# VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

### Document ID: 63882

Introduction Prerequisites Requirements Components Used Conventions Configure Network Diagram Configurations Configure the PIX Security Appliance Version 7.0 Use ASDM Verify Troubleshoot NetPro Discussion Forums – Featured Conversations Related Information

## Introduction

This document provides a sample configuration for a VPN/IPsec with Open Shortest Path First (OSPF) on Cisco PIX Security Appliance Software Version 7.0 or Cisco Adaptive Security Appliance (ASA).

PIX 7.0 allows OSPF unicast to run over an existing VPN connection. You no longer need to configure a Generic Routing Encapsulation (GRE) tunnel.

## Prerequisites

### **Requirements**

Before you attempt this configuration, ensure that you meet this requirement:

• You can establish the VPN connection.

### **Components Used**

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

- Cisco 3600 that runs Cisco IOS® Software Release 12.3
- Cisco 2600 that runs Cisco IOS Software Release 12.3
- PIX Security Appliance Software Version 7.0

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.

Cisco - VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

## 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:



## Configurations

This document uses these configurations:

- Router Rodney
- Router House

```
Router Rodney
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname rodney
memory-size iomem 15
ip subnet-zero
1
ip audit notify log
ip audit po max-events 100
1
interface Loopback1
ip address 22.22.22.22 255.255.255.0
1
interface Ethernet0/1
ip address 192.168.4.2 255.255.255.0
1
router ospf 22
log-adjacency-changes
```

```
network 22.22.22.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.4.1
no ip http server
!
line con 0
line aux 0
line vty 0 4
login
!
end!
End
```

#### **Router House** version 12.3 service timestamps debug uptime service timestamps log uptime no service password-encryption 1 hostname house 1 ip subnet-zero no ip domain-lookup interface Loopback1 ip address 11.11.11.11 255.255.255.0 1 interface FastEthernet0/1 ip address 192.168.3.2 255.255.255.0 router ospf 11 log-adjacency-changes network 11.11.11.0 0.0.0.255 area 0 network 192.168.3.0 0.0.0.255 area 0 ip classless ip route 0.0.0.0 0.0.0.0 192.168.3.1 ip http server 1 line con O line aux O line vty 0 4

### **Configure the PIX Security Appliance Version 7.0**

You can configure the PIX Security Appliance by either command–line interface (CLI) or GUI, with use of the Advanced Security Device Manager (ASDM). The configuration in this section is for the PIX "Lion". You configure the PIX "Tiger" in the same way. This document does not demonstrate the PIX Tiger configuration with the ASDM example. However, you can find CLI configurations for both in the Use ASDM section.

In order to configure the PIX Security Appliance version 7.0, console into the PIX. From a cleared configuration, use the interactive prompts in order to enable the ASDM GUI for the management of the PIX from workstation 10.1.1.5.

#### PIX/ASDM Bootstrap

Pre-configure Firewall now through interactive prompts [yes]? Firewall Mode [Routed]: Enable password [<use current password>]: cisco Allow password recovery [yes]? Clock (UTC): Year [2005]: Month [Aug]: Dav [6]: Time [06:00:44]: Inside IP address: 192.168.4.1 Inside network mask: 255.255.255.0 Host name: lion Domain name: cisco.com IP address of host running Device Manager: 192.168.4.50 The following configuration will be used: Enable password: cisco Allow password recovery: yes Clock (UTC): 06:00:44 Aug 6 2005 Firewall Mode: Routed Inside IP address: 192.168.4.1 Inside network mask: 255.255.255.0 Host name: lion Domain name: cisco.com IP address of host running Device Manager: 192.168.4.50 Use this configuration and write to flash? yes INFO: Security level for "inside" set to 100 by default. Cryptochecksum: 34f55366 a32e232d ebc32ac1 3bfa201a 969 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

### Use ASDM

Complete these steps in order to configure via the ASDM GUI:

1. From workstation 192.168.4.50, open a browser and use ADSM.

In this example, you use https://192.168.4.1.

- 2. Click **Yes** on the certificate prompts.
- 3. Log in with the enable password.

This login appears in the PIX/ASDM Bootstrap configuration.

4. At the prompt to use ASDM Launcher or ASDM as a Java App, make a selection.

Cisco – VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

This prompt appears only if this is the first time that you have run ASDM on the PC.

This example has selected and installed the ASDM Launcher.

5. Go to the ASDM Home screen and click the **Configuration** tab.

File Rules Search Options Tools Wizards Help	Refresh Save Hep
Device Information	Interface Status
General       License         Host Name:       lion.cisco.com         POK Version:       7.0(0)102       Device Uptime:       0d 0h 44m 43s         ASDM Version:       5.0(0)73       Device Type:       PDK 515E         Firewall Mode:       Routed       Context Mode:       Single         Total Flash:       16 MB       Total Memory:       64 MB         VPN Status       IIPSec Tunnels:       0       IPSec Tunnels:       0         CPU       CPU Usage (percent)       CPU       CPU Usage (percent)	Interface IP Address/Mask Line Link Current Kbps Inside 192.168.4.1/24 O up 0 up 18 Select an interface to view input and output Kbps Traffic Status Connections Per Second Usage
01     06       03     07 20 43       Memory     Memory Usage (MB)       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     07 20 43       04     04 20 43	UDP: TCP: Total:      UDP: TCP: Total:      Inside' Interface Traffic Usage (Kbpt)      12      1
Systog Disabled Device configuration loaded successfully.	<admin> NA (15) 🔐 🙆 3/18/05 1:20:43 AM UTC</admin>

6. In order to configure the outside interface, choose **Interface > Edit**.

File Roles 8	5.0 for PIX - 192.168.4.1 earch Options Tools Wizards	s Help						_[] ×
Home	Configuration Monitoring	Back Forwar	rd Search	Refresh	Save Help			Cisco Systems
Features	Configuration > Features > Inte	infaces	0.1					
Interfaces		a 105 <u>155</u> 165 1 4	3					
6.	Interface	Name Ena	abled Security Level	IP Address	Subnet Mask	Management Only	MTU	Add
Security Policy	Ethernet1	inside Y	es 10	0192.168.4.1	255.255.255.0	No	1500	Edit
23	Ethernet0	1	NO.			No		Delete
NAT								
VPN								
350								
Routing								
8								
Building Blocks								
Device								
Administration								
Properties	L.						•	
	Enable traffic between tw	vo or more interfac	es which are o	configured with sa	ime security levels			
			Apply	Re	eset			
Wizards /			7.	admina NA	45	A	ut out a	1-06-60 AM LITO

7. Click **OK** in the editing interface dialog box.

付 Warning	
	Editing interface Ethernet0 may cause temporary or permanent loss of connectivity.
	ок

8. Enter the interface details and click **OK** when complete.

Hardware Port:	Ethernet0	Configure Hardware Properties
Enable Interface	Dedicate this interface to manage	gement only
Interface Name:	outside	
Security Level:	0	
IP Address		
Use Static IP	C Obtain Address via DHCP	
IP Address:	10.64.10.6	
Subnet Mask:	255.255.255.0	
MTU:	1500	
Descriptions		
Jescription:		

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



10. In order to accept the interface configuration, click **Apply**.

File Rules St	0 for PIX - 192.168.4.1 arch Options Tools Wizard	s Help							
di Home	Configuration Monitoring	Back For	ward Se	Qearch	Refresh	Save Help			CISCO SYSTEMS
Features	Configuration > Features > Inb	enfaces biologic R. 27	149						
Interfaces	A 22 A IN LUIS -	~ 105 20 105	<u> </u>						
6	Interface	Name B	Enabled Le	ecurity evel	IP Address	Subnet Mask	Management Only	MTU	Add
Security Policy	Ethernet1	inside	Yes	1001	92.168.4.1	255.255.255.0	No	1500	Edit
NAT	Ethernet0	outside	Yes	01	0.64.10.6	255.255.255.0	No	1500	Delete
VPN									
Routing									
Building Blocks									
Administration									
Properties	4								
	Enable traffic between the	wo or more inter	rfaces which	h are co	nfigured with sa	me security levels			
Wizards /			A	4pply	Re	eset			
1	1			<a< td=""><td>dmin&gt; NA (</td><td>(15)</td><td>1 1 🔒 3</td><td>V18/05 1</td><td>1:30:13 AM UTC</td></a<>	dmin> NA (	(15)	1 1 🔒 3	V18/05 1	1:30:13 AM UTC

The configuration also gets pushed onto the PIX.

**Note:** This example uses static routes.

11. Choose **Features > Routing**, then choose **Static Route > Add**.

File Rules B	5.0 for PIX - 192.168.4.1 earch Options Tools Wizard	s Help	
Chine Home	Configuration Monitoring	Back Forward Search Refresh Save Help	CISCO SYSTEMS
Features	Configuration > Features > Re	uting > Routing > Static Route	
Interfaces Interfaces Security Policy NAT Security Policy NAT Security Policy Provide Administration Properties	Construction     C	Static Route Specify static routes.	Add Edit Delete
Wizards		Apply Reset	
1 THEOREM		admin> NA (15) 🛃 🔂 3/1	8/05 1:33:53 AM UTC

12. Configure the default gateway and click **OK**.

🚰 Add Static Route		×
Interface Name:	outside	<b>_</b>
IP Address:	0.0.0.0	
Mask:	0.0.0.0	•
Gateway IP:	10.64.10.15	j j
<ul> <li>Metric</li> </ul>	1	_
C Tunneled (Use	d only for default	route)
ок	Cancel	Help

13. In order to accept the interface configuration, click **Apply**.

Cisco ASDM 5.0	o for PIX - 192.168.4.1		
Home C	Configuration Monitoring	Back Forward Search Refresh Save Help	Cisco Systems
Features	Configuration > Features > R	uting > Routing > Static Route	
Interfaces Interfaces Security Policy NAT Security Policy	Routing Static Route RIP CProxy ARPs Soft Multicast Micoute	Static Route Specify static routes.	Add Edit Delete
Wizards 🗵		Apply Reset	
		admin> NA (15) 🔐 🔂 🔒 און 🔒 און	8/05 1:41:53 AM UTC

The configuration also gets pushed onto the PIX.

14. In order to use the VPN Wizard and create the LAN–to–LAN connection, choose Wizards > VPN Wizard....

File Rules S	5.0 for PIX - 192.168.4.1 earch Options Tools Wizard	Is Help	-					<u>_0×</u>
Home	Configuration Monitor	up Wizard Wizard	) Q ind Searc	h Refrest	h Save	? Help		CISCO STSTEMS
Features	Configuration > Features > Ro	outing > Routing >	Static Route					
Interfaces Interfaces Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy	Correction	Static Route Specify static r Interface outside	UP Address	Netmask 0.0.0	Oateway IP 10.64.10.15	Metric 1	Tunneled No	Add Edit Delete
Wizards /	1			App	ly	Reset		
1				<admin></admin>	NA (15)	<b>B B</b>	6 3/	21/05 6:36:42 AM UTC

15. In the VPN Wizard window, where Site-to-Site is the default selection, click Next.

💼 VPN Wizard		×
VPN Wizard	VPN Tunnel Type (Step 1 of)	
VPN Wizard	VPN Tunnel Type (Step 1 of)         Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.         This wizard creates basic tunnel configurations that you can edit later using the ASDM.         VPN Tunnel Type:         Site-to-Site         Image: Site-to-Site         VPN Tunnel Type:         Site-to-Site         Image: Site-to-Site         VPN Remote Access	
66	C Remote Access	
	VPN Tunnel Interface: outside	
	Back Next > Finish Cancel Help	

16. Add the Peer IP Address, Tunnel Group Name (which is the IP address), and Pre–Shared Key information, and click **Next**.

📸 VPN Wizard		×
VPN Wizard	Remote Site Peer (Step 2 of 7)	
Branch Branch ISP	Enter the IP address and the tunnel group of the peer device for this site-to-site tunnel. Then select the authentication method: a password shared by both sites or a certificate issued by a Certificate Authority.	
Home	Peer IP Address: 10.64.10.15	
Corporato	Tunnel Group Name: 10.64.10.15	
THE E	Authentication	
	Pre-shared Key     Pre-shared Key:     Cisco	
	C Certificate Certificate Signing Algorithm:	
	Trustpoint Name:	
	< Back Next > Finish Cancel Help	,

17. Add the Encryption type, Authentication type, and DH Group information, and click Next.

💼 VPN Wizard	×
VPN Wizard	IKE Policy (Step 3 of 7)
Brends	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.
Corporate Network	Encryption: DES
	Authentication: MD5
	DH Group:
	< Back Next > Finish Cancel Help

18. Add the IPsec parameters, Encryption type, and Authentication type information, and click Next.

💏 VPN Wizard	
VPN Wizard	IPSec Encryption and Authentication (Step 4 of 7)
Branch	Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.
Corporato Network	Encryption: DES
	Authentication: MD5
	< Back Next > Finish Cancel Help

19. Configure the inside host network.

In order to move the address to the Selected Host/Networks field within this window, click Add. When complete, click Next

📬 VPN Wizard		X
VPN Wizard	Local Hosts and Networks (Step 5 of 7)	
Branch Branch Branch	An IPSec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. You identify hosts and networks for the local site on this screen and for the remote site on the next screen.	
Home	Host/Network to Be Added Selected Hosts/Network	(S:
Corporato	Group     192.168.4.0/24	
THE THE	Interface: inside	
	IP address: 192.168.4.0 Delete	
	Mask: 255.255.255.0	
	< Back Next > Finish Cancel Hel	p

Cisco – VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

20. Configure the outside host network.

In order to move the address to the Selected Host/Networks field within this window, click **Add**. When complete, click **Next**.

📬 VPN Wizard	
VPN Wizard	Remote Hosts and Networks (Step 6 of 7)
Brandh Brandh	Enter the hosts and networks at the remote site of the IPSec connection.
Home	Host/Network to Be Added Selected Hosts/Networks:
Corporate Network	IP Address     C Name     C Group     192.168.3.0/24
THE IN	Interface: Outside
	IP address: 192.168.3.0 Delete
2 Taylull	Mask: 255.255.255.0
TTTTT	
C.P.	
	< Back Next > Finish Cancel Help

21. Review the Summary for accuracy, then click **Next**.



22. In order to verify the LAN–to–LAN tunnel configurations that the VPN Wizard created, choose **Configuration > VPN**.

File Roles 6	5.0 for PIX - 192.168.4.1 Search Options Tools Wizards	Help					
Home	Configuration Monitoring	Back Forward	Q Search R	efresh Save	? Help	C1	SCO SYSTEMS
Features	Consguration > Features > VFN	IPSec > Tunnel P Tunnel Policy Specify Tunnel Pol Interface Outside	olicy licy Type & Priority static - 20	Transform Set ESP-DES-MD5	Peer 10.64.10.15	Connection Ty Bidirections	Add
NAT	Address Manageme Pro-Fragmentation Address Manageme Assignment Pro-Fragmentation Pro-Fragment						Delete
Wizards /			App	ly I	Reset		
			<admir< td=""><td>&gt; NA (15)</td><td>😡 🍰 🔂</td><td>3/18/05 8:50</td><td>:53 AM UTC</td></admir<>	> NA (15)	😡 🍰 🔂	3/18/05 8:50	:53 AM UTC

23. Create an access list in order to allow OSPF traffic to go across the VPN.

This VPN access list is for the OSPF routes that are learned. Choose **Configuration > VPN**.

Cisco ASDM File Roles	5.0 for PIX - 192.168.4.1
Home	Configuration Monitoring Back Forward Search Refresh Save Help
Features	Configuration > Features > VPN > General > VPN System Options
Interfaces Security Policy NAT Security Policy	Image: Constraint of the second se
Wizards	
	<admin> NA (15) 😡 🛃 4/3/05 5:12:45 AM UT(</admin>

24. Choose **IPSec** > **IPSec Rules** > **Add**.



Cisco - VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

25. Add the OSPF neighbor (IP Address) data in this window and click **OK**.

Note: Be sure that you work on the outside interface.

Action	Tunnel Policy
	Policy: outside:static-20  New
Relect an action: Interct	
Select an action. Iprotect	Time Range
	Time Range: Not Applied 💌 New
Firewall Side Host/Network	Remote Side Host/Network
IP Address     C Name     C Group	IP Address     C Name     C Group
Interface: outside	Interface: outside
ID address	ID address: Loop to to to
IP address. 10.64.10.6	IP address. 10.64.10.15
Mask 255 255 255 255 💌	Mask: 255 255 255 255
any	outside
Protocol and Service	outside any
Protocol and Service	Manage Service Groups
Protocol and Service	Manage Service Oroups
Protocol and Service C TCP C UDP C ICMP © IP IP Protocol	outside any Manage Service Groups
Protocol and Service C TCP C UDP C ICMP C IP IP Protocol IP protocol: ospf	Anage Service Groups
Protocol and Service C TCP C UDP C ICMP © IP IP Protocol IP protocol: ospf	outside     any         Manage Bervice Groups
Protocol and Service C TCP C UDP C ICMP C IP IP Protocol IP protocol: ospf	outside     any       Manage Service Oroups
Protocol and Service C TCP C UDP C ICMP C IP IP Protocol IP protocol: ospf	Outside any Manage Service Oroups slation
Protocol and Service     C TCP C UDP C ICMP C IP     IP Protocol     IP protocol     IP protocol: ospf      Exempt PIX side host/network from address trans Please enter the description below (optional):	outside     any         Manage Service Oroups   Islation
arry     outside       Protocol and Service     C TCP       C TCP     UDP       IP Protocol       IP protocol:       IP protocol:	outside     any         Manage Service Oroups   slation
any     outside       Protocol and Service     C TCP       C TCP     C UDP       IP Protocol       IP protocol:       IP protocol:	outside any Manage Bervice Oroups slation
arry     outside       Protocol and Service     C TCP       C TCP     UDP       IP Protocol       IP protocol:       IP protocol:	outside     any         Manage Service Groups   slation

26. Verify that the information is correct and click **Apply**.

Home Cont Features Cont Features Cont Riterfaces	Montoring           Iniguration         Features > VPP           *         *         *           *         *         *         *           *         *         *         *         *           *         *         *         *         *         *           *         *         *         *         *         *         *         *           *         <	Back	Forward Forward IPSec Rule Es Rules menu	Search Retresh	Save Help	Cisco St	STEM 5
Features	onfiguration > Features > VPN	I > IPSec >	IPSec Rule S S les Rules menu	s			
Security Policy	Group Policy     Default Tunnel Gat     McE     Policies     Certificate Group M     PSec     PSe	# 1 2	Action protect protect	PtX Side HostNetwork ■9192.168.4.0/24 ■ outside/ 10.64.10.6	Remote Side HostiNetwork	elete rules.	d it ete
Wizards /				Apply	C Show Summary Reset	C Show Detail	

27. In order to verify the Network Address Translation (NAT) configurations that the VPN Wizard created, choose **Configuration > NAT > Translation Exemption Rules**.

File Rules Sea	for PIX - 192.168.4.1 rch Options Tools	Wizards Help				-02
Home Co	anfiguration Monitor	ring Back	Forward	Q Q Search Refresh S	ave Help	Cisco Systems
Features	Configuration > Featu	res > NAT > Tran	Islation Exemptio	on Rules		
	* * * 🖉 🚺	1 X 🗠 🖻	666			
Interfaces	Enable traffic th	rough the firewa	II without addres	s translation		
<u>6</u> ,	C Translation Ru	les 🕫	ranslation Exem	ption Rules		
Security Policy	Show Rules for In	terface: All Inter	fares	Show All		
25	Duta		1010-0-0		When Connecting To	Add
NAT	# Enabled	Action	Interface	Host/Network	Host/Network	
<b>S</b>	1 🗹	exempt	inside (outbound)	<b>1</b> 92.168.4.0/24	<b>192.168.3.0/24</b>	Edit
VPN			(			Delete
Routing						
Building Blocks						
3						
Device Administration						
Properties						
	• Static NAT	Dynamic	NAT 🎝 St	atic Policy NAT	mamic Policy NAT	Manage Pools
				Apply	Reset	
Wizards /						
				<admin> NA (1</admin>	15) 😡 🛃 🔂	3/18/05 8:57:33 AM UTC

28. Because this example uses NAT, uncheck the check box for Enable traffic through the firewall

#### without address translation, then click Add.

This step configures the NAT Rule.

File Rules	5.0 for PIX - 19. Bearch Option:	2.168.4.1 s Tools Wizard	is Help					
Home	Configuration	Monitoring	Back For	ward Search	Refresh	Save Help	C1	SCO SYSTEMS
Features	Configuratio	n > Features > N	AT > Translation	Rules				
	• <u>•</u> •			<b>S</b>				
Interfaces	☐ Enab	e traffic through t	he firewall withou	it address trans	lation			
<u> </u>	Trans	lation Rules	C Translat	ion Exemption F	Rules			
Security Policy	Show R	ules for Interface:	All Interfaces	*	Show All			
NAT						Options		Add
53		DNS Rewrite	Maximum TCP Connections	Embryonic Limit	Maximum UDP Connections	Randomize Sequence Number	Description	Edit
VPN								Delete
Routing								
88								
Building Blocks								
Device								
Properties	1							
	· Stat	IC NAT	Dynamic NAT	Static Pol	icy NAT	Dynamic Policy NAT	Manage Pools	
					Apply	Reset		
Wizards								
					<admin> NA</admin>	(15) 😡 🚑 🔂	3/18/05 9:0	23 AM UTC

29. Configure the Source Network.

Choose **any > Manage Pools** to define the NAT pool addresses.

Use NA	at <u>o</u> u	Jse Policy NAT					
Source H	ost/Network-						
		Interface:	inside		*		
		IP Address:	0.0.0.0		_		
		Mask:	0.0.0.0		-		
			10.0.0.0		<u> </u>		
			Browse				
							NAT Options
inslate Ad	ddress on Inte	erface: outsi	ide 💌 💌	1			
inslate A	ddress on Inte	erface: outs	ide 💌	]			
inslate A Translate	ddress on Inte Address To	erface: outs	ide 👱	]			
rranslate A Granslate	ddress on Inte Address To Static	erface: outs	ide 💌	]	<u>_</u>		
ranslate Ar Franslate	ddress on Inte Address To Static Redirect	IP Address:	ide 💌		<b>*</b>		
ranslate Ar Franslate C י	ddress on Inte Address To – Static Redirect © TCP © UDP	erface: outs IP Address: port Original port	ide 🔽	] Translater	• I port:		
inslate Ar Franslate C 11	ddress on Inte Address To – Static Redirect C TCP C UDP Dynamic	erface: outs IP Address: port Original port Address Pool:	ide 💌	Translated	Y port:	nage Pools	
inslate Ar Franslate Culu	ddress on Inte Address To- Static Redirect C TCP C UDP Dynamic Pool ID	erface: outs IP Address: port Original port Address Pool:	ide 💌	Translater ress 💌	F port Ma	nage Pools	
inslate Ar Franslate Culu	ddress on Inte Address To – Static Redirect C TCP C UDP Dynamic Dynamic	erface: outsi IP Address: port Original port Address Pool: No address po	ide	Translater ress 💌 Idress	T port:	nage Pools	
inslate Ar Franslate C 1	ddress on Inte Address To – Static Redirect C TCP C UDP Dynamic Pool ID N/A	erface: outs IP Address: port Original port Address Pool: No address po	ide Same add Ad pol defined	Translated ress 💌	f port:	nage Pools	
inslate Ar Franslate C 1	ddress on Inte Address To - Static Redirect TCP C UDP Dynamic Pool ID N/A	erface: outsi IP Address: port Original port Address Pool: No address po	ide	Translater ress 💌 Idress	r I port: [ Ma	nage Pools	

30. Select the **outside** interface and click **Add**.

anage Global Ad	Idress Pools		
lobal Address I	Pools		
lobal Address P Idresses.	ools are used to cor	nfigure Dynamic Network Addres	ss Translation (NAT)
Interface	Pool ID	IP Address(es)	
nside utside			Add
			Edit
			Delete
	OK		Unin 1
	UK	Cancer	Help

31. Because Port Address Translation (PAT) uses the IP address of the interface in this example, click the **Port Address Translation (PAT) using the IP address of the interface** radio button.

	Jourside	<u> </u>	Pool ID:	1	
C Range					
C Port Ad	dress Translatio	in (PAT)			
Port Ad	dress Translatio	in (PAT) using	the IP address	of the interface	
-					
10.44	dress:		— – <b>–</b>		
IP AC	All a second		(		
IP Ad					
Netwo	ork Mask (option	ral):			
Netw	vork Mask (option	ial):			

32. Click **OK** after configuration of the PAT pools.

obal Address P dresses.	ools are used to con	figure Dynamic Network Address T	ranslation (NAT)
Interface	Pool ID	IP Address(es)	
side utside	1 10.64.	10.6(interface PAT)	Add
			Edit
			Delete

33. In the Add Address Translation Rule window, select the Address Pool that the configured Source Network will use.

• USE NAT	C U	se Policy NAT					
Source Hos	st/Network						
		Interface:	inside		-		
		IP Address:	0.0.0				
		Mask:	0.0.0.0		-		
			Browse .				
							NAT Options
	tion of the second states	A	and the second se				
anslate Add	iress on Inte	rface: outsi	de 💌				
anslate Add Translate A	dress on Inte .ddress To	rface: outsi	ide 🗾				
anslate Add Translate A C ·	dress on Inte ddress To — Static T Redirect p	rface: outsi IP Address:	ide 👤	-	2		
anslate Add Translate A C 1	dress on Inte ddress To – Static Redirect p © TCP © UDP	rface: outsi IP Address: port Original port:	ide 💌	Translated	port.		
anslate Add Translate A C 1 I I C 1	ddress on Inte ddress To – Static Redirect p C TCP C UDP Dynamic	rface: outsi IP Address: port Original port: Address Pool:	ide 🔍	Translated	port: Mana	ige Pools	
anslate Add Translate A C III I C III	ddress on Inte ddress To	rface: outsi IP Address: port Original port: Address Pool:	ide 💌	Translated	port Mana	ige Pools	
anslate Add Translate A C 11	dress on Inte ddress To – Static Redirect p C TCP C UDP Dynamic Pool ID	rface: outsi IP Address: oort Original port: Address Pool: 10.64.10.6(inte	ide	Translated ess I	port. Mana	ige Pools	
anslate Add Translate A	dress on Inte ddress To – Static Redirect p C TCP C UDP Dynamic Pool ID	rface: outsi IP Address: oort Original port: Address Pool: 10.64.10.6(inte	ide	Translated ess I	port: Mana	ige Pools	

34. In this window, which shows the output from the NAT configuration, click **OK**:

• Use NA	T CL	Jse Policy NAT				
Source He	ost/Network-					
		Interface: IP Address:	inside 0.0.0.0		-	
		Mask:	0.0.0.0 Browse	]	<b>-</b>	
						NAT Options
anslate Ac	ddress on Inte	erface: outs	ide 💌			
Translate	Address To -					
Translate C	Address To – Static	IP Address:		¥	[	
Translate راب C	Address To- Static Redirect C TCP C UDP	IP Address: port Original port	Г : Г тг	💌	ort	_
Translate C با س	Address To- Static Redirect ( C TCP C UDP Dynamic	IP Address: port Original port Address Pool:	Tr	anslated p	ort: Manage f	Pools
Translate C +	Address To- Static Redirect C TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool:	Tr 1 Addre	anslated p	ort. Manage H	Pools
Translate	Address To- Static Redirect C TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 10.64.10.6(inte	Tr 1 Addre	ansläted p	ort <b> </b> Manage H	Pools
Translate ۲۰۱۰	Address To- Static Redirect TCP UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 10.64.10.6(inte	Tr 1 Addre	anslated p ss	ort Manage H	Pools

35. Click **Apply** in order to save the configuration.

Cisco ASDM 5.0 File Rules Sea	for PIX - 192. rch Options	.168.4.1 Tools Wizar	ds Help				_10);
Home Co	onfiguration	Monitoring	Back Forward	Q Q Search Refresh	Save Help		Cisco Systems
Features	Configuration	> Features > N	AT > Translation Rules				
Interfaces		e traffic through ation Rules les for Interface	Re Re Re Re Paralel      Translation Exemp     All Interfaces	translation ation Rules			
1 AL	Rule		Original		1	Translated	Add
3	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
Routing Building Blocks Device Administration Properties	• •]• Static	NAT I	Dynamic NAT 🔒 Stat	ic Policy NAT	Dynamic Policy N	AT Manage Pools.	
Wizards /				- thirt	Nesei	1	
evice configuration	on loaded suc	cessfully.		<admin> N</admin>	A (15)	🗿 🛛 🔒 3/20/05	7:43:19 AM U

36. In order to set up OSPF on the PIX, choose **Configuration** > **Routing** > **OSPF** > **Setup** > **Process Instances**, then check **Enable this OSPF Process**.

Cisco ASDM 5	.0 for PIX - 192.168.4.1		
File Rules Se	arch Options Tools Wizards I	Help Q Q Q Q ack Forward Search Refresh Save Help	Cesco Systems
Features	Consiguration > Features > Routin  Consiguration > Features > Routin  Consiguration  Reveal a static Route  Reveal a static Reighbor  Static Reighbor  Static Reighbor  Static Reighbor  Static Reighbor  Multicast  Multic	9 > Routing > OSPF > Setup         Image: I	e an OSPF
Configuration cha	inges saved successfully.	<admin> NA (15) 🔯 🎰 🔂 🔒</admin>	3/28/05 9:26:57 AM UTC

37. Choose Area/Networks and click Add.



38. Enter the IP Address and Netmask of one network in the OSPF process field and click OK.

USPF Process:	100 -	·	Area ID: 0				
Area Type							
Normal							
C Stub	🔽 Summary (allows sending LSAs into the stub area)						
C NSSA	Redistribute (imports routes to normal and NSSA areas)						
	🔽 Summary (allows sending LSAs into the NSSA area)						
	🗖 Default In	formation Origina	te (generate a Type	7 default)			
	Metric	Value 1	Metric Type: 2	Ŧ			
– Area Networks							
Area Networks Enter IP Addr IP Address: Netmask:	ess and Mask	Add >> Delete	IP Address 192.168.4.0	Netmask 255.255.255.0			

39. Verify that the information is correct and click **Edit**.



40. Enter the IP Address and Netmask of the second network in the OSPF process field and click OK.

OSPF Process:	100 💌	I	Area ID: 🛛				
Area Type							
Normal							
C Stub	Summary (allows sending LSAs into the stub area)						
C NSSA	SA Redistribute (imports routes to normal and NSSA areas)						
	☑ Summary (allows sending LSAs into the NSSA area)						
	🗖 Default Info	- ormation Originat	e (generate a Type	7 default)			
		지 않는 것은 것이 많은 것이 같아졌다. 것이 없다.	and Brown and the states of the set				
– Area Networks –	Metric \	Value 1	Metric Type: 2				
– Area Networks – – Enter IP Addre IP Address:	Metric \ ss and Mask	Value 1 Add >>	Metric Type: 2 IP Address 192.168.4.0 10.64.10.0	Netmask 255.255.255.0 255.255.255.225			
– Area Networks – – Enter IP Addre IP Address: – Netmask: –	Metric V ess and Mask	Add >> Delete	Metric Type: 2 IP Address 192.168.4.0 10.64.10.0	Netmask 255.255.255.0 255.255.255.22			
Area Networks – Enter IP Addre IP Address: Netmask:	Metric V	Add >> Delete	Metric Type: 2	Netmask 255.255.255.0 255.255.255.22			

41. Verify that the information is correct and click **Apply**.

When the law the second states the second states
File Rules Search Options Tools Witzards Help
Home Configuration Monitoring Back Forward Search Refresh Save Help Clisco Systems
Features Configuration > Features > Routing > OSPF > Setup
Werkfaces   Werkfaces   Werkfaces   Werkfaces   With all Link   With all Li
Configuration changes saved successfully. <a href="https://www.admin">admin</a> NA (15) 🔯 🙀 🔂 3/28/05 9:32:47 AM UTC

42. Choose **OSPF > Interface > Properties > Outside** and click **Edit**.

🛍 Cisco ASDM	5.0 for PIX - 192.168.4.1		
File Rules S	earch Options Tools Wizards	: Help	
G Home	Configuration Montoring	Back Forward Search Refresh Save Help	Cisco Systems
Features	Configuration > Features > Ro	iting > Routing > OSPF > Interface	
Interfaces Security Policy NAT Security Policy Security Policy NAT Security Policy NAT Security Policy Policy Security Policy Security Policy Security Policy Policy Security Security Policy Security Security Policy Security Se	Cospective     C	Interface Configure Interface specific OSPF routing parameters. Authentication Properties Specify the OSPF routing properties for each interface Interface Broadcast Cost Prority MTU Ignore Database Filter inside yes 1 No No outside yes 1 No No	Edit
Configuration ct	anges saved successfully.	<admin> NA (15) 局 婦 局   合 3/28/0</admin>	5 9:33:47 AM UTC
o on anglor on on the	anges sares saccessiony.		10.00.41 Pm 010

43. Uncheck the **Broadcast** check box on the outside interface.

Note: This *must* be unicast.

🕵 Edit OSPF I	nterface Proper	ties		
Interface:	outside			I▼ (Broadcast
Cost:			Priority:	1
MTU Igr MTU mi receivin	nore (disable OSPI smatch detection ( g DBD packets)	F Database Fi on I outgoing LS/ OSPF interfa	lter (filter As to an ice)	Advanced
	ок	Cancel	Help	

44. Check the Broadcast column for the outside interface in order to verify that the selection is **no**, then click **Apply**.

Cisco ASDM	5.0 for PIX - 192.168.4.1		
File Rules St	earch Options Tools Wizard	Help	
G Home	Configuration Monitoring	Back Forward Search Refresh Save Help	CISCO SYSTEMS
Features	Configuration > Features > Ro	ting > Routing > OSPF > Interface	
Interfaces Security Policy NAT WPN Building Blocks Device Administration Properties	Comparison     C	Interface Configure Interface specific OSPF routing parameters. Authentication Properties Specify the OSPF routing properties for each interface Interface Broadcast Cost Prority MTU Ignore Database Filter inside yes 1 No No	Edit
Wizards /			
Configuration ch	anges saved successfully.	<admin> NA (15) 🔯 🚮 🔂 3/2</admin>	8/05 9:40:17 AM UTC

45. Choose **OSPF > Static Neighbor** and click **Add**.

Cisco ASDM	5.0 for PIX - 192.168.4.1					
File Rules Se	arch Options Tools Wizards	s Help				
Home C	Configuration Montoring	Back	Forward Search	Refresh Save	<b>?</b> Help	CISCO SYSTEMS
Features	Configuration > Features > Ro	uting > Ro	uting > OSPF > Static	Neighbor.		
-	◆ 生 平   ■   前   次 ◎	6 <b>6</b> 💁	ŝ 😂			
Interfaces	E-*ARouting **Static Route -*ARIP	Static Ne De	ighbor	in the point-to-point non-bro	adcast interface. A static ro	ute must be
Security Policy	D- COSPF	cre	ated to reach the stati	cally defined neighbor.		-
200	- Setup		OSPF Process	Neighbor	Interface	Add
NAT	- 12 Interface					Edit
<u> 7</u>	- Virtual Link					
VPN	- Elitering					Delete
430	Summary Addr					
Routing	🖻 🏰 Multicast					
	E B IGMP					
Building Blocks	MRoute					
.8						
Device						
Administration						
E-o			<b>a</b> 1			
Properties						
				Apply	Reset	
Wizards 🗵	•					
Configuration cha	anges saved successfully.			<admin> NA (15)</admin>	🗟 🍰 🔂 🔢 🔂 3	28/05 9:42:17 AM UTC

46. Enter the Neighbor IP address in the field for the outside interface and click **OK**.

🖆 Add Ospf Ne	ighbor Entr	у			
OSPF Proces	s: 100	•			
Neighbor :	10.64.10.	15	Interface :	outside	•
	ок	Can	cel	Help	

47. Verify that the information is correct and click **Apply**.

This action completes the configuration.

Cisco ASDM	5.0 for PIX - 192.168.4.1						
File Rules S Home	Configuration Monitoring	Help Back	Forward Search	Refresh Sa	we Help		Cisco Systems
Features	Configuration > Features > Rou	iling > Roi	iting > OSPF > Static I	Neighbor.			
Interfaces	Routing     State Route     RuP     Provy ARPs     Soper	Static Ne	ighbor ine static neighbors o ated to reach the stati	n the point-to-point r sally defined neighbo	non-broadcast i or.	nterface. A static ro	ute must be
245	-*aSetup	[	OSPF Process	Neighbor		Interface	Add
NAT	Static Neighbor     Static Neighbor     Static Neighbor     Summary Addr      S		100	10.04.10.10		Upitade	Delete
Wizards -	hanges saved successfully.			Apply <admin> NA (1</admin>	Rese	t	128/05 9:45:17 AM UTC

In order to view the CLI configuration, choose **File > Show Running Configuration in New Window**.

🔓 Cis	co ASDI	M 5.0 for	PIX - 192.	168.4.1		
File	Rules	Search	Options	Tools	Wizards	Help
Ref	resh AS	DM with t	he Runnir	ig Confi	guration or	n the Device
Res	set Devi	ce to the I	Factory De	fault Co	nfiguration	i
Sho	w Runr	ning Conf	iguration i	n New V	Vindow	
Sav	e Runn	ing Confi	guration to	Flash		
Sav	e Runn	ing Config	guration to	TFTP S	erver	
Sav	e Runn	ing Config	guration to	Standb	y Unit	
Sav	e Intern	al Log Bu	iffer to Fla	sh		
Prir	ıt					
Cle	ar ASDI	VI Cache				
Cle	ar Interr	hal Log Bi	uffer			
Exit						

PIX Lion PIX Version 7.0 interface Ethernet0 nameif outside security-level 0 ip address 10.64.10.6 255.255.0

Cisco - VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

```
ospf network point-to-point non-broadcast
interface Ethernet1
nameif inside
security-level 100
ip address 192.168.4.1 255.255.255.0
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Lion
domain-name cisco.com
ftp mode passive
!--- This traffic is from networks.
access-list inside_nat0_outbound extended permit ip 192.168.4.0 255.255.255.0
   192.168.3.0 255.255.255.0
access-list outside_cryptomap_20 extended permit ip 192.168.4.0 255.255.255.0
   192.168.3.0 255.255.255.0
access-list outside_cryptomap_20 extended permit ospf interface outside host 10.64.10.15
pager lines 24
logging enable
logging buffered informational
no logging message 713906
no logging message 715075
no logging message 715036
no logging message 715005
mtu outside 1500
mtu inside 1500
no failover
monitor-interface outside
monitor-interface inside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
!--- Do not translate traffic with NAT.
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
!--- This is OSPF.
router ospf 100
network 10.64.10.0 255.255.255.224 area 0
network 192.168.4.0 255.255.255.0 area 0
area O
neighbor 10.64.10.15 interface outside
log-adj-changes
route outside 0.0.0.0 0.0.0.0 10.64.10.15 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 192.168.4.50 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
```

!--- This is the IPsec configuration.

```
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 10.64.10.15
crypto map outside_map 20 set transform-set ESP-DES-MD5
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
tunnel-group 10.64.10.15 type ipsec-121
tunnel-group 10.64.10.15 ipsec-attributes
pre-shared-key *
class-map inspection_default
match default-inspection-traffic
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
1
service-policy asa_global_fw_policy global
Cryptochecksum: 3d5f16a67ec0fa20aa3882acaa348e28
: end
```

#### **PIX Tiger**

```
PIX Version 7.0
```

```
interface Ethernet0
nameif outside
security-level 0
ip address 10.64.10.15 255.255.255.0
```

```
interface Ethernet1
nameif inside
security-level 100
ip address 192.168.3.1 255.255.255.0
```

Cisco – VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

enable password 2KFQnbNIdI.2KYOU encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname tiger domain-name cisco.com ftp mode passive access-list inside\_nat0\_outbound extended permit ip 192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0 access-list outside\_cryptomap\_20 extended permit ip 192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0 pager lines 24 logging enable 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 global (outside) 1 interface !--- Do not translate traffic with NAT. nat (inside) 0 access-list inside\_nat0\_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 10.64.10.6 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 192.168.3.50 255.255.255.255 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp !--- This is the IPsec configuration. crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac crypto map outside\_map 20 match address outside\_cryptomap\_20 crypto map outside\_map 20 set peer 10.64.10.6 crypto map outside\_map 20 set transform-set ESP-DES-MD5 crypto map outside\_map interface outside isakmp enable outside isakmp policy 10 authentication pre-share isakmp policy 10 encryption des isakmp policy 10 hash md5 isakmp policy 10 group 1 isakmp policy 10 lifetime 86400 isakmp policy 65535 authentication pre-share isakmp policy 65535 encryption 3des isakmp policy 65535 hash sha isakmp policy 65535 group 2 isakmp policy 65535 lifetime 86400 telnet timeout 5 ssh timeout 5 console timeout 0 tunnel-group 10.64.10.6 type ipsec-121

Cisco – VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

```
tunnel-group 10.64.10.6 ipsec-attributes
pre-shared-key *
class-map inspection_default
match default-inspection-traffic
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_qlobal_fw_policy qlobal
Cryptochecksum: 5e99bf942a67f20dad116c7d99011315
: end
```

## Verify

This section provides information you can use to confirm that your configuration works properly.

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

- **logging buffer debugging** Shows the establishment of connections and denial of connections to hosts that go through the PIX. The PIX log buffer stores the information. You can see the output if you use the **show log** command.
- You can use ASDM in order to enable logging and to view the logs:
  - show crypto isakmp sa Shows the Internet Security Association and Key Management Protocol (ISAKMP) security association (SA) that is built between peers.

```
lion# show crypto isakmp sa
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 10.64.10.15
Type : L2L Role : responder
Rekey : no State : MM_ACTIVE
tiger# show crypto isa sa
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 10.64.10.6
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

show crypto ipsec sa Shows each Phase 2 SA that is built and the amount of traffic that is sent.

lion# show crypto ipsec sa interface: outside Crypto map tag: outside\_map, local addr: 10.64.10.6 local ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0) current\_peer: 10.64.10.15 #pkts encaps: 81, #pkts encrypt: 81, #pkts digest: 81 #pkts decaps: 81, #pkts decrypt: 81, #pkts verify: 81 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 81, #pkts comp failed: 0, #pkts decomp failed: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 10.64.10.6, remote crypto endpt.: 10.64.10.15 path mtu 1500, ipsec overhead 60, media mtu 1500 current outbound spi: 07DB50AF inbound esp sas: spi: 0x75E2D691 (1977800337) transform: esp-des esp-md5-hmac in use settings ={L2L, Tunnel, } slot: 0, conn\_id: 1, crypto-map: outside\_map sa timing: remaining key lifetime (kB/sec): (3824991/28084) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0x07DB50AF (131813551) transform: esp-des esp-md5-hmac in use settings ={L2L, Tunnel, } slot: 0, conn\_id: 1, crypto-map: outside\_map sa timing: remaining key lifetime (kB/sec): (3824992/28082) IV size: 8 bytes replay detection support: Y tiger# show crypto ipsec sa interface: outside Crypto map tag: outside\_map, local addr: 10.64.10.15 local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0) current\_peer: 10.64.10.6 #pkts encaps: 83, #pkts encrypt: 83, #pkts digest: 83 #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 83, #pkts comp failed: 0, #pkts decomp failed: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 10.64.10.15, remote crypto endpt.: 10.64.10.6 path mtu 1500, ipsec overhead 60, media mtu 1500 current outbound spi: 75E2D691 inbound esp sas: spi: 0x07DB50AF (131813551) transform: esp-des esp-md5-hmac in use settings ={L2L, Tunnel, } slot: 0, conn\_id: 1, crypto-map: outside\_map sa timing: remaining key lifetime (kB/sec): (4274992/28062)

```
IV size: 8 bytes
        replay detection support: Y
        outbound esp sas:
        spi: 0x75E2D691 (1977800337)
        transform: esp-des esp-md5-hmac
        in use settings ={L2L, Tunnel, }
        slot: 0, conn_id: 1, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4274991/28062)
        IV size: 8 bytes
        replay detection support: Y
• show debug Displays the debug output.
        lion(config)# show debug
        debug crypto ipsec enabled at level 1
        debug crypto engine enabled at level 1
        debug crypto isakmp enabled at level 1
        %PIX-6-609001: Built local-host outside:10.64.10.15
        %PIX-6-609001: Built local-host NPMar 20 09:26:11 [IKEv1] Id:
           QM IsRekeyed old sa not found by addr
        entity Ifc:10.64.10.6
        %PIX-6-302015: Built inbound UDP connection 133 for outside:10.64.10.15/500
           (10.64.10.15/500) to NP Identity Ifc:10.64.10.6/500 (10.64.10.6/500)
        %PIX-7-715005: Group = , IP = 10.64.10.15 , processing SA payload
        PIX-7-715005: Group = , IP = 10.64.10.15 , Oakley proposal is acceptable
        %PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
        %PIX-7-715049: Group = , IP = 10.64.10.15 Received Fragmentation VID,
        *PIX-7-715064: Group = , IP = 10.64.10.15 IKE Peer included IKE
           fragmentation capability flags: Main Mode: True Aggressive Mode: True,
        %PIX-7-715005: Group = , IP = 10.64.10.15 , processing IKE SA
        %PIX-7-715028: Group = , IP = 10.64.10.15 IKE SA Proposal # 1,
           Transform # 1 acceptable Matches global IKE entry # 3,
        *PIX-7-715005: Group = , IP = 10.64.10.15 , constructing ISA_SA for isakmp
        %PIX-7-715046: Group = , IP = 10.64.10.15 constructing Fragmentation
           VID + extended capabilities payload,
        %PIX-7-713906: IP = 10.64.10.15 , IKE DECODE SENDING Message (msgid=0)
           with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 108
        %PIX-7-713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message (msgid=0)
           with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
           + VENDOR (13) + VENDOR (13) + NONE (0) total length : 224
        %PIX-7-715005: Group = , IP = 10.64.10.15 , processing ke payload
        %PIX-7-715005: Group = , IP = 10.64.10.15 , processing ISA_KE
        %PIX-7-715001: Group = , IP = 10.64.10.15 processing nonce payload,
        %PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
        %PIX-7-715049: Group = , IP = 10.64.10.15 Received Cisco Unity client VID,
        %PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
        %PIX-7-715049: Group = , IP = 10.64.10.15 Received xauth V6 VID,
        %PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
        %PIX-7-715038: Group = , IP = 10.64.10.15 Processing VPN3000/ASA
           spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001),
        %PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
        %PIX-7-715049: Group = , IP = 10.64.10.15 Received Altiga/Cisco VPN3000/
           Cisco ASA GW VID,
        %PIX-7-715005: Group = , IP = 10.64.10.15 , constructing ke payload
        %PIX-7-715001: Group = , IP = 10.64.10.15 constructing nonce payload,
        *PIX-7-715046: Group = , IP = 10.64.10.15 constructing Cisco Unity VID
           payload,
        %PIX-7-715046: Group = , IP = 10.64.10.15 constructing xauth V6 VID
           payload,
        %PIX-7-715048: Group = , IP = 10.64.10.15 Send IOS VID,
        %PIX-7-715038: Group = , IP = 10.64.10.15 Constructing ASA spoofing IOS
           Vendor ID payload (version: 1.0.0, capabilities: 20000001),
        %PIX-7-715046: Group = , IP = 10.64.10.15 constructing VID payload,
        %PIX-7-715048: Group = , IP = 10.64.10.15 Send Altiga/Cisco VPN3000/Cisco
```

```
ASA GW VID,
PIX-7-713906: IP = 10.64.10.15 , Connection landed on tunnel_group
  10.64.10.15
%PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , Generating keys
  for Responder...
%PIX-7-713906: IP = 10.64.10.15 , IKE DECODE SENDING Message (msgid=0)
  with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
   + VENDOR (13) + VENDOR (13) + NONE (0) total length : 224
%PIX-7-713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message (msgid=0)
  with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) +
  VENDOR (13) + NONE (0) total length : 103
*PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 Processing ID,
PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15, processing hash
%PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , computing hash
%PIX-7-715034: IP = 10.64.10.15 Processing IOS keep alive payload:
  proposal=32767/32767 sec.,
%PIX-7-715047: Group = 10.64.10.15, IP = 10.64.10.15 processing VID
   payload,
%PIX-7-715049: Group = 10.64.10.15, IP = 10.64.10.15 Received DPD VID,
%PIX-7-713906: IP = 10.64.10.15 , Connection landed on tunnel_group
   10.64.10.15
*PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 constructing ID,
%PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , construct hash
  pavload
%PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , computing hash
%PIX-7-715034: IP = 10.64.10.15 Constructing IOS keep alive payload:
  proposal=32767/32767 sec.,
*PIX-7-715046: Group = 10.64.10.15, IP = 10.64.10.15 constructing dpd
  vid payload,
%PIX-7-713906: IP = 10.64.10.15 , IKE DECODE SENDING Message (msgid=0)
  with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14)
   + VENDOR (13) + NONE (0) total length : 102
%PIX-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for
  user = 10.64.10.15
%PIX-3-713119: Group = 10.64.10.15, IP = 10.64.10.15 PHASE 1 COMPLETED,
%PIX-7-713121: IP = 10.64.10.15 Keep-alive type for this connection: DPD,
%PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , Starting phase 1
  rekey timer:
  73440000 (ms)
*PIX-7-714003: IP = 10.64.10.15 IKE Responder starting QM: msg id =
   6a9f3592,
%PIX-7-713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message (msgid=
   6a9f3592) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5)
   + ID (5) + NOTIFY (11) + NONE (0) total length : 192
%PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , processing hash
%PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , processing SA
  payload
%PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 processing nonce
  payload,
%PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 Processing ID,
%PIX-7-7140111D_IPV4_ADDR_SUBNET ID received--192.168.3.0--255.255.255.0,
%PIX-7-713035: Group = 10.64.10.15, IP = 10.64.10.15 Received remote IP
   Proxy Subnet data in ID Payload: Address 192.168.3.0, Mask
   255.255.255.0, Protocol 0, Port 0,
*PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 Processing ID,
%PIX-7-7140111D_IPV4_ADDR_SUBNET ID received--192.168.4.0--255.255.255.0,
%PIX-7-713034: Group = 10.64.10.15, IP = 10.64.10.15 Received local IP
  Proxy Subnet data in ID Payload: Address 192.168.4.0, Mask s,
  Protocol 25585052, Port 0,
*PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , Processing Notify
  payload
%PIX-5-713904: QM IsRekeyed old sa not found by addr
%PIX-7-713221: Group = 10.64.10.15, IP = 10.64.10.15 Static Crypto Map
   check, checking map = outside_map, seq = 20...,
```

%PIX-7-713225: Group = 10.64.10.15, IP = 10.64.10.15 Static Crypto Map check, map outside\_map, seq = 20 is a successful match, %PIX-7-713066: Group = 10.64.10.15, IP = 10.64.10.15 IKE Remote Peer configured for SA: outside\_map, %PIX-7-713906: Group = 10.64.10.15, IP = 10.64.10.15 , processing IPSEC SA %PIX-7-715027: Group = 10.64.10.15, IP = 10.64.10.15 IPSec SA Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20, \*PIX-7-713906: Group = 10.64.10.15, IP = 10.64.10.15, IKE: requesting SPI! %PIX-7-713906: Received unexpected event EV\_ACTIVATE\_NEW\_SA in state MM ACTIVE %PIX-7-715006IKE got SPI from key engine: SPI = 0xcb804517, %PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , oakley constucting quick mode %PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , constructing blank hash %PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , constructing ISA\_SA for ipsec \*PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 constructing ipsec nonce payload, %PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 constructing proxy ID, %PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , Transmitting Proxy Id: Remote subnet: 192.168.3.0 Mask 255.255.255.0 Protocol 0 Port 0 Local subnet: 192.168.4.0 mask 255.255.255.0 Protocol 0 Port 0 %PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , constructing qm hash %PIX-7-714005IKE Responder sending 2nd QM pkt: msg id = 6a9f3592, PIX-7-713906: IP = 10.64.10.15 , IKE DECODE SENDING Message (msgid=6a9f3592) with payloads : HDR + HASH (8) + SA (1) + NONCE (10)+ ID (5) + ID (5) + NONE (0) total length : 164 %PIX-7-713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message (msgid=6a9f3592) with payloads : HDR + HASH (8) + NONE (0) total length : 48 %PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , processing hash %PIX-7-715005: Group = 10.64.10.15, IP = 10.64.10.15 , loading all IPSEC SAs %PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 Generating Quick Mode Key!, %PIX-7-715001: Group = 10.64.10.15, IP = 10.64.10.15 Generating Quick Mode Key!, %PIX-5-713049: Group = 10.64.10.15, IP = 10.64.10.15 Security negotiation complete for LAN-to-LAN Group (10.64.10.15) Responder, Inbound SPI = 0xcb804517, Outbound SPI = 0x6935flee, %PIX-7-715007IKE got a KEY\_ADD msg for SA: SPI = 0x6935flee, %PIX-7-715005: pitcher: rcv KEY\_UPDATE, spi 0xcb804517 %PIX-6-713905: Group = 10.64.10.15, IP = 10.64.10.15 , PHASE 2 COMPLETED (msqid=6a9f3592)%PIX-6-609001: Built local-host inside:192.168.4.2 %PIX-6-609001: Built local-host outside:192.168.3.2

• Verify that the LAN–to–LAN connection passes routing traffic:

• **show ip route** Displays IP routing table entries.

rodney# show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, \* - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route Gateway of last resort is 192.168.4.1 to network 0.0.0.0 1.0.0.0/24 is subnetted, 1 subnets C 1.1.1.0 is directly connected, Tunnel0 20.0.0.0/24 is subnetted, 1 subnets C 20.20.20.0 is directly connected, Loopback0 22.0.0.0/24 is subnetted, 1 subnets C 22.22.22.0 is directly connected, Loopback1 C 192.168.4.0/24 is directly connected, Ethernet0/1 10.0.0.0/24 is subnetted, 1 subnets S 10.10.10.0 is directly connected, Tunnel0 11.0.0.0/32 is subnetted, 1 subnets O 11.11.11.11 [110/11112] via 1.1.1.1, 00:13:34, Tunnel0 S\* 0.0.0.0/0 [1/0] via 192.168.4.1

rodney# ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

house# show ip route Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area \* - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route

Gateway of last resort is 192.168.3.1 to network 0.0.0.0

1.0.0.0/24 is subnetted, 1 subnets C 1.1.1.0 is directly connected, Tunnel0 20.0.0.0/24 is subnetted, 1 subnets S 20.20.20.0 is directly connected, Tunnel0 22.0.0.0/32 is subnetted, 1 subnets O 22.22.22.22 [110/11112] via 1.1.1.2, 00:14:29, Tunnel0 10.0.0.0/24 is subnetted, 1 subnets C 10.10.10.0 is directly connected, Loopback0 11.0.0.0/24 is subnetted, 1 subnets C 11.11.11.0 is directly connected, Loopback1 C 192.168.253.0/24 is directly connected, FastEthernet0/0 C 192.168.3.0/24 is directly connected, FastEthernet0/1 S\* 0.0.0.0/0 [1/0] via 192.168.3.1

house# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

Complete these steps in order to view the logs:

1. Choose Configuration > Properties > Logging > Logging Setup, check Enable logging, and click Apply.

Cisco ASDM S File Rules Bi	.0 for PIX - 192.168.4.1 earch Options Tools Wizard	ts Help	
Home	Configuration Monitoring	Back Forward Search Refresh Save Help	CISCO SYSTEMS
Features	Configuration > Features > Pr	aperties > Logging > Logging Setup	
Interfaces Security Policy NAT Security Policy NAT WPN Security Routing Building Bocks Device Administration	AAA Setup AAA Setup AAA Server Grou AAA Servers Auth. Prompt Advanced Auto Spoofing Art Spoofing Art Spoofing Art Static Table Auto Update DHCP Server DHCP Server DHCP Relay DHCP RELAY DH	Logging Setup Enable logging Enable logging Enable logging on the failows Send debug messages as syslogs Send syslogs in EMBLEM for Logging to Internal Buffer Specify the size of the internal buffer to which syslogs will be saved. When the buffer overwritten. Buffer Size: 4096 bytes You can choose to save the buffer contents before the buffer is overwritten. Save Buffer To: FTP Server Configure FTP Settings Flash Configure FIAsh Usage ASDM Logging Specify the size of the queue for syslogs intended for viewing in ASDM. Queue Size: 100 Apply Reset	er standby unit rmat fler fills up, it will
Wizards /			
		<admin> NA (15) 🔯 🛃 🔂 30</admin>	20/05 8:00:19 AM UTC

2. Choose **Monitoring > Logging > Log Buffer > Logging Level**, select **Logging Buffer** from the drop–down menu, and click **View**.

Cisco ASDM 5.0 File Rules Sea	) for PIX - 192.168.4.1 arch Options Tools Wizard	s Help
Gi Home	Configuration Monitoring	Back Forward Search Refresh Save Help
Features	Monitoring > Features > Loggi	ng > Log Buffer Log Buffer
Interfaces		
VPN		Click the View button below to display syslog messages in the logging butter for ASDM as of now. Select the desired logging level to see messages at that severity or higher.
Routing		Logging Level: Debugging
Administration		
Connection Graphs		
Logging		View
IP Audit		
Configuration sha		Leadmins INF (15) IRL SIG

Here is an example of the Log Buffer:

Find text	in messages below:	Find Next		
Severity	Time			
07	Mar 20 2005 09:42:18	715007IKE got a KEY_ADD msg for SA: SPI = 0xb9b5cc02,		
D 7	Mar 20 2005 09:42:18	713906: IP = 10.64.10.15, IKE DECODE SENDING Message (msgid=fb7d1b90) wi		
0 7	Mar 20 2005 09:42:18	714006IKE Initiator sending 3rd QM pkt: msg id = fb7d1b90,		
07	Mar 20 2005 09:42:18	715005: Group = 10.64.10.15, IP = 10.64.10.15, oakley constructing final quick mod		
<u>R</u> 5	Mar 20 2005 09:42:18	713049: Group = 10.64.10.15, IP = 10.64.10.15 Security negotiation complete for LA		
07	Mar 20 2005 09:42:18	715001: Group = 10.64.10.15, IP = 10.64.10.15 Generating Quick Mode Keyl,		
D 7	Mar 20 2005 09:42:18	715001: Group = 10.64.10.15, IP = 10.64.10.15 Generating Quick Mode Keyl,		
P 7	Mar 20 2005 09:42:18	715005: Group = 10.64.10.15, IP = 10.64.10.15, loading all IPSEC SAs		
0 7	Mar 20 2005 09:42:18	714011ID_IPV4_ADDR_SUBNET ID received192.168.3.0255.255.255.0,		
D 7	Mar 20 2005 09:42:18	715001: Group = 10.64.10.15, IP = 10.64.10.15 Processing ID,		
0 7	Mar 20 2005 09:42:18	714011ID_IPV4_ADDR_SUBNET ID received192.168.4.0255.255.255.0,		
0 7	Mar 20 2005 09:42:18	715001: Group = 10.64.10.15, IP = 10.64.10.15 Processing ID,		
D 7	Mar 20 2005 09:42:18	715001: Group = 10.64.10.15, IP = 10.64.10.15 processing nonce payload,		
7	Mar 20 2005 09:42:18	715005: Group = 10.64.10.15, IP = 10.64.10.15, processing SA payload		
0 7	Mar 20 2005 09:42:18	715005: Group = 10.64.10.15, IP = 10.64.10.15 , processing hash		
7	Mar 20 2005 09:42:18	713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message (msgid=fb7d1b90) v		
8.5	Mar 20 2005 09:42:18	713904: IP = 10.64.10.15 , Received encrypted packet with no matching SA, droppin		
D 7	Mar 20 2005 09:42:18	713906: IP = 10.64.10.15 , IKE DECODE SENDING Message (msgid=fb7d1b90) wi		
P 7	Mar 20 2005 09:42:18	714004IKE Initiator sending 1st GM pkt: msg id = fb7d1b90,		
₽ 7	Mar 20 2005 09:42:18	715005: Group = 10.64.10.15, IP = 10.64.10.15, constructing qm hash		
D 7	Mar 20 2005 09:42:18	714007IKE Initiator sending Initial Contact,		
7	Mar 20 2005 09:42:18	715005: Group = 10.64.10.15, IP = 10.64.10.15 , Transmitting Proxy Id:		
D 7	Mar 20 2005 09:42:18	715001: Group = 10.64.10.15, IP = 10.64.10.15 constructing proxy ID,		
D 7	Mar 20 2005 09:42:18	715001: Group = 10.64.10.15, IP = 10.64.10.15 constructing ipsec nonce payload,		
D 7	Mar 20 2005 09:42:18	715005: Group = 10.64.10.15, IP = 10.64.10.15, constructing ISA_SA for ipsec		
07	Mar 20 2005 09:42:18	715005: Group = 10.64.10.15, IP = 10.64.10.15, constructing blank hash		
•				

In order to view related graphs, choose **Monitoring > VPN > IPSEC Tunnels**. Then, move **IPSec Active Tunnels** and **IKE Active Tunnels** to Selected Graphs, and choose **Show Graphs**.

🔂 Cisco ASDM 5.0 for PIX - 192.168.4.1 - Graph (3)
Cisco ASDM 5.0 for PIX - 192.168.4.1 - Graph (3)
Graph Table
IPSec Tunnels, IKE Active Tunnels
IVE Active Tuppels
t
e 0.5 I
S.
09:24:39 09:26:09 09:27:39 09:29:09 09:30:39 09:32:09 09:33:39
Firewall Time (UTC)
View: Real-time, data every 10 sec 💌
Granh Toble
iPSec Tunnels, iPSec Active Tunnels
1 IPSec Active Tunnels
t u la
n
e 0.5
s l
Firewall Time (UTC)
View: Real-time, data every 10 sec
Export Print Bookmark Close Help

## 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 VPN

Service Providers: VPN Service Architectures

Service Providers: Network Management

Virtual Private Networks: General

## **Related Information**

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco PIX 500 Series Security Appliances
- Cisco Secure PIX Firewall Command References
- Requests for Comments (RFCs)
- Technical Support & Documentation Cisco Systems

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

Updated: Jun 28, 2005

Document ID: 63882