Table of Contents

PIX Security Appliance (Version 7.x) or ASA 5500 with Three Internal Networks Configuration	<u>ation</u>
<u>Example</u>	1
<u>Document ID: 63880</u>	1
Introduction	1
Prerequisites	1
<u>Requirements</u>	1
Components Used	1
Conventions.	2
<u>Configure</u> .	2
Network Diagram.	2
Configurations	2
	22
Troubleshoot	22
Troubleshooting Commands.	22
NetPro Discussion Forums – Featured Conversations.	
Related Information	27

PIX Security Appliance (Version 7.x) or ASA 5500 with Three Internal Networks Configuration Example

Document ID: 63880

Introduction Prerequisites Requirements Components Used Conventions Configure Network Diagram Configurations Verify Troubleshoot Troubleshooting Commands NetPro Discussion Forums – Featured Conversations Related Information

Introduction

This document provides a sample configuration for PIX Security Appliance (Version 7.x) or Adaptive Security Appliance (ASA) 5500, with three internal networks. For simplicity, static routes are used.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- PIX Security Appliance 515E with Software version 7.0
- Cisco routers with Cisco IOS® Software Release 12.3(7)T

Note: While the configuration in this document was tested on a PIX Security Appliance, it is also compatible with the ASA 5500.

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.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses this network setup:



The default gateway of the hosts on the 10.1.1.0 network points to RouterA. A default route on RouterB is added that points to RouterA. RouterA has a default route that points to the PIX inside interface.

Configurations

This document uses these configurations:

- RouterA Configuration
- RouterB Configuration
- PIX Security Appliance (Version 7.0) Configuration, including both:
 - ♦ PIX Security Appliance Advanced Security Device Manager (ASDM) Bootstrap and GUI
 - ◆ PIX Security Appliance Command Line Interface (CLI)

RouterA Configuration

```
RouterA#show running-config
Building configuration...
```

```
Current configuration : 1151 bytes
```

Cisco - PIX Security Appliance (Version 7.x) or ASA 5500 with Three Internal Networks Configuration Exam

```
!
version 12.3
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname RouterA
!
interface Ethernet2/0
ip address 10.2.1.1 255.255.255.0
half-duplex
1
interface Ethernet2/1
ip address 10.1.1.2 255.255.255.0
half-duplex
1
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
!
1
line con 0
line aux 0
line vty 0 4
1
end
RouterA#
```

RouterB Configuration RouterB#show running-config Building configuration... Current configuration : 1132 bytes version 12.3 service config service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption hostname RouterB interface FastEthernet0/0 ip address 10.1.1.3 255.255.255.0 speed auto interface Ethernet1/0 ip address 10.3.1.1 255.255.255.0 half-duplex ip classless ip route 0.0.0.0 0.0.0.0 10.1.1.2 control-plane

!

1

1

!

1

1

! !

```
line con 0
line aux 0
line vty 0 4
!
end
RouterB#
```

If you would like to use the ASDM for configuration of the PIX Security Appliance, but have not yet bootstrapped the device, see these instructions:

- Console into the PIX.
- From a cleared configuration, use the interactive prompts to enable ASDM for the management of the PIX from the Workstation 10.1.1.

```
PIX Security Appliance (Version 7.0) Configuration
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
 Year [2005]:
 Month [Mar]:
 Day [15]:
 Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5
The following configuration will be used:
         Enable password: cisco
         Allow password recovery: yes
         Clock (UTC): 14:45:00 Mar 15 2005
         Firewall Mode: Routed
         Inside IP address: 10.1.1.1
         Inside network mask: 255.255.255.0
        Host name: OZ-PIX
        Domain name: cisco.com
         IP address of host running Device Manager: 10.1.1.5
Use this configuration and write to flash? yes
         INFO: Security level for "inside" set to 100 by default.
         Cryptochecksum: a0bff9bb aa3d815f c9fd269a 3f67fef5
965 bytes copied in 0.880 secs
         INFO: converting 'fixup protocol dns maximum-length 512' to MPF commands
         INFO: converting 'fixup protocol ftp 21' to MPF commands
         INFO: converting 'fixup protocol h323_h225 1720' to MPF commands
         INFO: converting 'fixup protocol h323_ras 1718-1719' to MPF commands
         INFO: converting 'fixup protocol netbios 137-138' to MPF commands
         INFO: converting 'fixup protocol rsh 514' to MPF commands
         INFO: converting 'fixup protocol rtsp 554' to MPF commands
         INFO: converting 'fixup protocol sip 5060' to MPF commands
         INFO: converting 'fixup protocol skinny 2000' to MPF commands
         INFO: converting 'fixup protocol smtp 25' to MPF commands
         INFO: converting 'fixup protocol sqlnet 1521' to MPF commands
         INFO: converting 'fixup protocol sunrpc_udp 111' to MPF commands
         INFO: converting 'fixup protocol tftp 69' to MPF commands
         INFO: converting 'fixup protocol sip udp 5060' to MPF commands
         INFO: converting 'fixup protocol xdmcp 177' to MPF commands
```

Complete these steps to configure via the ASDM GUI:

- 1. From Workstation 10.1.1.5, open a Web browser to use ADSM (in this example, https://10.1.1.1).
- 2. Click **yes** on the certificate prompts.
- 3. Log in with the enable password, as configured above.
- 4. If this is the first time ASDM is run on the PC, you are prompted to use ASDM Launcher or ASDM as a Java App. In this example, the ASDM Launcher is selected and installed.
- 5. Go to the ASDM Home screen. Click the **Configuration** tab.

Image: NonitoringImage: NonitoringIm	Refresh Save Interface Status Interface Interface IP Address/Mask Inside 10.1.1.1/24 Select an interface to view input and out Traffic Status Connections Per Second Usage
Device Information General License Host Name: OZ-PIX.cisco.com PIX Version: 7.0(0)102 Device Uptime: 0d 0h 9m 19s ASDM Version: 5.0(0)73 Device Type: PIX 515E Firewall Mode: Routed Context Mode: Single Total Flash: 16 MB Total Memory: 64 MB VPN Status IKE Tunnels: 0 IPSec Tunnels: 0 System Resources Status CPU Usage (percent) 000000000000000000000000000000000000	Interface Status Interface IP Address/Mask inside 10.1.1.1/24 Select an interface to view input and out Traffic Status Connections Per Second Usage
18 % 44 14:52:41 14:52:31 Memory 14:52:31 14:52:41 14:52:31 14:52:41 14:52:31 Latest ASDM Syslog Messages Syslog Disabled	0.5 14:52:31 UDP: 0 TCP: 0 'inside' Interface Traffic Usage (Kbps) 80 44 32 16 14:52:31 Input Kbps: 0 Outp

6. Configure the Outside Interface by selecting **Interface > Edit**.

📧 Cisco ASDM	5.0 for PIX - 10.1.1.1						
File Rules Se	earch Options Tools Wizards	Help					
G Home	Configuration Monitoring	Back Fo	• rward	Q Search	Refresh S	Save Help	
Features	Configuration > Features > Inter	faces					
Interfaces	ቀ <u>ቀ</u> ∓ 	896	3 			1	
<u>6</u> ,	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Ma On
Security Policy	Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	
NAT	Ethernet0		No				
S VPN							
♦ Routing							
Building Blocks							
Device Administration							
	•						
Properties	Enable traffic between two) or more inte	erfaces wi	hich are c	onfigured with sa	me security levels	
Wizards /				Apply	Re	set	
	11				<admin> N/</admin>	A (15)	

7. Click **OK** on the Warning dialog box.



8. Enter the Interface details. Click **OK** when finished.

🖆 Edit Interface		
Hardware Port:	Ethernet0	Configure Hardware Properties
🗹 Enable Interface	🔲 Dedicate this interface to manag	ement only
Interface Name:	outside	
Security Level:	0	
- IP Address		
• Use Static IP	C Obtain Address via DHCP	
IP Address:	209.165.200.225	
Subnet Mask:	255.255.255.224	
MTU:	1500	
Description:		
	OK Cancel	Help

9. Click **OK** on the Security Level Change dialog box.



10. Click **Apply** to accept the interface configuration. The configuration also gets pushed onto the PIX.

Co	nfiguration > Features > Interfa	aces						
4		667	(()					
	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
	Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	No	1500
	Ethernet0	outside	Yes	0	209.165.200.225	255.255.255.224	No	1500
		I						
								_
	<u> </u>							
	🗖 Enable traffic between two	or more int	erfaces wi	hich are c	onfigured with sar	ne security levels		
				Apply	Res	et		
					codmine MA	(15)		15/02/0
								110/03/0

11. Review the Security Policy Rule used by choosing **Security Policy** on the **Features** Tab. In this example, the Default Inside Rule is used.

Gisco ASDM 5 File Rules Sea	.0 for PIX - arch Options	10.1.1 . s Tools	.1 Wiza	ırds Help						
Home C	onfiguration	Monito	pring	O Back) Forward	Q Search	Q Refresh	I Save	Hel) p
Features	Configuratio	in ≻ Featu	ures >	Security Po	licy > Access	Rules				
Interfaces	Access	∣ 🗹 ∣ 🖞 s Rules es for Inte	گ ∣ گ ⊂ Av erface:	AA Rules	C Filter Rul	es C Ser Show All	vice Policy R	ules		
Security Policy	# Ru	ule A	ction	Sour	ce (Network	Des	tination t(Network	Rule A	oplied	Interfa
NAT	-		~	🄄 any	A CLINICIA	s any	Pretmont	To Hu		inside (outboun
Ø VPN ♦Ž¢										
Routing Routing Building Blocks										
Device Administration										
Properties	•				-					
	V Allov	w traffic		o Deny tr	апіс	1		1	• Sh	ow Sumr
Wizards 🕗					Apply		Reset		Advar	nced
							<admin></admin>	NA (15)		🛃 🔂

12. In this example, NAT is used. Uncheck the box for **Enable traffic through the firewall without** address translation. Click Add to configure the NAT Rule.

Gisco ASDM 5.0 File Rules Sear	<mark>0 for PIX - 1</mark> ch Options	0.1.1.1 Tools Wizard	is Help					
Home Co	ogg nfiguration	Monitoring	O Back	O Forward	Q Search	Refresh	I Save	? Help
Features	Configuration	> Features > N/	AT > Transl	ation Rules				
Interfaces	🕈 👲 🐺	■2 前 み traffic through ti	he firewall v	vithout addre	ss translat	lion		
Security Policy	 Transla Show Rule 	tion Rules es for Interface:	C Tra	nslation Exer	mption Rul	Show All		
NAT	Rule			Original	_	I		Tr
<u> </u>	Туре	Interface	Sourc	e Network	Desti	nation Network	Interfac	ce
Routing Building Blocks Device Administration Properties	↓ ↓ Static	NAT 👯 [Dynamic NA	л "Д S	tatic Policy	NAT	Dynamic Po	licy NAT
Wizards /					Ар	ply <admin></admin>	Reset	t

13. Configure the Source Network. In this example, 10.0.0.0 is used for the IP address, and 255.0.0.0 is used for the mask.

Click **Manage Pools** to define the NAT Pool Addresses.

🕵 Add Address Tr	anslation	Rule					X
Use NAT	C U	se Policy NAT					
_ Source Host/N	letwork—						
		Interface:	inside	•]		
		IP Address:	10.0.0.0				
		Mask:	255.0.0.0	~			
					<u>.</u>		
			Browse				
						NAT Options	
Translate Addres	ss on Inter	face: outsid	le 💌				
- Translate Addi	ress To —						
O 🕂 Sta	atic	IP Address:		~			
	Redirect p	ort					
	C UDP	Original port:	Т	ranslated port			
⊙ י∰ Dyi	namic	Address Pool:	same addres	s 🔻	Manage Pools		
	Pool ID		Addre	ess			
	N/A	No address poo)l defined				
		014		1	11-1-1		
	_	UK	Cancel		неір		

14. Select the outside Interface. Click Add.

obal Address P	ools are used to cont	figure Dynamic Network Address	Translation (NAT)
dresses.			
Interface	Pool ID	IP Address(es)	
side Iteide			Add
nside			
			Edit
			Delata
			Delete

15. In this example, a Range and PAT Address Pool are configured. Configure the Range NAT Pool Address. Click **OK**.

🖆 Add Global Pool Item 🛛 🔀
Interface: outside 💌 Pool ID: 1
Range
C Port Address Translation (PAT)
C Port Address Translation (PAT) using the IP address of the interface
IP Address: 209.165.200.228 - 209.165.200.229
Network Mask (optional): 255.255.254
OK Cancel Help

16. Configure the PAT Address Pool.

it Global Pool	ltem					Ľ	2
	uteide	_	DealUD				
entace: jo	utside		Pool ID:	1			
~ (======							
Range							
Port Address	; Translation (P	AT)					
O Port Address	s Translation (P	AT) using t	the IP addres	s of the in	nterface		
IP Address	200 165 20	00 227	— _ r				
	. 209.105.20	50.227					
Notwork M	lack (ontional):	255.0	255 255 224				
Network IN	ask (optional).	200.2	200.200.224				
	ок	Canc	el	Help			
nage Global A obal Address P	ddress Pools 'ools						
nage Global A obal Address P obal Address P dresses.	oddress Pools ools ools are used to	o configure	e Dynamic Ne	etwork Ado	dress Trar	nslation (Na	AT)
nage Global A obal Address P obal Address P dresses. Interface	oddress Pools Pools ools are used to Pool ID	o configure	e Dynamic Ne IP Addre	etwork Add ss(es)	dress Trar	nslation (N,	AT)
nage Global A Ibal Address P Ibal Address P Ibal Address P Interface Side	ools ools are used to Pool ID	o configure	e Dynamic Ne IP Addre	etwork Ado ss(es)	dress Trar	nslation (N	AT) Add
nage Global A Ibal Address P Ibal Address P Ibal Address P Interface Interface side Itside	ools are used to Pool ID	o configure 09.165.200 09.165.201	Dynamic Ne IP Addre 0.227 0.228-209.16	etwork Add ss(es) 35.200.229	dress Trar	nslation (N,	AT) Add
nage Global A Ibal Address P Ibal Address P Interface side Itside	ools are used to Pools Pool ID Pool ID 1 2 2	o configure 09.165.20 09.165.20	Dynamic Ne IP Addre 0.227 0.228-209.19	etwork Add ss(es) 65.200.229	dress Trar 9	nslation (N/	AT) Add Edit
nage Global A obal Address P ibal Address P iresses. Interface side itside	ools are used to Pool ID	o configure 09.165.20 09.165.20	Dynamic Ne IP Addre 0.227 0.228-209.16	etwork Add ss(es) 35.200.229	dress Trar 9	nslation (N.	AT) Add Edit
nage Global A bbal Address P bal Address P dresses. Interface side dtside	ools are used to Pool ID	o configure 09.165.201	Dynamic Ne IP Addre 0.227 0.228-209.16	etwork Add ss(es) 35.200.229	dress Trar 9	nslation (N/	AT) Add Edit Delete
nage Global A obal Address P obal Address P dresses. Interface side itside	ools are used to Pool ID	o configure 09.165.20 09.165.20	Dynamic Ne IP Addre 0.227 0.228-209.16	etwork Add ss(es) 35.200.229	dress Trar 9	nslation (N.	AT) Add Edit Delete
nage Global A obal Address P obal Address P dresses. Interface side itside	ools are used to Pool ID	o configure 09.165.201	e Dynamic Ne IP Addre 0.227 0.228-209.16	etwork Add ss(es) 35.200.229	dress Trar 9	nslation (N/	AT) Add Edit Delete
nage Global A obal Address P obal Address P dresses. Interface side itside	ools are used to Pool ID	o configure 09.165.20 09.165.20	e Dynamic No IP Addre 0.227 0.228-209.10	etwork Ado ss(es) 35.200.229	dress Trar	nslation (N.	AT) Add Edit Delete
nage Global A bbal Address P bbal Address P dresses. Interface side itside	ools are used to Pool ID	o configure 09.165.201	e Dynamic Ne IP Addre 0.227 0.228-209.16	etwork Add ss(es) 35.200.229	dress Trar 9	nslation (N/	AT) Add Edit Delete
nage Global A obal Address P obal Address P dresses. Interface side utside	ools are used to Pool ID	o configure 09.165.20 09.165.20	Dynamic Ne IP Addre 0.227 0.228-209.10	etwork Add ss(es) 35.200.229	dress Trar	nslation (N.	AT) Add Edit Delete
nage Global A obal Address P dresses. Interface side itside	ools are used to Pool ID	o configure 09.165.201	e Dynamic Ne IP Addre 0.227 0.228-209.16	etwork Add ss(es) 35.200.229	dress Trar 9	nslation (N/	AT) Add Edit Delete
nage Global A obal Address P dresses. Interface side itside	ools are used to Pool ID Pool ID 1 2 2	o configure 09.165.20 09.165.20	9 Dynamic Ne IP Addre 0.227 0.228-209.10	etwork Add ss(es) 35.200.229	dress Trar 9	nslation (N.	AT) Add Edit Delete
nage Global A obal Address P obal Address P dresses. Interface side itside	ools are used to Pool ID Pool ID 1 2 2	o configure 09.165.201	e Dynamic Ne IP Addre 0.227 0.228-209.16	etwork Add	dress Trar 9	nslation (N	AT) Add Edit Delete
nage Global A obal Address P obal Address P dresses. Interface side itside	ools are used to Pool ID Pool ID 1 2 2	o configure	Dynamic Ne IP Addre 0.227 0.228-209.10	etwork Add ss(es) 35.200.229	dress Trar 9 Help	nslation (N	AT) Add Edit Delete

Click OK.

Add Edit Delete
Edit Delete
Edit Delete
Delete
Delete

17. On the Edit Address Translation Rule, select the Pool Id to be used by the Source Network configured. Click **OK**.

Edit Address	; Translatio	n Rule					
🖲 Use NA	r ou	Jse Policy NAT					
-Source Ho	st/Network-						
		Interface:	inside		Y		
		IP Address:	10.0.0.0				
		Mask:	255.0.0.0		~		
			Browse	1			
				_		_	NAT Options
Translate Ad	dress on Inte	erface: outsi	de 👱]			
_ Translate .	Address To –						
0 II	Static	IP Address:			~		
	Redirect	port					
	C UDP	Original port:		Translated	i port:		
• ¶	Dynamic	Address Pool:	1	•	Manage	Pools	
	Pool ID		Ac	Idress			
	1	209.165.200.2	27 29-200 165 2	00.220			
		12113 1113 2110 2		00.224			
				(

18. Click **Apply** to push the configured NAT Rule to the PIX.

File Rules Se	5.0 for PIX - earch Options	10.1.1.1 Tools Wizar	ds Help			
Shome	Configuration	Monitoring	Back Forward	Q Q Search Refresh	Save Help	
Features	Configuration	n ≻ Features ≻ N	AT > Translation Rules			
	🗣 🏦 🐨	e traffic through t	📭 🛍 💁 🏹 🗳 I	s translation		
Geourity Policy	 Transl Show Ru 	lation Rules Iles for Interface	C Translation Exem	ption Rules		
NAT	Rule		Original			Tra
<u> </u>	Туре	Interface	Source Network	Destination Network	Interface	
VPN	-18	inside	_⊡ 10.0.0.0/8	🎨 any	outside	209.16 209.16
Routing		1	1			
Ruilding Blocks						
Device Administration						
Properties						
	• Statio	NAT	Dynamic NAT 🛛 🔒 Sta	tic Policy NAT 🛛 🔒 D)ynamic Policy N	IAT
Wizards /				Apply	Reset	
Device configura	ation loaded suc	ccessfully.		<admin> N</admin>	VA (15)	🛃 🔂

19. In this example, static routes are used. Choose Routing under the **Features** Tab. Choose **Static Route** > **Add**

File Rules Se	Configuration	zards Help O Back For	ward Searc	h Refres	, 調	? Help	
Features	Configuration > Features > Configuration > Configuration > Configuration > Configu	Routing > Routing Static Route - Specify static Interface	Static Route Static Route	Netmask	Gateway IP	Reset	
				<admin></admin>	NA (15)		} 🗖

20. Configure the Default Gateway. Click **OK**.

🖆 Add Static Route		×
Interface Name:	outside 💌	
IP Address:	0.0.0.0	
Mask:	0.0.0.0	
Gateway IP:	209.165.200.226	
Metric	1	
C Tunneled (Used or	nly for default route)	
ок	Cancel Help	

21. Click **Add**. Add the routes to the Inside Networks.

🕵 Add Static Route		
Interface Name	e: inside 💌	
IP Address:	10.2.1.0	
Mask:	255.255.255.0	
Gateway IP:	10.1.1.2	
 Metric 	1	
C Tunneled (U:	sed only for default route)	
ок	Cancel Help	

🖆 Add Static Route	
Interface Name:	inside 💌
IP Address:	10.3.1.0
Mask:	255.255.255.0
Gateway IP:	10.1.1.3
Metric	1
C Tunneled (Used o	nly for default route)
ок	Cancel Help

22. Confirm that the Correct Routes are configured. Click Apply.



Configuration via the ASDM GUI is now complete.

The following configuration is what you should see via the command line interface:

```
PIX Security Appliance Command Line Interface (CLI)

pixfirewall(config)# write terminal

PIX Version 7.0(0)102

names

!

interface Ethernet0

nameif outside

security-level 0

ip address 209.165.200.225 255.255.224

!
```

Cisco - PIX Security Appliance (Version 7.x) or ASA 5500 with Three Internal Networks Configuration Exam

```
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
1
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname OZ-PIX
domain-name cisco.com
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 209.165.200.228-209.165.200.229 netmask 255.255.255.224
global (outside) 1 209.165.200.227 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0
route inside 10.3.1.0 255.255.255.0 10.1.1.3 1
route inside 10.2.1.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 209.165.200.226 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00
   h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00
   sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.5 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
1
class-map inspection_default
match default-inspection-traffic
I.
1
policy-map asa_global_fw_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
service-policy asa_global_fw_policy global
```

Cisco – PIX Security Appliance (Version 7.x) or ASA 5500 with Three Internal Networks Configuration Exam

The resulting CLI configuration can be viewed in ASDM by choosing **File > Show Running Configuration in New Window**.

File	Rules	Search	Options	Tools	Wizards	Help
Re Re	fresh AS set Devi	DM with t ce to the f	he Runnir Factory De	ig Confij fault Co	guration or nfiguration	n the Device
Sh	ow Runr	ning Confi	guration i	n New M	/indow	
Sar Sar Sar Sar	ve Runni ve Runni ve Runni ve Intern	ing Config ing Config ing Config al Log Bu	guration to guration to guration to ffer to Flas	Flash TFTP S Standb sh	erver y Unit	
Pri	nt					
Cle Cle	ear ASDN ear Interr	vl Cache nal Log Bu	Jffer			
Exi	t					

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

Note: Before issuing debug commands, refer to Important Information on Debug Commands.

- **debug icmp trace** Shows whether ICMP requests from the hosts reach the PIX. To run this debug, you need to add the **access–list** command to permit ICMP in your configuration.
- **logging buffer debugging** Shows connections being established and denied to hosts that go through the PIX. The information is stored in the PIX log buffer and the output can be seen using the **show log** command.

ASDM can be used to enable logging, and also to view the logs:

1. Choose Configuration > Properties > Logging > Logging Setup. Choose Enable Logging. Click Apply.

Cisco ASDM 5	5.0 for PIX - 10.1.1.1		
File Rules Se	arch Options Tools Wizards	Help	
G Home C	Configuration Monitoring E	C C C C C C C C C C C C C C C C C C C	h Save Help
Features	Configuration > Features > Prope	rties ≻ Logging ≻ Logging Setup	
Interfaces Interfaces Security Policy Security Policy NAT Security Policy NAT Security VPN Security Properties	AAA Setup AAA Setup AAA Server Grou AAA Servers AAA S	Cogging Setup Image: Setup	I Enable logging is Send syslogs i o which syslogs will be saved. ntents before the buffer is over Configure FTP Settings Configure Flash Usage gs intended for viewing in ASE
		Sagrinis	14A (15)

Cisco ASDM ! File Rules Se	5.0 for PIX - 10.1.1.1 arch Options Tools Wizar	rds Help
Iome	Configuration	O O Q Q Image: Constraint of the state o
Features Interfaces VPN Routing Administration Connection Graphs Logging IP Audit	Monitoring > Features > Logg	Click the View button below to display syslog messages in the ASDM as of now. Select the desired logging level to see mess or higher. Logging Level: Debugging View
		<admin> NA (15) 🛛 🛃</admin>

2. Choose **Monitoring > Logging > Log Buffer > Logging Level**. Choose **Logging Buffer** from the drop–down list. Click **View**.

G Cisco ASDM 5 File Rules Se	5.0 for PIX - 10.1.1.1 arch Options Tools Wizar	ds Help					
Contraction of the second seco	Configuration	G Back	O Forward	Q Search	Q Refresh	I Save	? Help
Features Interfaces VPN Connection Graphs Logging IP Audit	Monitoring > Features > Logo	ing > Log Buffe	uffer Click the Vi ASDM as o or higher. L	ew button belo f now. Select ti ogging Level:	ow to displ he desired Debug	ay syslog r logging le ging	nessages in the vel to see mess
	I			<a< th=""><th>dmin≻</th><th>NA (15)</th><th></th></a<>	dmin≻	NA (15)	

3. Here is an exampe of the Log Buffer.

🖆 Log Buffer

This screen shows syslog messages in ASDM logging buffer as of now.

Find text in messages below:

Find Next

Severity	Time		
<u>4</u> 6	Mar 15 2005 15:30:19	605005: Login permitted from 10.1.1.5/3776 to inside:10.1.1.1/https for user "enab	i
▲ 6	Mar 15 2005 15:30:19	302013: Built inbound TCP connection 123 for inside:10.1.1.5/3776 (10.1.1.5/3776)
0 2	Mar 15 2005 15:30:12	106001: Inbound TCP connection denied from 209.165.200.226/23 to 209.165.200)
🖬 3	Mar 15 2005 15:29:56	710003: UDP access denied by ACL from 10.1.1.5/138 to NP Identity Ifc:10.1.1.255	1
🖬 3	Mar 15 2005 15:29:56	710003: UDP access denied by ACL from 10.1.1.5/138 to NP Identity Ifc:10.1.1.255	1
🖬 3	Mar 15 2005 15:29:56	710003: UDP access denied by ACL from 10.1.1.5/138 to NP Identity Ifc:10.1.1.255	<u> </u>
0 2	Mar 15 2005 15:29:45	106001: Inbound TCP connection denied from 209.165.200.226/23 to 209.165.200)
▲ 6	Mar 15 2005 15:29:21	606001: ASDM session number 0 from 10.1.1.5 started	
▲ 6	Mar 15 2005 15:29:21	605005: Login permitted from 10.1.1.5/3775 to inside:10.1.1.1/https for user "enab	1
▲ 6	Mar 15 2005 15:29:21	302013: Built inbound TCP connection 122 for inside:10.1.1.5/3775 (10.1.1.5/3775)
▲ 6	Mar 15 2005 15:29:21	302014: Teardown TCP connection 121 for inside:10.1.1.5/3774 to NP Identity Ifc:1	t I
▲ 6	Mar 15 2005 15:29:21	605005: Login permitted from 10.1.1.5/3774 to inside:10.1.1.1/https for user "enab	1
▲ 6	Mar 15 2005 15:29:21	302013: Built inbound TCP connection 121 for inside:10.1.1.5/3774 (10.1.1.5/3774)
▲ 6	Mar 15 2005 15:29:21	302014: Teardown TCP connection 120 for inside:10.1.1.5/3773 to NP Identity Ifc:1	t I
▲ 6	Mar 15 2005 15:29:21	605005: Login permitted from 10.1.1.5/3773 to inside:10.1.1.1/https for user "enab	I
▲ 6	Mar 15 2005 15:29:21	302013: Built inbound TCP connection 120 for inside:10.1.1.5/3773 (10.1.1.5/3773)
▲ 6	Mar 15 2005 15:29:21	606003: ASDM logging session number 0 from 10.1.1.5 started	
▲ 6	Mar 15 2005 15:29:21	605005: Login permitted from 10.1.1.5/3772 to inside:10.1.1.1/https for user "enab	1
▲ 6	Mar 15 2005 15:29:21	302013: Built inbound TCP connection 119 for inside:10.1.1.5/3772 (10.1.1.5/3772)
<u> </u>	Mar 15 2005 15:29:21	609001: Built local-host NP Identity Ifc:10.1.1.1	
<u>∔</u> 6	Mar 15 2005 15:29:21	609001: Built local-host inside:10.1.1.5	
▲ 6	Mar 15 2005 15:29:21	609002: Teardown local-host NP Identity Ifc:10.1.1.1 duration 0:00:00	
▲ 6	Mar 15 2005 15:29:21	609002: Teardown local-host inside:10.1.1.5 duration 0:00:00	
▲ 6	Mar 15 2005 15:29:21	302014: Teardown TCP connection 118 for inside:10.1.1.5/3771 to NP Identity Ifc:1	I I
▲ 6	Mar 15 2005 15:29:21	605005: Login permitted from 10.1.1.5/3771 to inside:10.1.1.1/https for user "enab	1
			Ě
			1
	Refresh Save	Log As Clear Close Help	

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

- PIX Security Appliance Technical Support and Documentation
- Cisco Adaptive Security Device Manager (ASDM) Troubleshoot and Alerts
- Requests for Comments (RFCs)
- Technical Support Cisco Systems

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 09, 2005

Document ID: 63880