

PIX/ASA : Kerberos Authentication and LDAP Authorization Server Groups for VPN Users via ASDM/CLI Configuration Example

Document ID: 68881

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configure Authentication and Authorization for VPN Users using ASDM

- Configure Authentication and Authorization Servers
- Configure a VPN Tunnel Group for Authentication and Authorization

Configure Authentication and Authorization for VPN Users using CLI

Verify

Troubleshoot

Related Information

Introduction

This document describes how to use the Cisco Adaptive Security Device Manager (ASDM) to configure Kerberos authentication and LDAP 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.

Note: Refer to Allowing HTTPS Access for ASDM in order to allow the PIX to be configured by the ASDM.

Components Used

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

- Cisco PIX Security Appliance Software Version 7.x and later
- Cisco ASDM Version 5.x and later

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

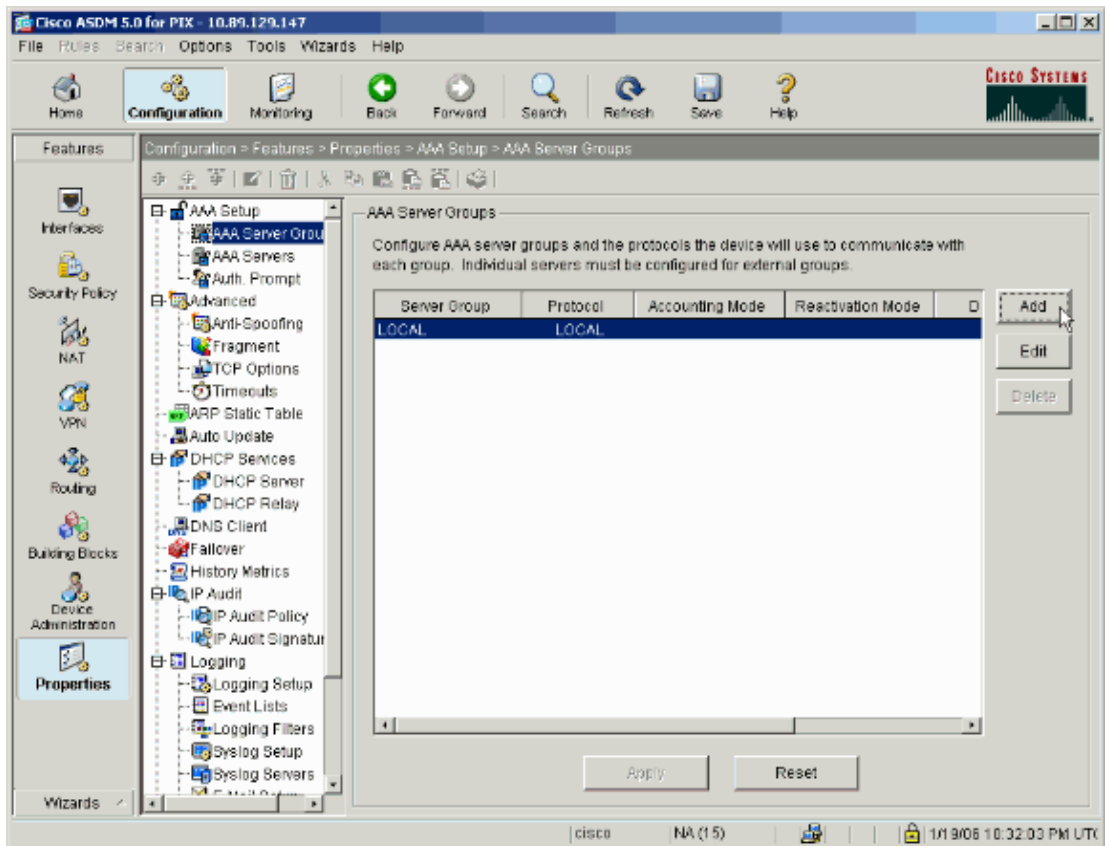
Note: Kerberos is used for the authentication and LDAP is used for the authorization of VPN users in this example.

Configure Authentication and Authorization for VPN Users using ASDM

Configure Authentication and Authorization Servers

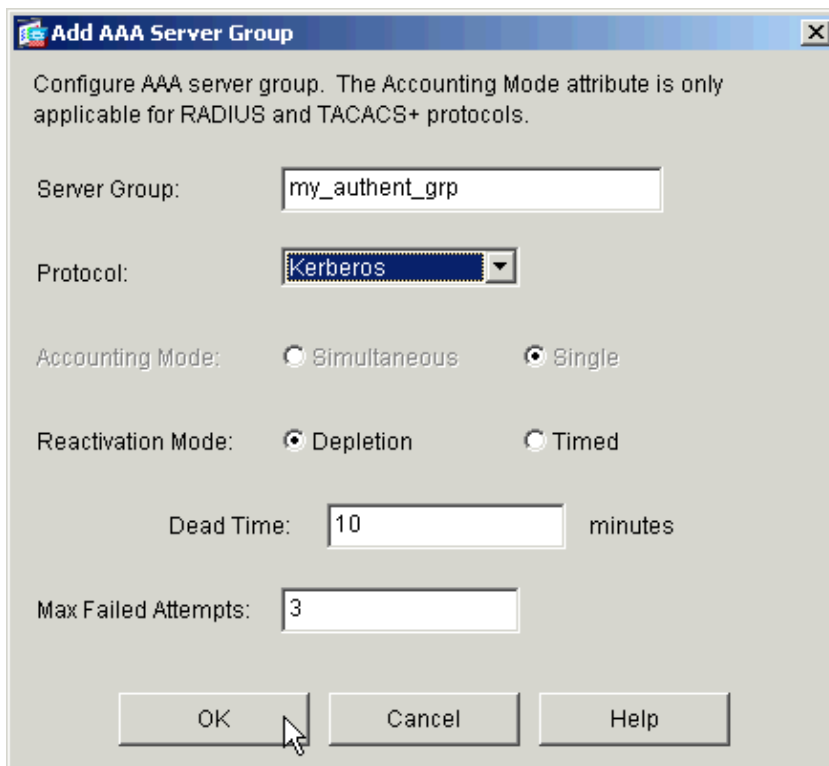
Complete these steps to configure authentication and authorization server groups for VPN users via ASDM.

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

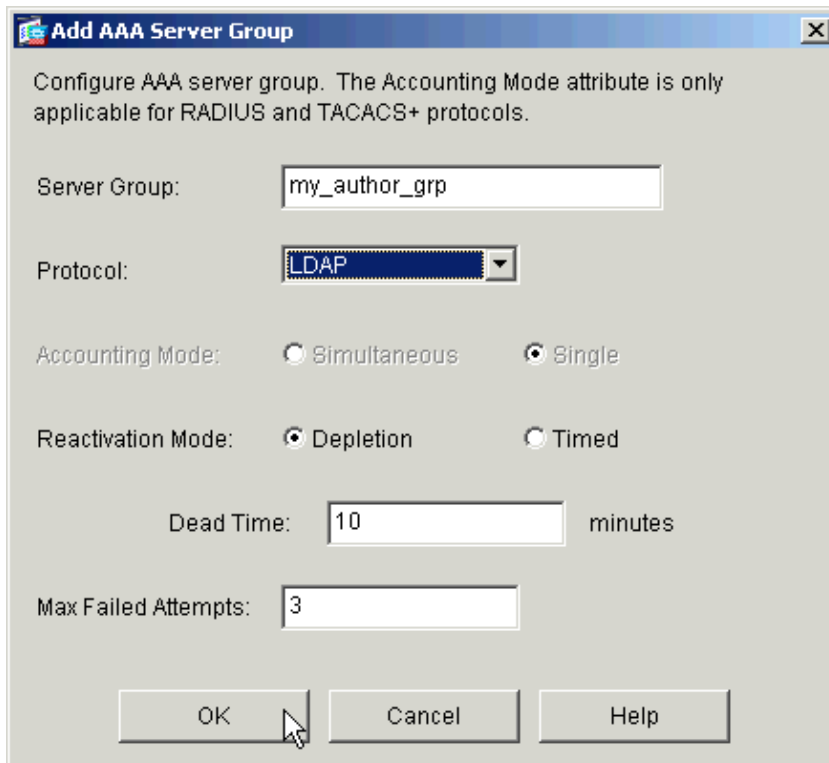


2. Define a name for the new authentication server group and choose a protocol.

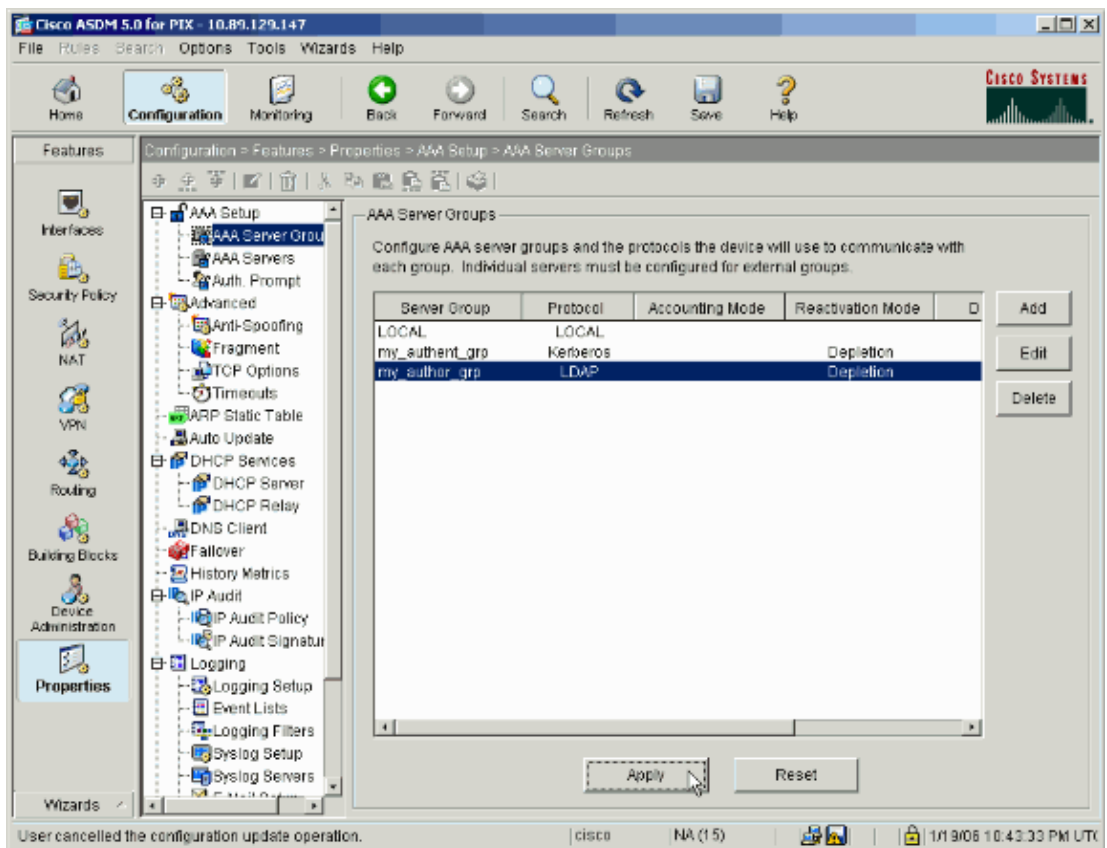
The Accounting Mode option is for RADIUS and TACACS+ only. Click **OK** when you are done.



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

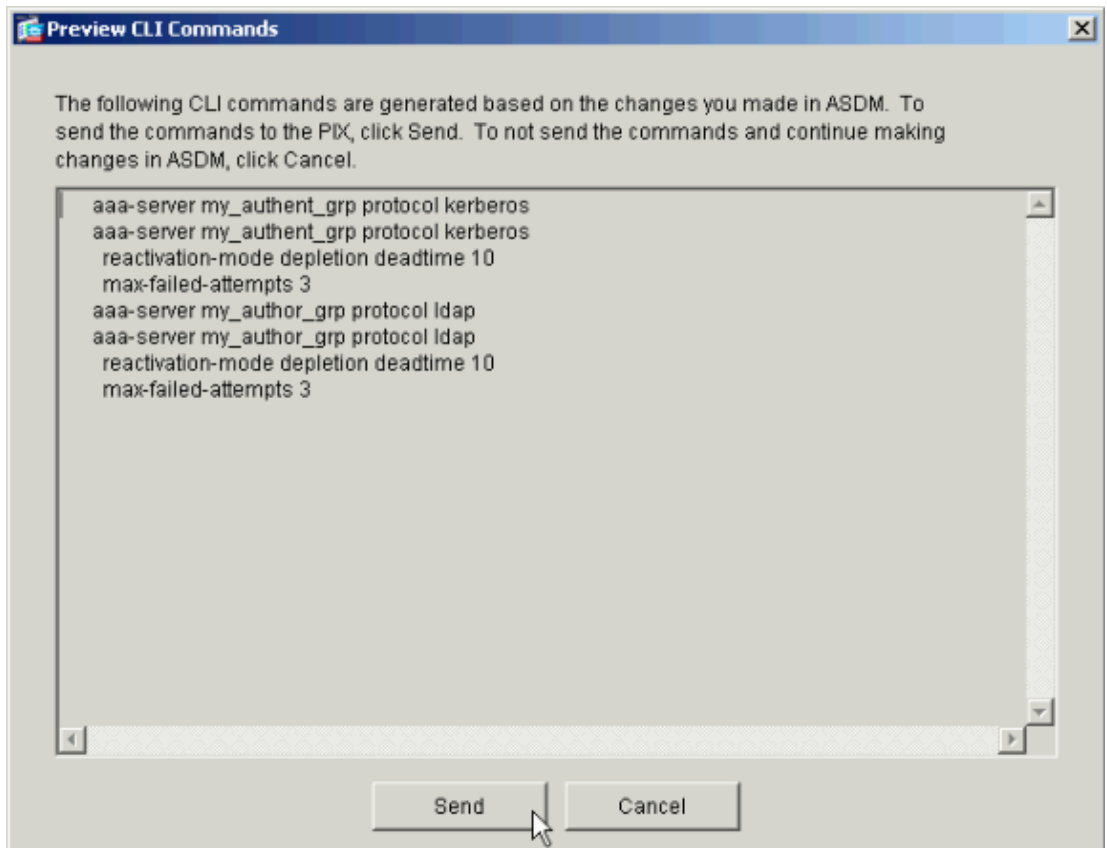


4. Click **Apply** to send the changes to the device.



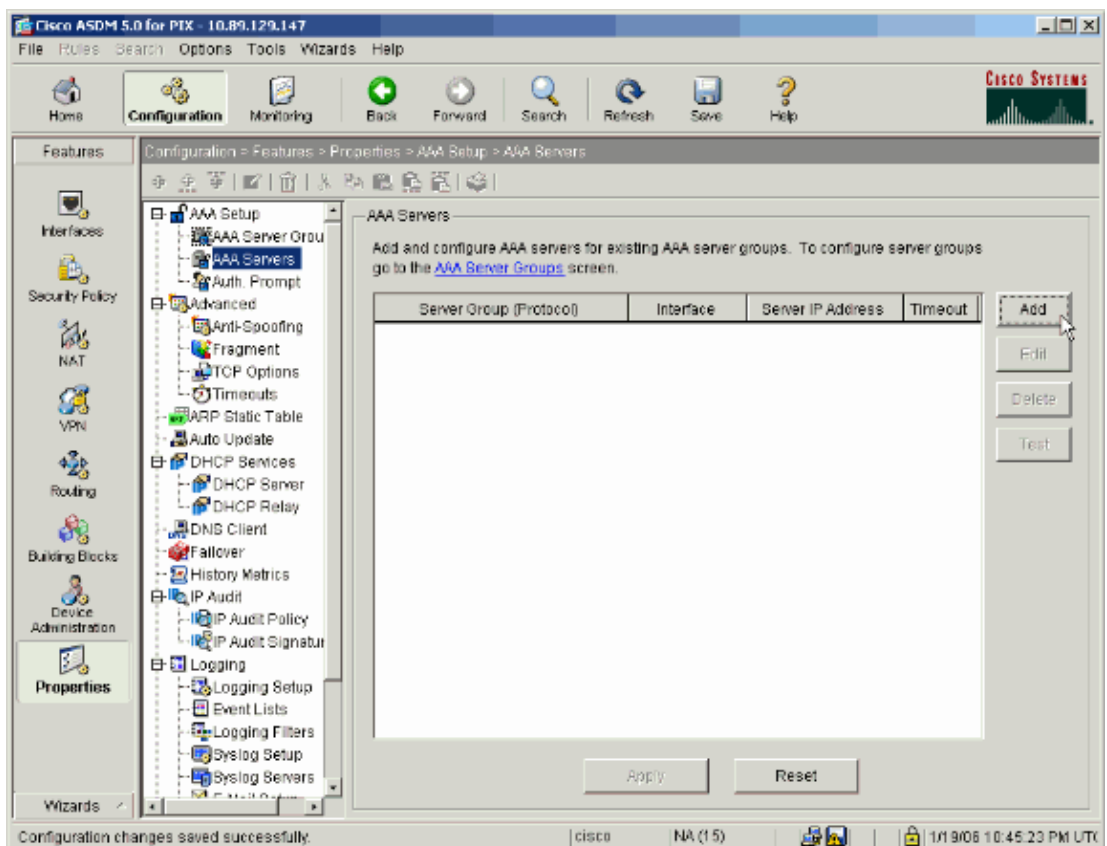
If you have it configured to do so, the device now previews the commands that are added to the running configuration.

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. Choose **Configuration > Properties > AAA Setup > AAA Servers** and click **Add**.



7. Configure an authentication server. Click **OK** when you are done.

Add AAA Server

Server Group: my_authent_grp

Interface Name: inside

Server IP Address: 172.22.1.100

Timeout: 10 seconds

Kerberos Parameters

Server Port: 88

Retry Interval: 10 seconds

Kerberos Realm: REALM.CISCO.COM

OK Cancel Help

- ◆ **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** 389 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.

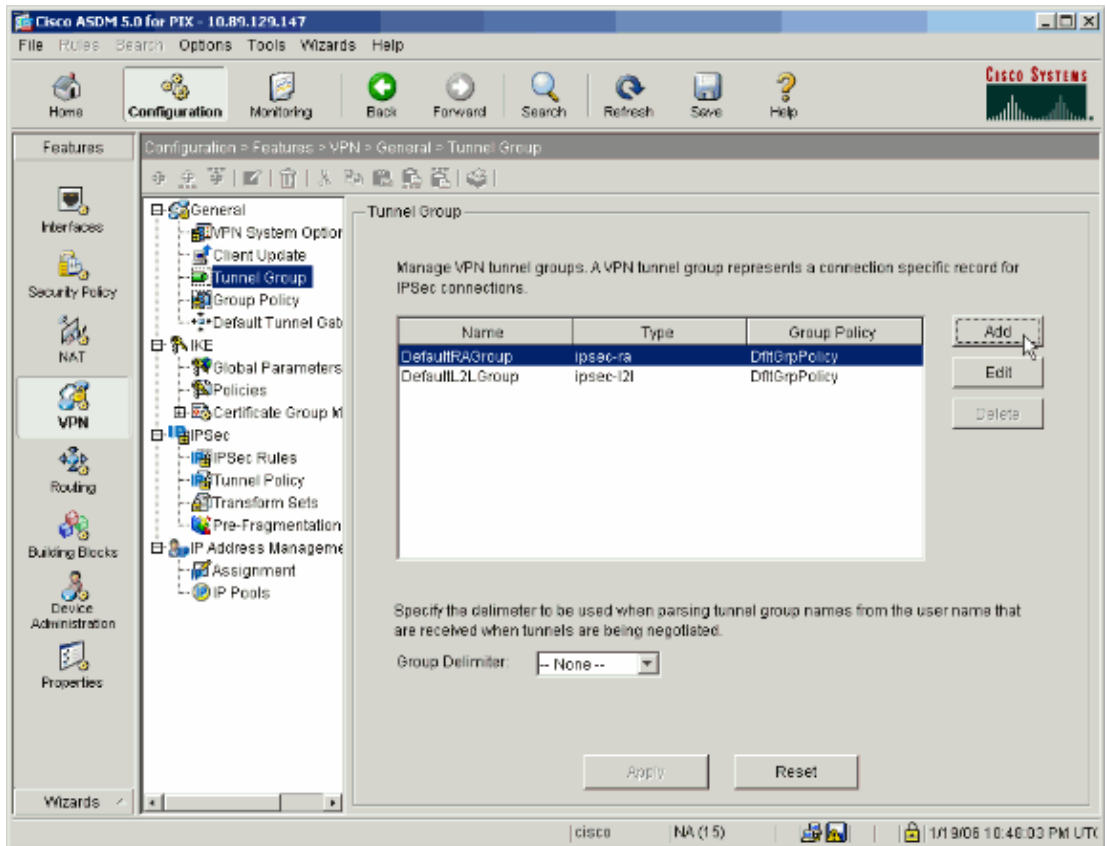
If you have it configured to do so, the PIX now previews the commands that are added to the running configuration.

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

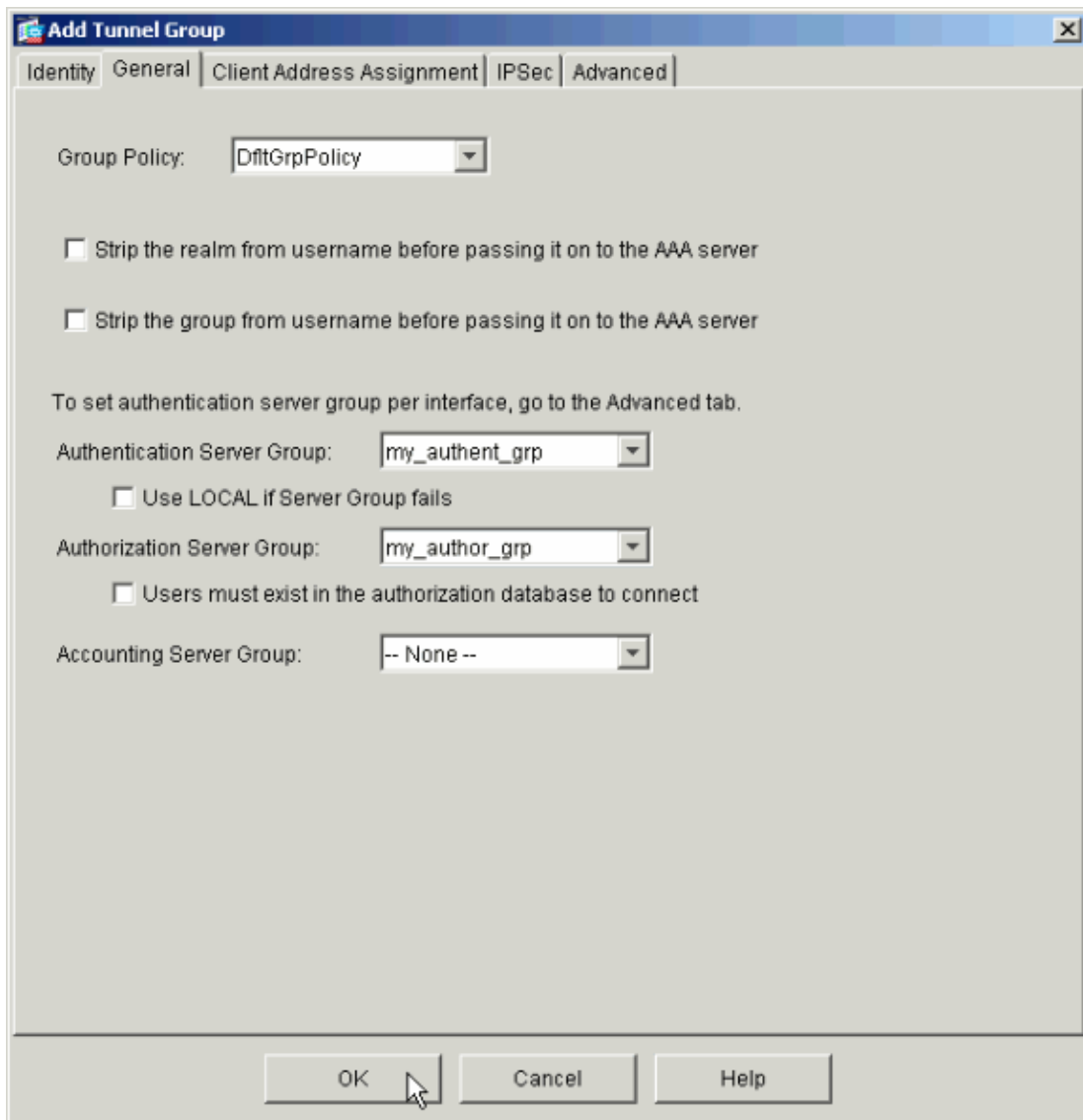
Configure a VPN Tunnel Group for Authentication and Authorization

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

1. Choose **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 add a new tunnel group.
4. Click **OK** when you are done.
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.

Configure Authentication and Authorization for VPN Users using CLI

This is the equivalent CLI configuration for the Authentication and Authorization server groups for VPN users.

Security Appliance CLI Configuration
<pre>pixfirewall#show run : Saved : PIX Version 7.2(2) ! hostname pixfirewall</pre>

```

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

!

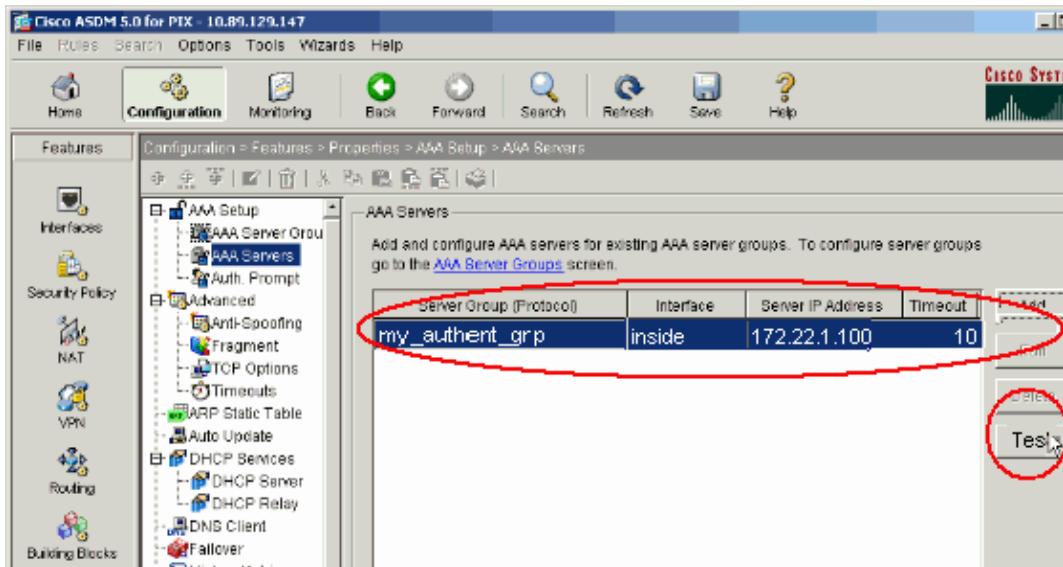
!--- Output is suppressed.

```

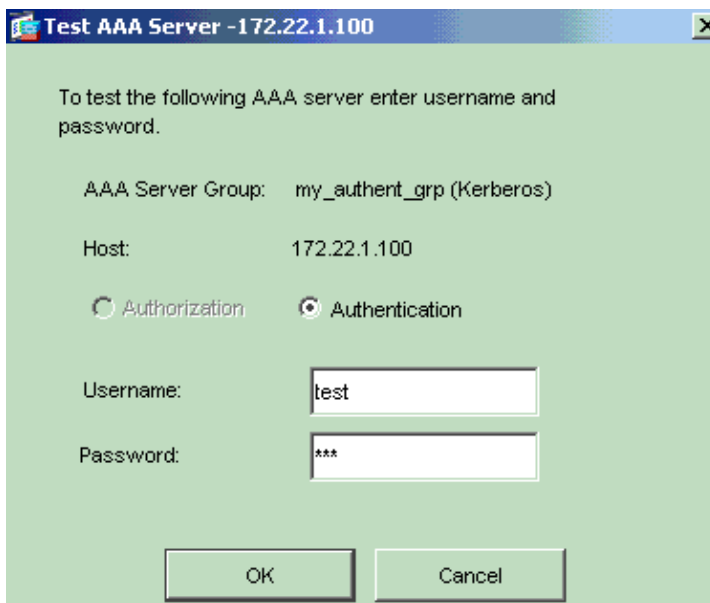
Verify

Complete these steps in order to verify the user authentication between the PIX/ASA and AAA server:

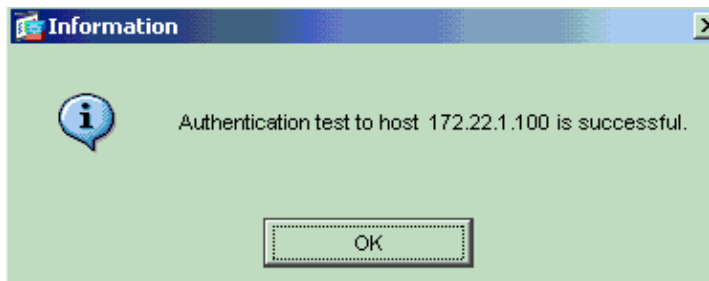
1. Choose **Configuration > Properties > AAA Setup > AAA Servers** and select the server group (my_authent_grp). Then click **Test** to validate the user credentials.



2. Provide the Username and Password (for example, username: test and password: test) and click **OK** in order to validate.



3. You can see the Authentication is successful.



Troubleshoot

1. One frequent cause of authentication failure is clock skew. Be sure that the clocks on the PIX or ASA and your authentication server are synchronized.

When authentication fails due to Clock Skew, you might receive this error message: :- ERROR: Authentication Rejected: Clock skew greater than 300 seconds.. Also, this

log message will be seen:

```
%PIX|ASA-3-113020: Kerberos error : Clock skew with server  
ip_address greater than 300 seconds
```

`ip_address` The IP address of the Kerberos server.

This message is displayed when authentication for an IPSec or WebVPN user through a Kerberos server fails because the clocks on the security appliance and the server are more than five minutes (300 seconds) apart. When this occurs, the connection attempt is rejected.

Synchronizing the clocks on the security appliance and the Kerberos server resolves the issue.
2. Pre-authentication on the Active Directory (AD) should be disabled or it can lead to user authentication failure.

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](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 30, 2007

Document ID: 68881
