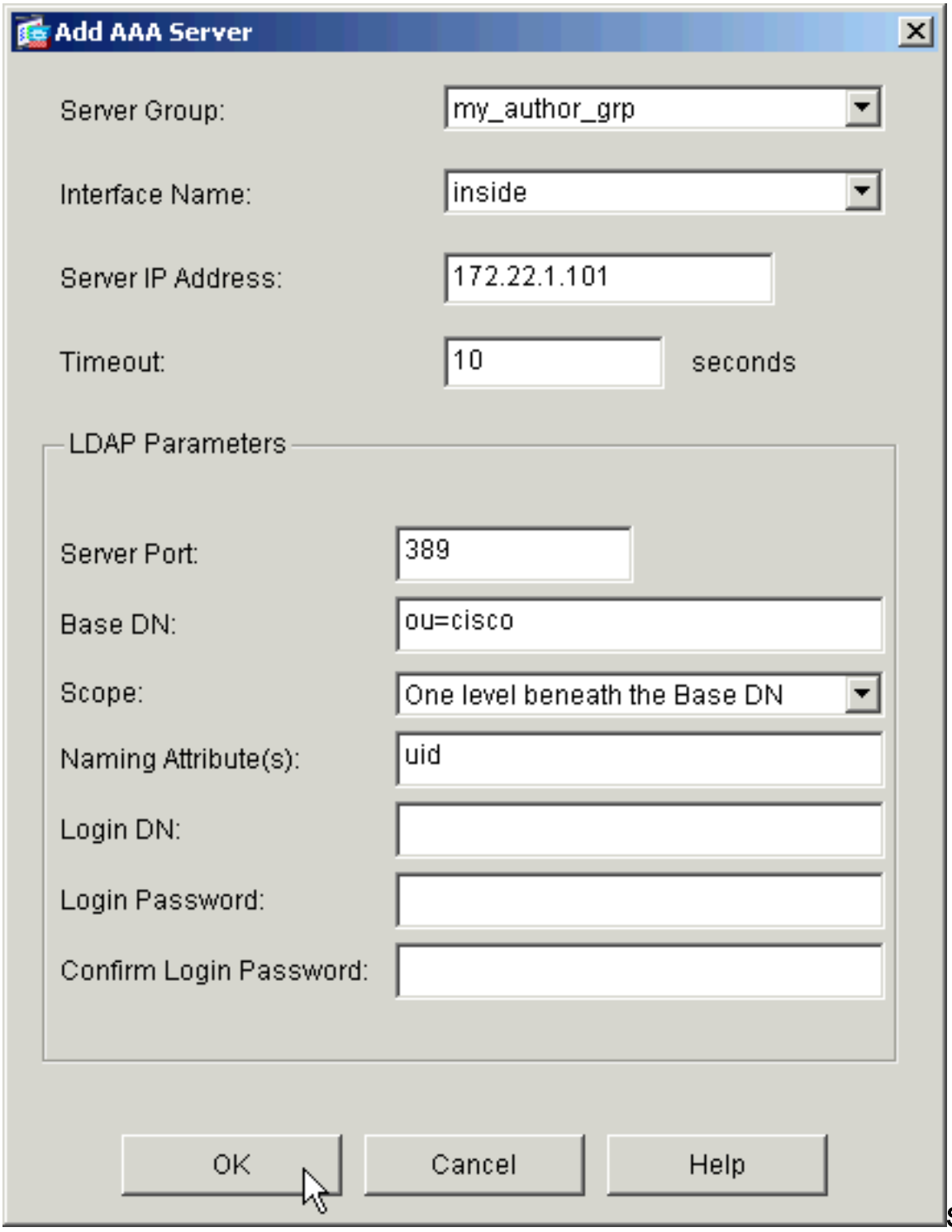


7. 配置身份驗證伺服器。完成後按一下**OK**。



Server Group — 選擇步驟2中配置的身份驗證伺服器組。**Interface Name** — 選擇伺服器所在的介面。**Server IP Address** — 指定身份驗證伺服器的IP地址。**Timeout** — 指定等待伺服器響應的最長時間（以秒為單位）。**Kerberos引數：伺服器端口** — 88是Kerberos的標準埠。**重試間隔** (Retry Interval) — 選擇所需的重試間隔。**Kerberos Realm** — 輸入Kerberos領域的名稱。這通常是所有大寫字母的Windows域名。

8. 配置授權伺服器。完成後按一下**OK**。



Server Group — 選擇步驟3中配置的授權伺服器組。**Interface Name** — 選擇伺服器所在的介面。**Server IP Address** — 指定授權伺服器的IP地址。**Timeout** — 指定等待伺服器響應的最長時間（以秒為單位）。**LDAP引數：伺服器端**口 — 389是LDAP的預設埠。**基本DN** — 在LDAP層次結構中輸入伺服器在收到授權請求後應開始搜尋的位置。**Scope** — 選擇伺服器在收到授權請求後搜尋LDAP層次結構的範圍。**Naming Attribute(s)**-輸入Relative Distinguished Name(s)屬性，LDAP伺服器上的條目可依據該屬性進行唯一定義。常用命名屬性包括公用名(cn)和使用者ID(uid)。**登入DN** — 某些LDAP伺服器（包括Microsoft Active Directory伺服器）要求裝置通過身份驗證繫結建立握手，然後才接受任何其他LDAP操作的請求。Login DN欄位定義裝置的身份驗證特性，這些特性應與具有管理許可權的使用者所對應的身份驗證特性。例如，cn=administrator。對於匿名訪問，請將此欄位留空。**Login Password** — 輸入登入DN的密碼。**Confirm Login Password** — 確認登入DN的密碼。

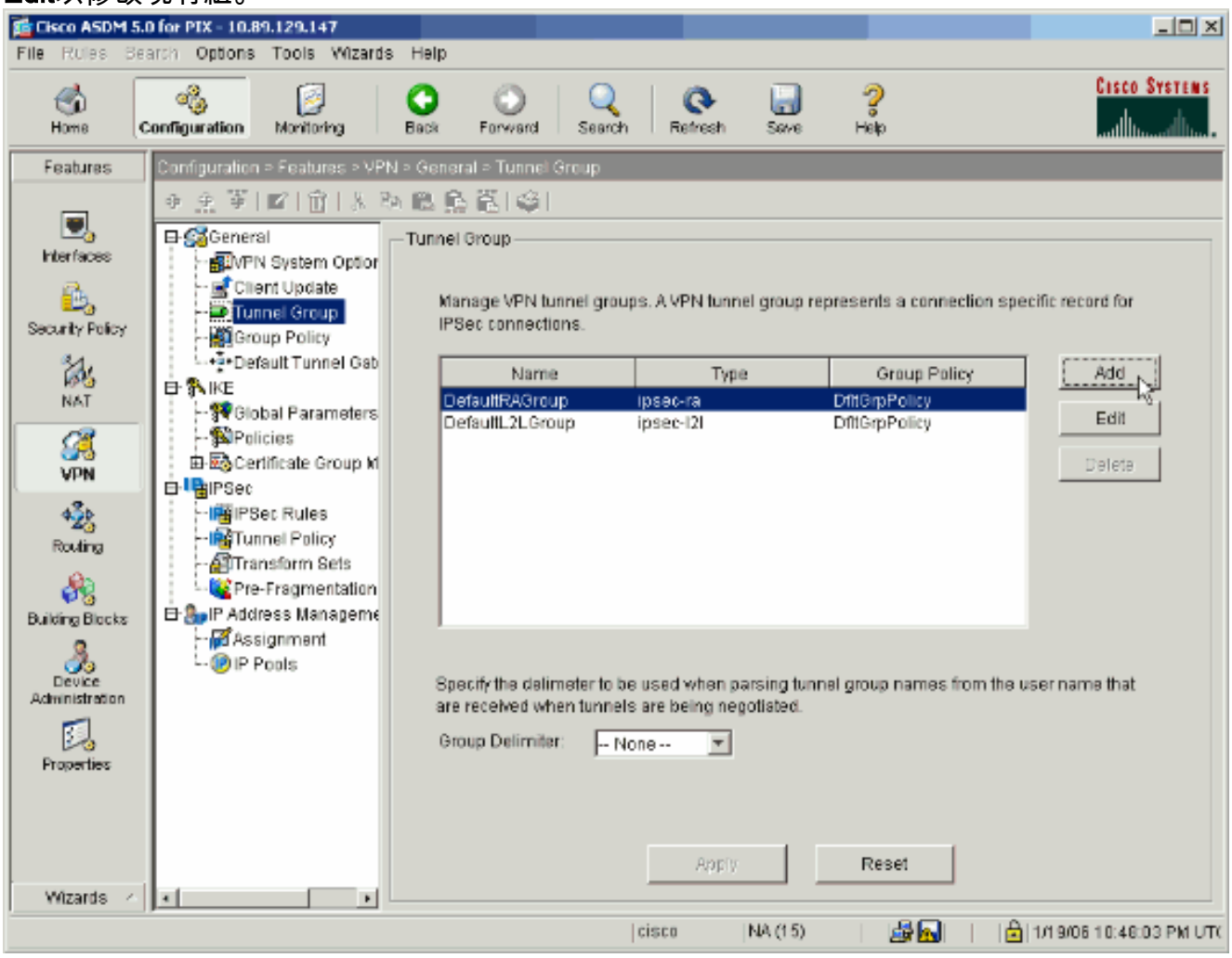
9. 按一下**Apply**可在新增所有身份驗證和授權伺服器之後將更改傳送到裝置。如果已經進行了配置，PIX現在將預覽新增到運行配置中的命令。

10. 按一下「**Send**」將命令傳送到裝置。

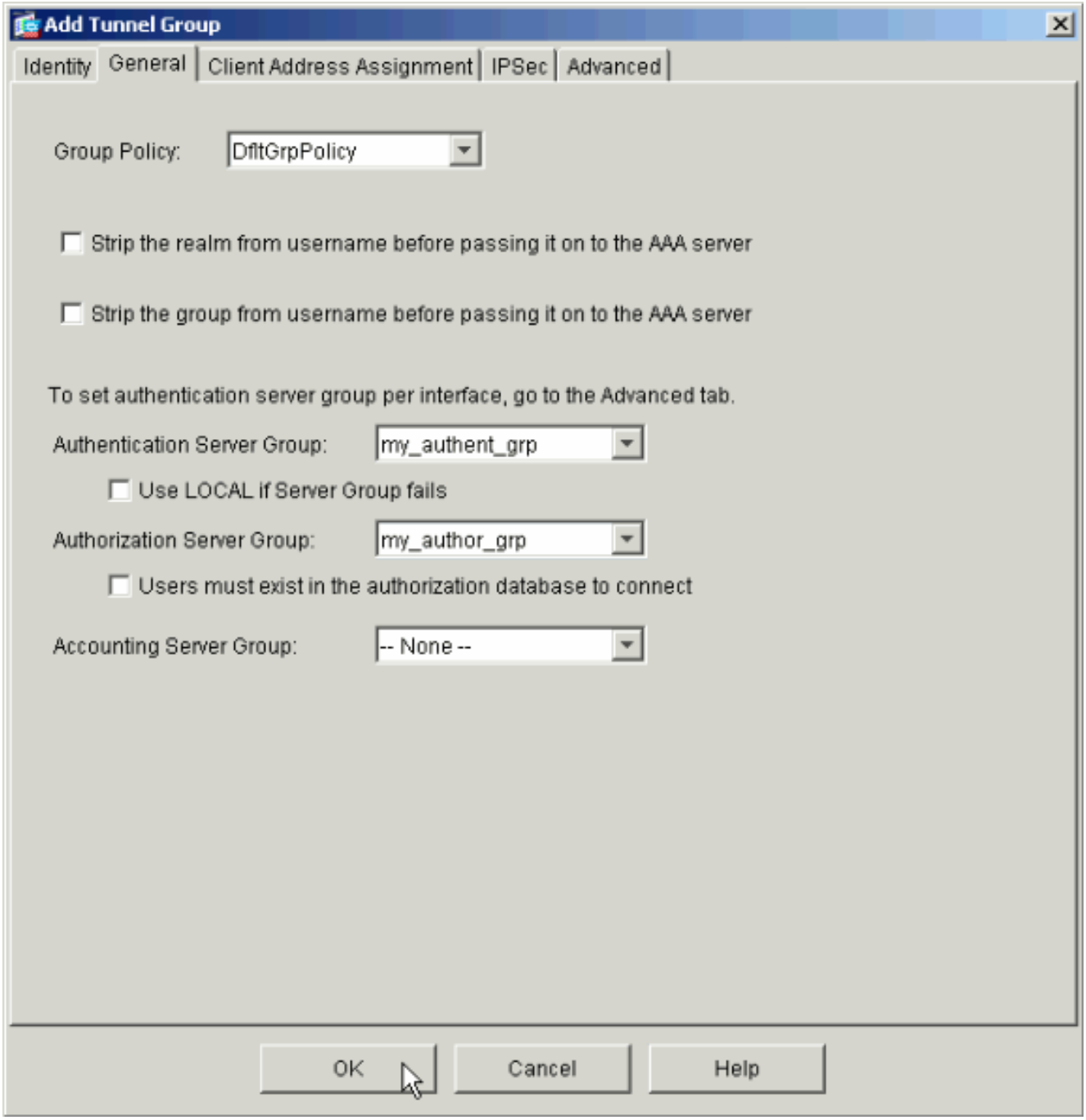
配置VPN隧道組以進行身份驗證和授權

完成這些步驟，將剛才配置的伺服器組新增到VPN隧道組。

1. 選擇**Configuration > VPN > Tunnel Group**，然後按一下**Add**以建立新的隧道組，或按一下**Edit**以修改現有組。



2. 在出現的視窗的General頁籤上，選擇之前配置的伺服器組。



3. *可選：* 如果新增新隧道組，請在其它頁籤上配置其餘引數。
4. 完成後按一下**OK**。
5. 按一下「**Apply**」，以在完成通道組設定後將變更傳送到裝置。如果已經進行了配置，PIX現在將預覽新增到運行配置中的命令。
6. 按一下「**Send**」將命令傳送到裝置。

使用CLI為VPN使用者配置身份驗證和授權

這是適用於VPN使用者的身份驗證和授權伺服器組的等效CLI配置。

安全裝置CLI配置

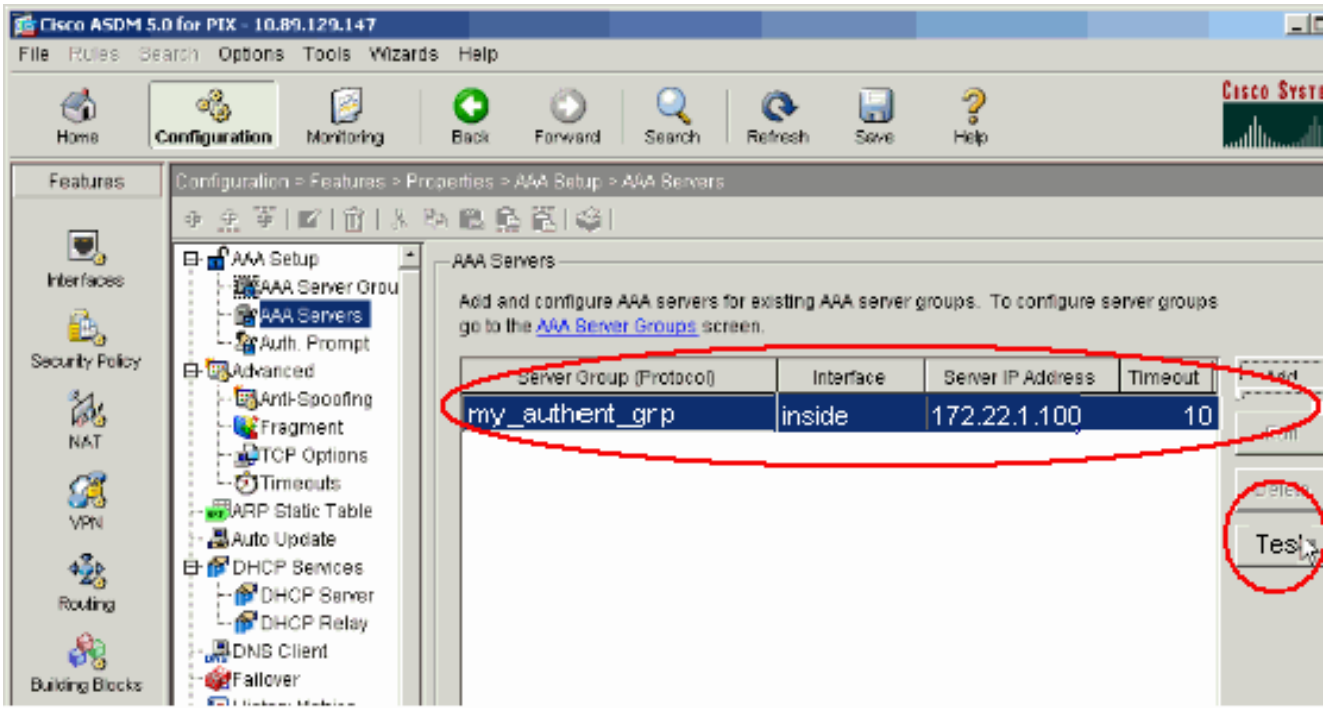
`pixfirewall#show run`
`: Saved`
`:`
`PIX Version 7.2(2)`

```
!
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.
```

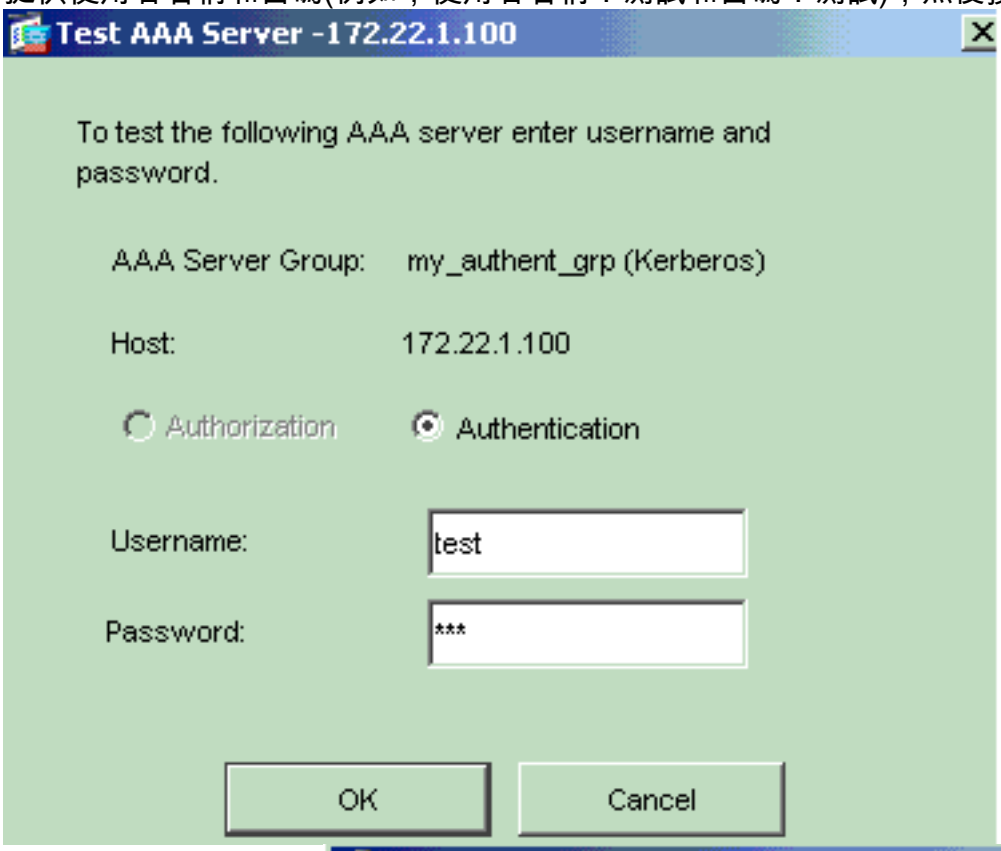
驗證

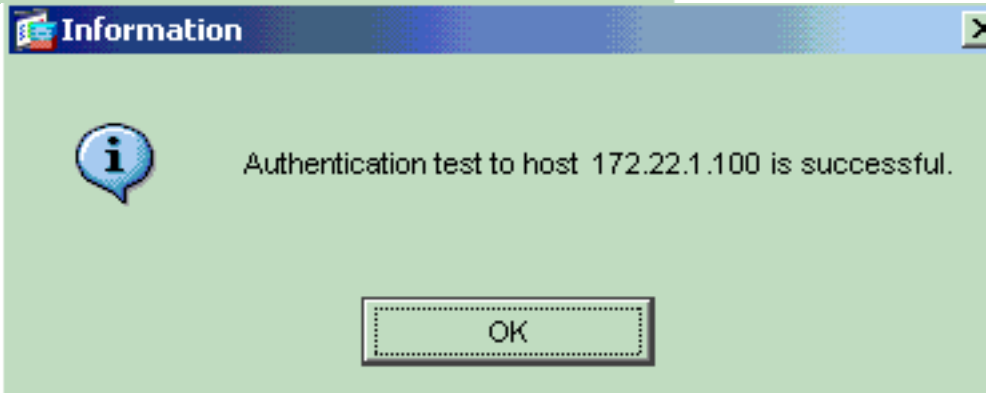
完成以下步驟，驗證PIX/ASA和AAA伺服器之間的使用者身份驗證：

1. 選擇**Configuration > Properties > AAA Setup > AAA Servers**，然後選擇伺服器組(my_authent_grp)。 然後按一下**測試**以驗證使用者憑據。



2. 提供使用者名稱和密碼(例如，使用者名稱：測試和密碼：測試)，然後按一下OK以進行驗證。





3. 您可以看到驗證成功。

疑難排解

1. 身份驗證失敗的一個常見原因是時鐘偏差。確保PIX或ASA上的時鐘與您的身份驗證伺服器同步。當身份驗證因時鐘偏差而失敗時，您會收到以下錯誤消息：`: – 300`.此外，還會顯示以下日誌消息：`%PIX|ASA-3-113020:Kerberosip_address300 ip_address` - Kerberos伺服器的IP地址。當通過Kerberos伺服器對IPSec或WebVPN使用者進行身份驗證失敗時，會顯示此消息，因為安全裝置和伺服器上的時鐘間隔超過五分鐘（300秒）。發生這種情況時，連線嘗試被拒絕。為了解決此問題，請同步安全裝置和Kerberos伺服器上的時鐘。
2. 必須禁用Active Directory(AD)上的預身份驗證，否則可能會導致使用者身份驗證失敗。
3. VPN客戶端使用者無法對Microsoft證書伺服器進行身份驗證。出現以下錯誤消息：`""14` 要解決此問題，請取消選中身份驗證伺服器上的**Do not require kerberose preauthentication**覈取方塊。

相關資訊

- 配置AAA伺服器和本地資料庫
- Cisco ASA 5500系列自適應安全裝置產品支援
- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems