Table of Contents

Authentication and Authorization Server Groups for VPN Users via ASDM Configuration Example

Document ID: 68881

Introduction

This document describes how to use the Cisco Adaptive Security Device Manager (ASDM) to configure authentication and authorization server groups on the Cisco PIX 500 Series Security Appliance. In this example, the server groups created are used by the policy of a VPN tunnel group to authenticate and authorize incoming users.

Prerequisites

Requirements

This document assumes that the PIX is fully operational and configured to allow the ASDM to make configuration changes.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco PIX Security Appliance Software Version 7.0(4)
- Cisco ASDM Version 5.0(4)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with Cisco Adaptive Security Appliance (ASA) Version 7.x.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Not all of the possible authentication and authorization methods available in PIX/ASA 7.x software are supported when you deal with VPN users. This table details what methods are available for VPN users:

	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	No
Authorization	Yes	Yes	No	No	No	No	Yes

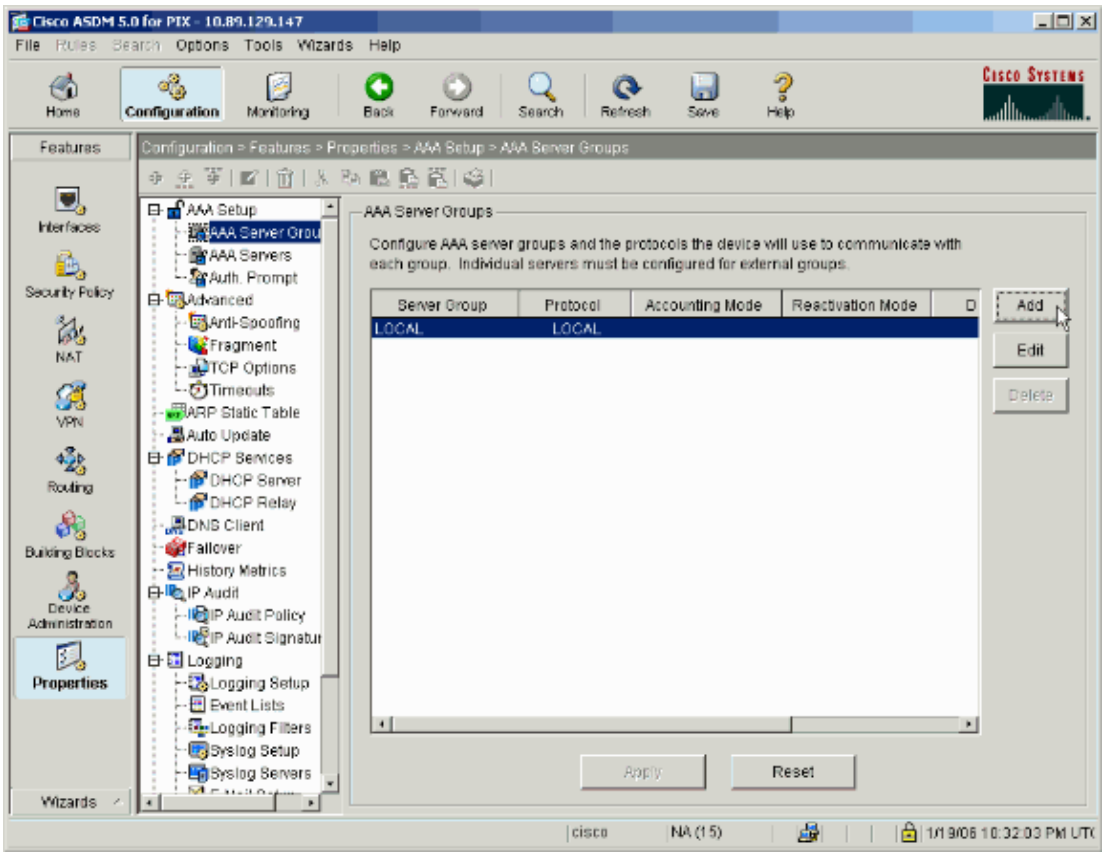
Note: Kerberos is used for the authentication and LDAP is used for the authorization of VPN users in this example.

Configure Authentication and Authorization for VPN Users

Configure Authentication and Authorization Servers

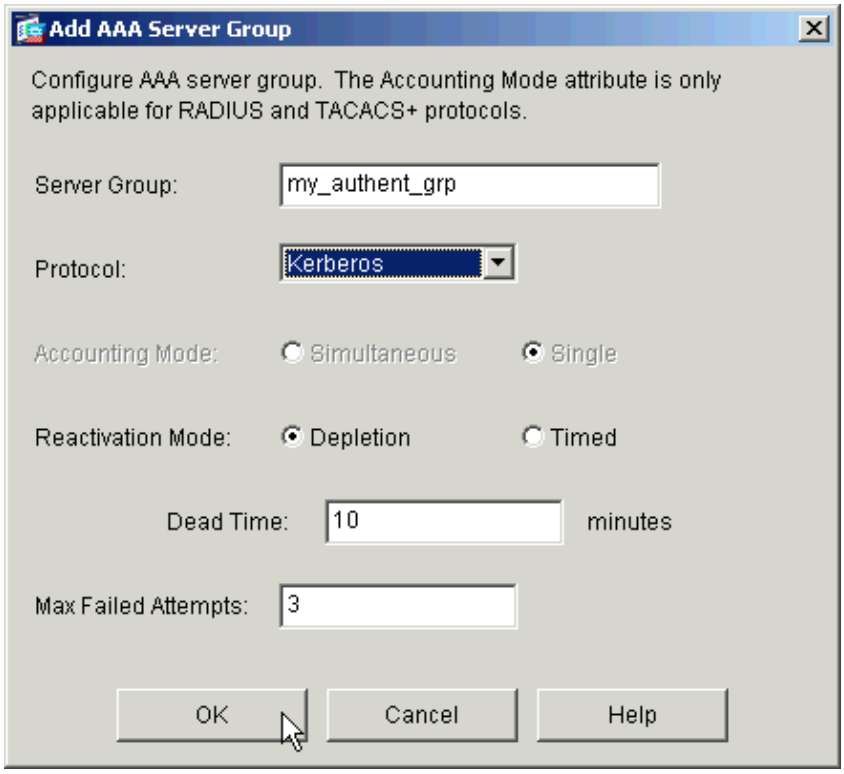
Complete these steps to configure authentication and authorization server groups for VPN users via ASDM.

1. Select **Configuration > Properties > AAA Setup > AAA Server Groups** and click **Add**.

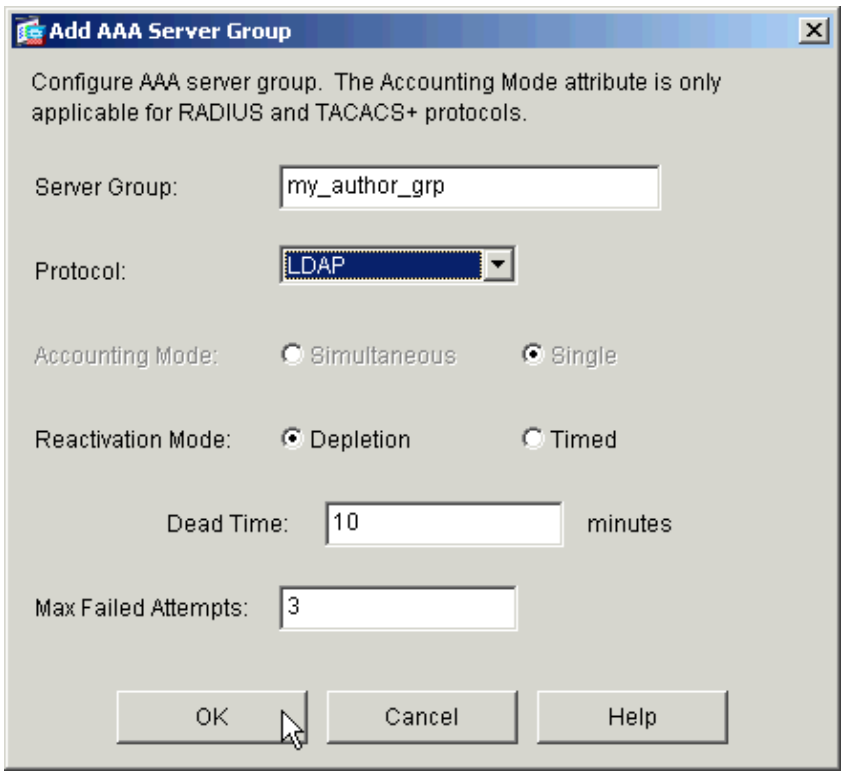


2. Define a name for the new authentication server group and choose a protocol.

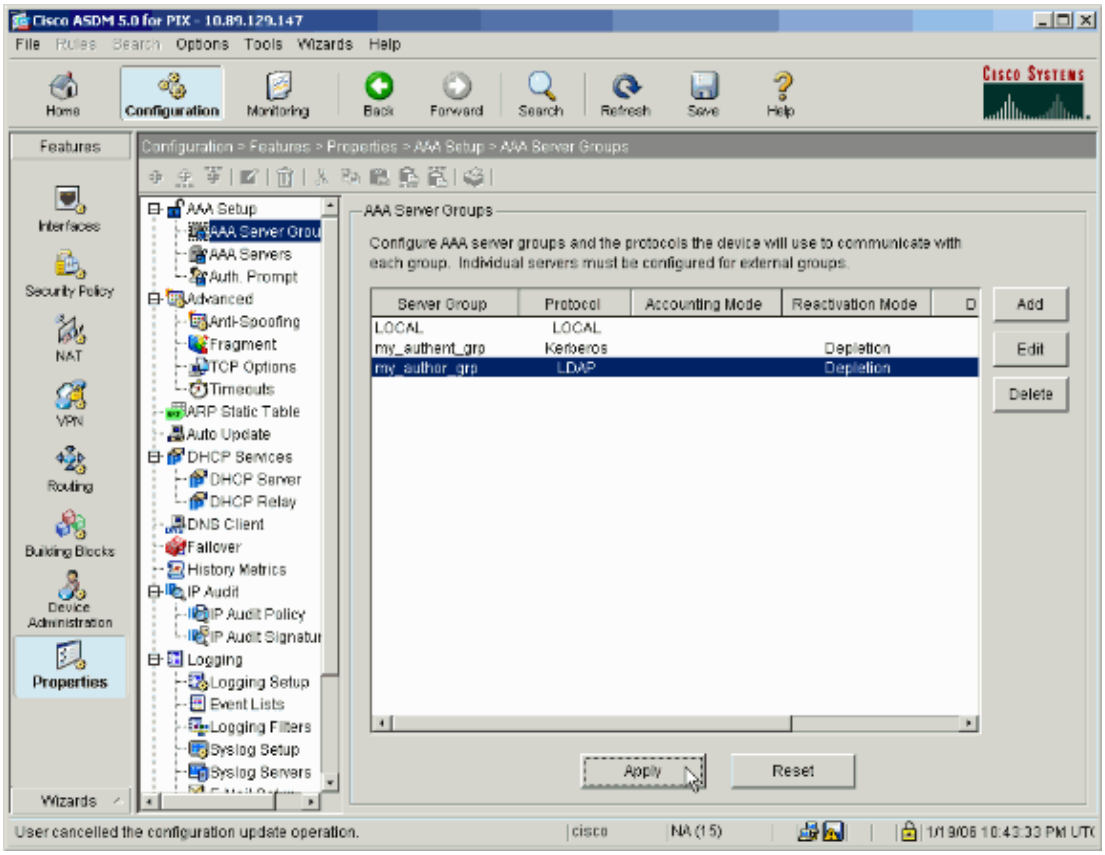
The Accounting Mode option is for RADIUS and TACACS+ only. Click **OK** when finished.



3. Repeat steps 1 and 2 to create a new authorization server group.

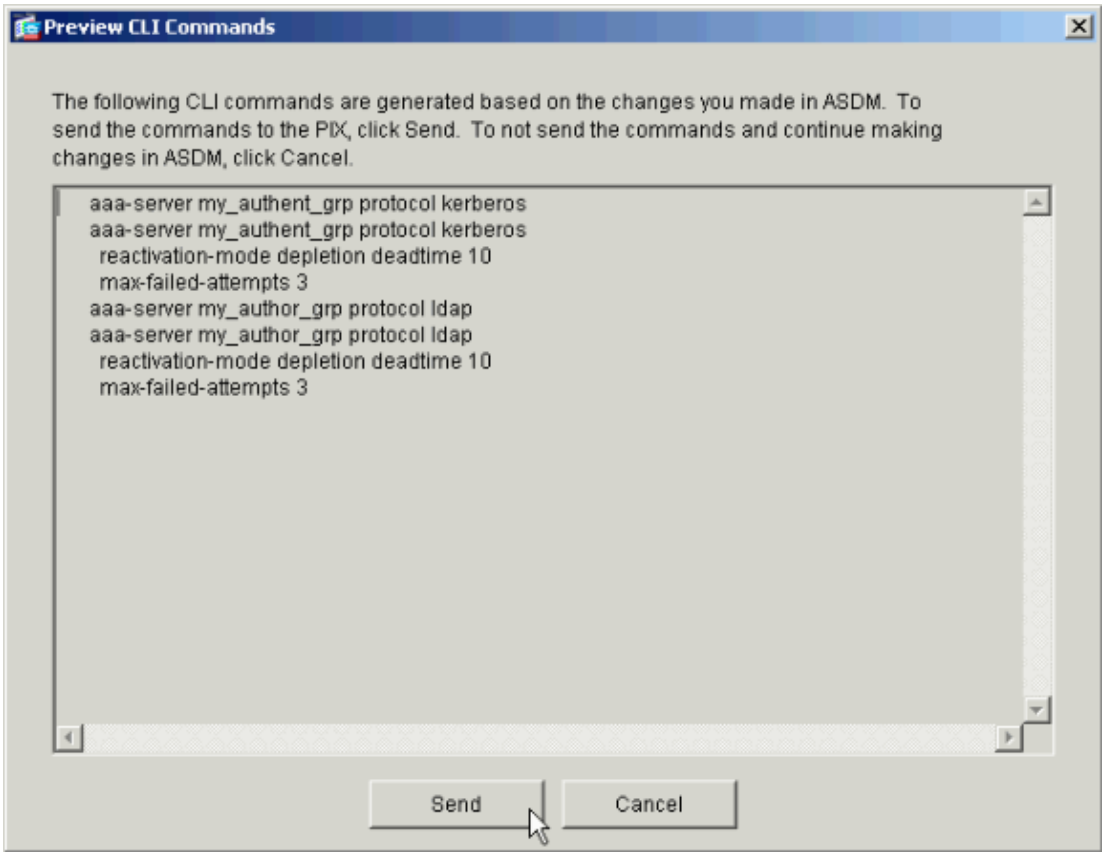


4. Click **Apply** to send the changes to the device.



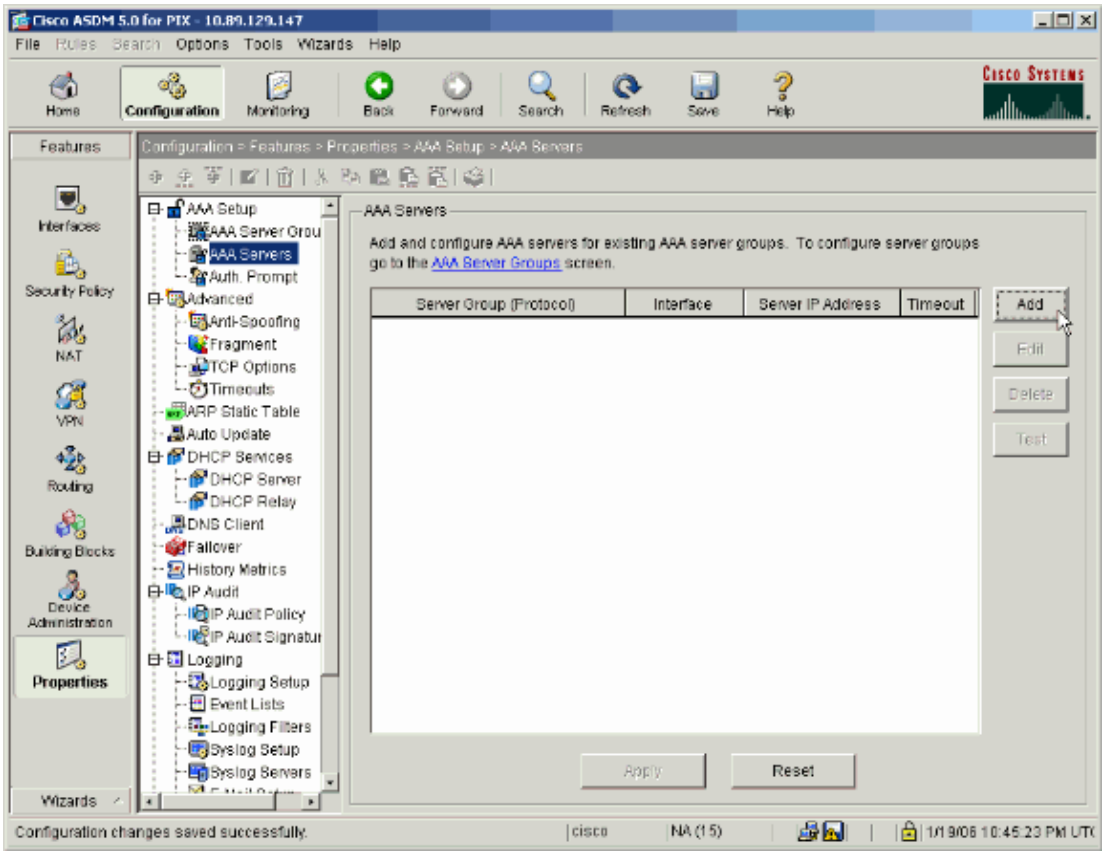
If you have it configured to do so, the device now previews the commands that are added to the running configuration.

5. Click **Send** to send the commands to the device.

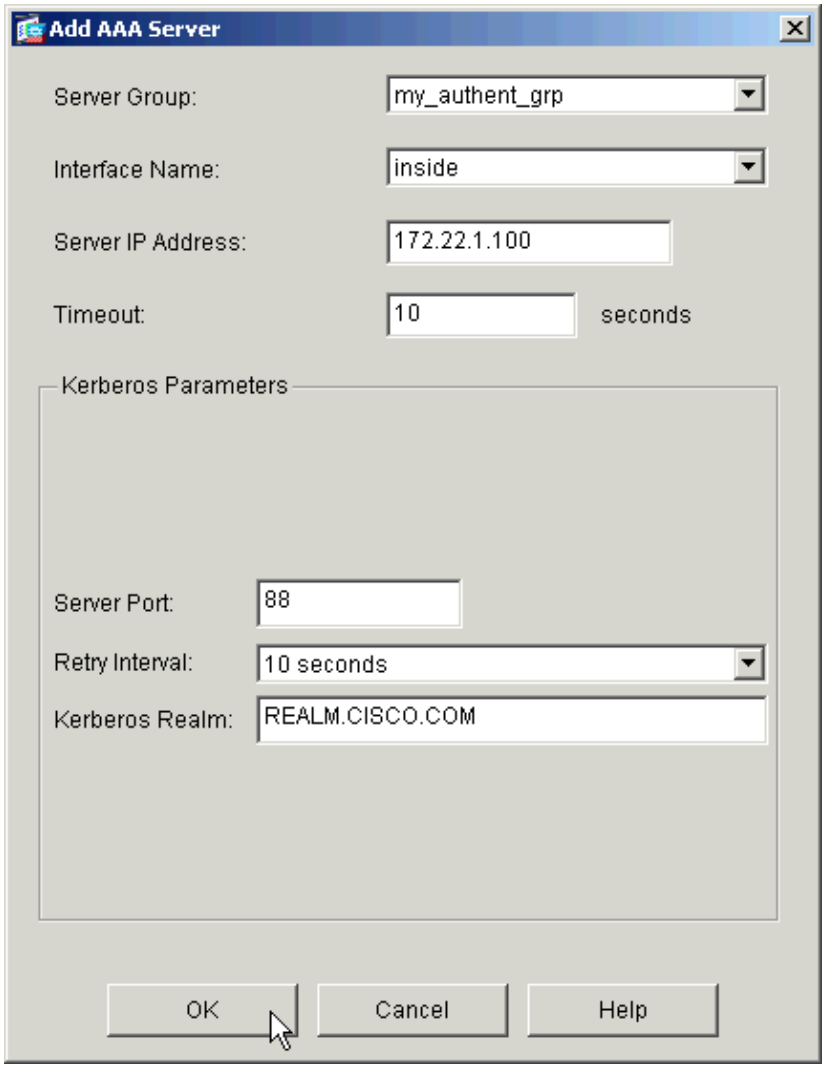


The newly created server groups must now be populated with authentication and authorization servers.

6. Select **Configuration > Properties > AAA Setup > AAA Servers** and click **Add**.

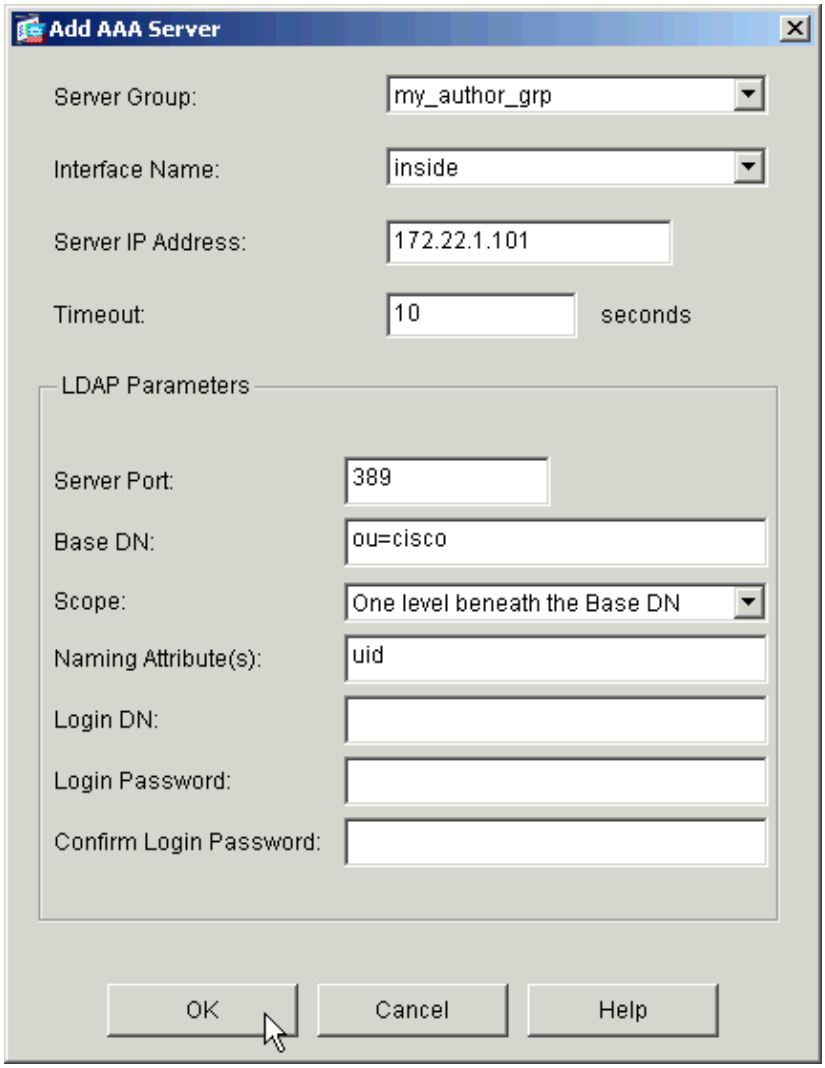


7. Configure an authentication server. Click **OK** when finished.



- **Server Group** Choose the authentication server group configured in step 2.
- **Interface Name** Choose the interface on which the server resides.
- **Server IP Address** Specify the IP address of the authentication server.
- **Timeout** Specify the maximum time, in seconds, to wait for a response from the server.
- **Kerberos Parameters:**
  - **Server Port** 88 is the standard port for Kerberos.
  - **Retry Interval** Choose the desired retry interval.
  - **Kerberos Realm** Enter the name of your Kerberos realm. This is frequently the Windows domain name in all uppercase letters.

8. Configure an authorization server. Click **OK** when finished.



- **Server Group** Choose the authorization server group configured in step 3.
- **Interface Name** Choose the interface on which the server resides.
- **Server IP Address** Specify the IP address of the authorization server.
- **Timeout** Specify the maximum time, in seconds, to wait for a response from the server.
- **LDAP Parameters:**

    - **Server Port**£89 is the default port for LDAP.
    - **Base DN** Enter the location in the LDAP hierarchy where the server should begin to search once it receives an authorization request.
    - **Scope** Choose the extent to which the server should search the LDAP hierarchy once it receives an authorization request.
    - **Naming Attribute(s)** Enter the Relative Distinguished Name attribute(s) by which entries on the LDAP server are uniquely defined. Common naming attributes are Common Name (cn) and User ID (uid).
    - **Login DN** Some LDAP servers, including the Microsoft Active Directory server, require the device to establish a handshake via authenticated binding before they accept requests for any other LDAP operations. The Login DN field defines the authentication characteristics of the device, which should correspond to those of a user with administration privileges. For example, cn=administrator. For anonymous access, leave this field blank.
    - **Login Password** Enter the password for the Login DN.

◊ **Confirm Login Password** Confirm the password for the Login DN.

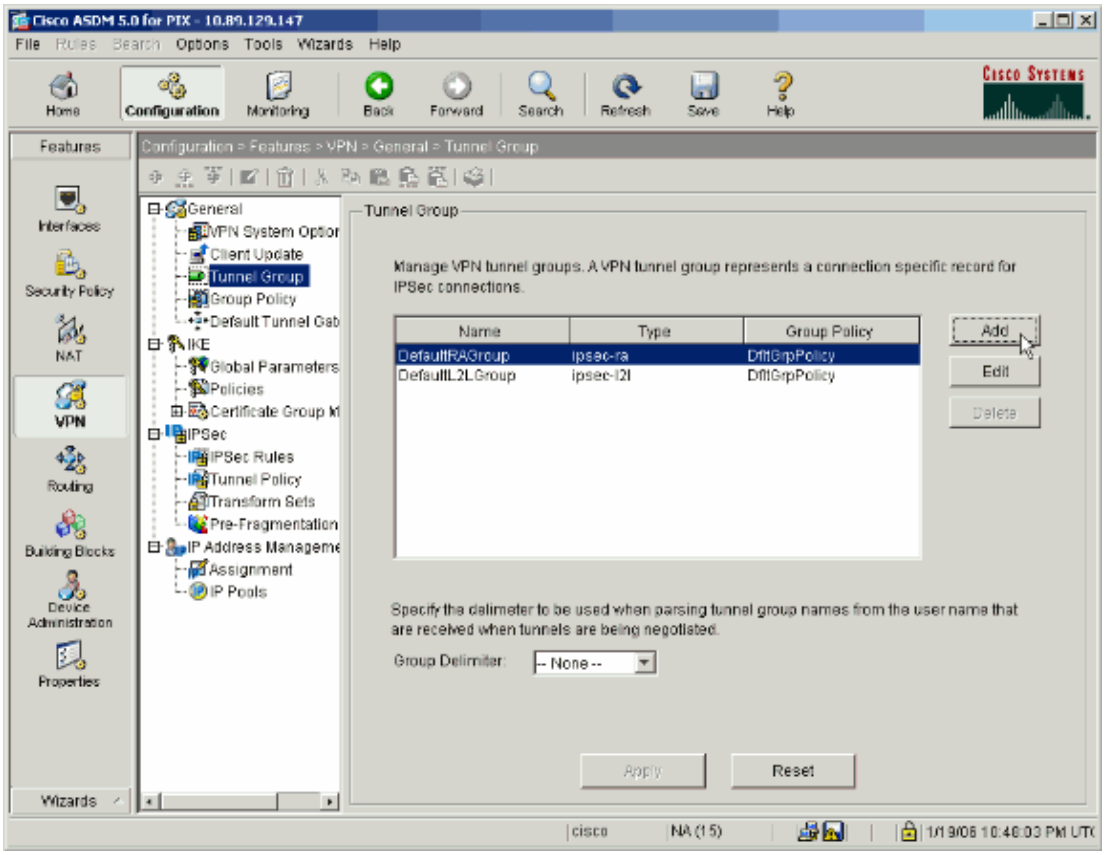
9. Click **Apply** to send the changes to the device after all authentication and authorization servers are added.

   If you have it configured to do so, the PIX now previews the commands that are added to the running configuration.
10. Click **Send** to send the commands to the device.

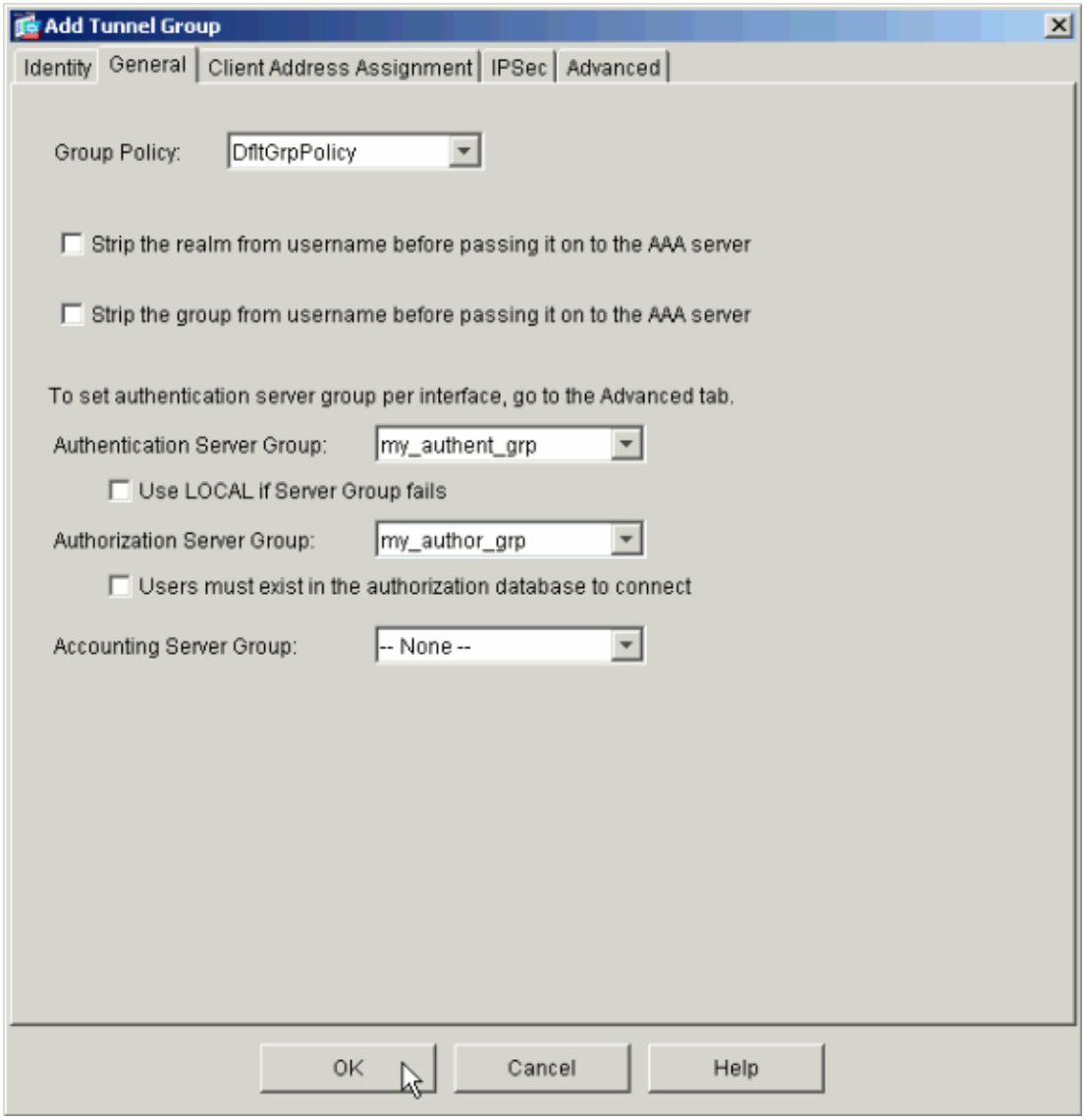
Configure a VPN Tunnel Group for Authentication and Authorization

Complete these steps to add the server groups you just configured to a VPN tunnel group.

1. Select **Configuration > VPN > Tunnel Group** and click **Add** to create a new tunnel group, or **Edit** to modify an existing group.



2. On the General tab of the window that appears, select the server groups configured earlier.



3. *Optional:* Configure the remaining parameters on the other tabs if you are adding a new tunnel group.
4. Click **OK** when finished.
5. Click **Apply** to send the changes to the device after the tunnel group configuration is complete.

   If you have it configured to do so, the PIX now previews the commands that are added to the running configuration.
6. Click **Send** to send the commands to the device.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **Configuring AAA Servers and the Local Database**
- **Cisco ASA 5500 Series Adaptive Security Appliances Product Support**
- **Cisco PIX Firewall Software**
- **Cisco Secure PIX Firewall Command References**
- **Security Product Field Notices (including PIX)**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 22, 2006 Document ID: 68881