# **Table of Contents**

Authentication and Authorization Server Groups for VPN Users via ASDM Configuration Example	<u>21</u>
Document ID: 68881	1
Introduction	1
Prerequisites	1
Requirements	1
Components Used	1
Related Products	1
<u>Conventions</u>	2
Background Information	2
Configure Authentication and Authorization for VPN Users	2
Configure Authentication and Authorization Servers	2
Configure a VPN Tunnel Group for Authentication and Authorization.	9
Verify	10
Troubleshoot	10
NetPro Discussion Forums – Featured Conversations.	11
Related Information	11

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

#### Document ID: 68881

Introduction Prerequisites Requirements Components Used Related Products Conventions Background Information Configure Authentication and Authorization for VPN Users Configure Authentication and Authorization Servers Configure a VPN Tunnel Group for Authentication and Authorization Verify Troubleshoot NetPro Discussion Forums – Featured Conversations Related Information

## 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	ιδάρ
Authentication	Ves	Ves	Ves	Ves	Ves	Ves	No
Authorization	Ves	Ves	No	No	No	No	Ves

**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.

🔂 Add AAA Server Gro	pup	×
Configure AAA server applicable for RADIUS	group. The Accounting 3 and TACACS+ protoco	Mode attribute is only Is.
Server Group:	my_authent_grp	
Protocol:	Kerberos	•
Accounting Mode:	C Simultaneous	● Single
Reactivation Mode:	Output in the second	C Timed
Dead Tir	ne: 10	minutes
Max Failed Attempts:	3	
ок	Cancel	Help

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

🐞 Add AAA Server Gro	🔂 Add AAA Server Group			
Configure AAA server g applicable for RADIUS	group. The Accounting Mode attribute is only and TACACS+ protocols.			
Server Group:	my_author_grp			
Protocol:				
Accounting Mode:	C Simultaneous 💿 Single			
Reactivation Mode:	Depletion     O Timed			
Dead Tin	ne: 10 minutes			
Max Failed Attempts:	3			
ОК	Cancel Help			

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

Cisco ASDM 5.0	) for PIX - 10.89.129.147	Hain				
		0 0	$Q \mid Q$		2	Cisco Systems
Home	configuration Monitoring	Back Forward	Search Refresh	Save H	ekp	Միս
Features	Configuration > Features > Prop	erties > AAA Setup > AA	A Berver Groups			
_	●金革 ■ 前 あち	( 🛍 🕵 🛍 🤪 👘				
	🕀 🚽 🗛 Setup	AAA Server Groups				
Interfaces	AAA Server Grou	Configure AAA server (	proups and the prot	tocols the device w	III use to communicate	e with
📄 🔒,	- BAA Servers	each group. Individua	servers must be c	onfigured for extern	al groups.	
Security Policy	B Advanced	Server Group	Protocol A	Accounting Mode	Reactivation Mode	D Add
24	Anti-Spoofing	LOCAL	LOCAL			
NAT	Fragment	my_authent_grp	Kerberos		Depletion Depletion	Edit
07	Timeouts	my_addror_grp	CD/P		Depletion	Delete
VPN	- ARP Static Table					
43.	E Auto Update					
Pation	- PDHCP Server					
0	- 🚰 DHCP Relay					
68	DNS Client					
Building Blocks	- Se History Metrics					
<u></u>	🕀 🍋 IP Audit					
Administration	- Il@IP Audit Policy					
51	E Logging					
Properties	- 🖏 Logging Setup 🦷					
	- Event Lists	1				
	Syslog Setup					
	Byslog Servers		Арр	IV D	Reset	
Wizards <						
User cancelled th	e configuration update operation		cisco	NA (15)	😹 🔂 🔢 🗎	1/19/06 10:43:33 PM UTC

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**.

Cisco ASDM 5.0	) for PIX - 10.89.129.147	Hale		
File Rules be	and Opports roots wizards	neip		Casco Systems
	antinum Maniadan	Early Engaged Saards Endersh		alı. di.
nome (G		baba Purward asarch Pherean	Same Help	Antillinead line -
Features	Configuration > Features > Pro	nerties > AVA Setup > AVA Servers		
	a 7 a m 1 1 2 0			
Interfaces	H MAK Setup	AAA Servers		
<u>a</u> .	AAA Servers	Add and configure AAA servers for existing on to the AGA Server Groups screen	AAA server groups. To configure	server groups
Security Policy	- Star Auth. Prompt			
31.	H MAdvanced	Server Group (Protocol)	nterface Server IP Address	Timeout Add
NAT.	Fragment			Edit
	- PTCP Options			
S.	ARP Static Table			Delete
VPN	- 🛃 Auto Update			Test
423	E PDHCP Services			
Routing	- DHCP Sawar			
- <b>8</b> 2	DNS Client			
Building Blocks	Fallover			
2.	Plistory Metrics			
Device Administration	Paulit Policy			
	는 나 叱찮 IP Audit Signatur			
Properties				
	🔁 Event Lists			
		1		
	-Bysing Servers	Apply	Reset	
Wizards - 4	1 1 M = 11.2 O			
Configuration cha	inges saved successfully.	cisco	NA (15) 🎼 🛃 📔	🚔   1/19/06 10:46:23 PM UTC

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

付 Add AAA Server						×
Server Group:		my_authent	t_grp		•	
Interface Name:		inside			•	
Server IP Address:		172.22.1.10	0			
Timeout:		10		seconds		
Kerberos Parame	ters					]
Server Port:	88					
Retry Interval:	10 second:	s			•	
Kerberos Realm:	REALM.CIS	SCO.COM				
ОК		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.
  - **A 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.

🚰 Add AAA Server	×
Server Group:	my_author_grp
Interface Name:	inside 💌
Server IP Address:	172.22.1.101
Timeout:	10 seconds
LDAP Parameters	
Server Port:	389
Base DN:	ou=cisco
Scope:	One level beneath the Base DN
Naming Attribute(s):	uid
Login DN:	
Login Password:	
Confirm Login Password:	
ок 🔓 –	Cancel Help

- 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.
  - **\langle 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.

File Rules S	5.0 for PIX - 10.89.129.147 earch Options Tools Wizards	s Help			
ổ Home	Configuration Monitoring	Back Forward Search	Refresh Save	? Help	CISCO SYSTEMS
Features	Configuration > Features > VP	'N > General > Tunnel Group			
Interfaces	Client Update     Client	Tunnel Group Manage VPN tunnel grau IPSec connections.	ps. A VPN tunnel group	represents a connection s;	pecific record for
64	E SIKE	Name	Туре	Group Policy	Add
VIDAL	Global Parameters     Solution     Gertificate Group M     Gertificate Group M     GiPSec     GiPSec Rules     GiPSec Rules     GiPSec Rules     GiP Pre-Fragmentation     GiP Address Manageme     GiP Address Manageme     GiP Pools	Specify the delimeter to b are received when tunnel Group Delimiter:	ipsec-121 s used when parsing tu s are being negotiated. one  Apply	DiffGrpPolicy nnel group names from the Reset	Edit Delete
THEATUS -			Lainea Iblà (15)		
			cisco NA (15)		1/19/06/10:46:03 PM UTC

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

🚰 Add Tunnel Group	×
Identity General Client Address Assignment IPSec Advanced	
Group Policy: DfltGrpPolicy	
Strip the realm from username before passing it on to the AAA server	
Strip the group from username before passing it on to the AAA server	
To set authentication server group per interface, go to the Advanced tab.	
Authentication Server Group: my_authent_grp	
Use LOCAL if Server Group fails	
Authorization Server Group: my_author_grp	
Users must exist in the authorization database to connect	
Accounting Server Group:	
OK Cancel Help	

- 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

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Feb 22, 2006

Document ID: 68881