Table of Contents

IPsec: Router-to-PIX Security Appliance 7.x and Later or ASA Configuration Example	1
Document ID: 63883	1
Introduction	1
Prerequisites	1
Requirements	1
Components Used	1
Conventions	1
Background Information	2
Configure	2
Network Diagram.	2
Configurations	2
Configuration using ASDM.	7
Verify	14
Troubleshoot	14
Troubleshooting Commands	14
NetPro Discussion Forums – Featured Conversations	14
Related Information	15

IPsec: Router-to-PIX Security Appliance 7.x and Later or ASA Configuration Example

Document ID: 63883

Introduction Prerequisites Requirements Components Used Conventions Background Information Configure Network Diagram Configurations Configuration using ASDM Verify Troubleshoot Troubleshoot MetPro Discussion Forums – Featured Conversations Related Information

Introduction

This document demonstrates how to configure an IPsec tunnel from PIX Security Appliance 7.x and later or the Adaptive Security Appliance (ASA) with one internal network to a 2611 router that runs a crypto image. Static routes are used for simplicity.

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-525 with PIX Software version 7.0
- Cisco 2611 router with Cisco IOS® Software Release 12.2(15)T13

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

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

Background Information

On the PIX, the **access–list** and **nat 0** commands work together. When a user on the 10.1.1.0 network goes to the 10.2.2.0 network, the access list is used to permit the 10.1.1.0 network traffic to be encrypted without Network Address Translation (NAT). On the router, the **route–map** and **access–list** commands are used to permit the 10.2.2.0 network traffic to be encrypted without NAT. However, when those same users go anywhere else, they are translated to the 172.17.63.230 address through Port Address Translation (PAT).

These are the configuration commands required on the PIX Security Appliance in order for traffic *not* to run through PAT over the tunnel, and traffic to the Internet to run through PAT

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

Configure

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

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

These configuration examples are for the command line interface. See the Configuration using Adaptive Security Device Manager (ASDM) section of this document if you prefer to configure using ASDM.

• Headquarters PIX

Branch Router

Headquarters PIX HQPIX(config)#**show run** PIX Version 7.0(0)102 names interface Ethernet0 description WAN interface nameif outside security-level 0 ip address 172.17.63.229 255.255.255.240 . interface Ethernet1 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0 1 interface Ethernet2 shutdown no nameif no security-level no ip address 1 interface Ethernet3 shutdown no nameif no security-level no ip address 1 interface Ethernet4 shutdown no nameif no security-level no ip address 1 interface Ethernet5 shutdown no nameif no security-level no ip address 1 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname HQPIX domain-name cisco.com ftp mode passive clock timezone AEST 10 access-list 100 extended permit ip any any access-list 150 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 access-list nonat extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 pager lines 24 logging enable logging buffered debugging 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 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0
access-group 100 in interface inside
route outside 0.0.0.0 0.0.0.0 172.17.63.230 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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partner protocol tacacs+
username cisco password 3USUcOPFUiMCO4Jk encrypted
http server enable
http 10.1.1.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
crypto ipsec transform-set avalanche esp-des esp-md5-hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec df-bit clear-df outside
crypto map forsberg 21 match address nonat
crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside
isakmp identity address
isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 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 172.17.63.230 type ipsec-121
tunnel-group 172.17.63.230 ipsec-attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
1
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
```

Cisco – IPsec: Router-to-PIX Security Appliance 7.x and Later or ASA Configuration Example

```
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect http
!
service-policy asa_global_fw_policy global
Cryptochecksum:3a5851f7310d14e82bdf17e64d638738
: end
SV-2-8#
```

Branch Router
BranchRouter# show run Building configuration
Current configuration : 1719 bytes !
<pre>! Last configuration change at 13:03:25 AEST Tue Apr 5 2005 ! NVRAM config last updated at 13:03:44 AEST Tue Apr 5 2005 !</pre>
version 12.2 service timestamps debug datetime msec service timestamps log uptime no service password-encryption !
hostname BranchRouter
logging queue-limit 100 logging buffered 4096 debugging !
username cisco privilege 15 password 0 cisco memory-size iomem 15 clock timezone AEST 10 ip subnet-zero !
: ip audit notify log ip audit po max-events 100 ! !
rypto isakmp policy 11 encr 3des
authentication pre-share group 2
crypto isakmp key ciscol23 address 172.17.63.229 ! !
crypto ipsec transform-set sharks esp-des esp-md5-hmac !
crypto map nolan 11 ipsec-isakmp set peer 172.17.63.229 set transform-set sharks
match address 120
1
1
!
1 1

```
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
1
1
mta receive maximum-recipients 0
1
1
!
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex
ip nat pool branch 172.17.63.230 172.17.63.230 netmask 255.255.255.0
ip nat inside source route-map nonat pool branch overload
no ip http server
no ip http secure-server
ip classless
ip route 10.1.1.0 255.255.255.0 172.17.63.229
1
1
access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any
1
route-map nonat permit 10
match ip address 130
!
call rsvp-sync
!
1
mgcp profile default
1
dial-peer cor custom
1
1
!
!
1
line con O
line aux 0
line vty 0 4
login
!
!
end
```

Configuration using ASDM

This example demonstrates how to configure the PIX using the ASDM GUI. A PC with a browser and IP address 10.1.1.2 is connected to the inside interface e1 of the PIX. Ensure http is enabled on the PIX.

This procedure illustrates the ASDM configuration of the Headquarters PIX.

1. Connect the PC to the PIX and choose a download method.

	CISCO SYSTEMS
CIECO MODIMI D'O	allineatilline.
isco ASDM 5.0 provides an intuitive graphical user into onfigure and manage your Cisco Security Appliances.	erface that makes it easy to set up,
isco ASDM runs as either a local application or a Java	Applet.
tunning Cisco ASDM as a local Application	h
Upgrades of the local application are perform You can invoke ASDM from desktop shortcuts One desktop shortcut allows you to connect to	ed automatically. . No browser is required. o <i>multiple</i> Security Appliances.
Download ASDM Launcher a	and Start ASDM
Junning Fisco &EDM as a Taus Anolat	
You can run Cisco ASDM as a Java applet that is dyn	amically downloaded from the device to
which you connect.	an in anani in anno 1996 an 11 1998 an 199
5	
Bun ASDM as a Jav	a Applet

ASDM loads the existing configuration from the PIX.

Cisco ASOM 5.0 for PIX - 10.1.1.1 File Roles Search Options Tools Wizards Help	
Home Configuration Monitoring Back Forward Search	Refresh Save Hep Cisco Status
Device Information	Interface Status
General License	Interface IP Address/Mask Line Link Current Kbps
Host Name:	
PIX Version: Device Uptime:	
ASDM Version: Device Type:	
Firewall Mode: Status	X
Total Flash:	
VPN Status Please wait while ASDM is lo	ading the current configuration from your
IKE Tunnels: device.	
CPU CPU Usage (p 62	Total:
Memory Usag	
Latest ASDM Syslog Messages	Input Kbps:
Initializing Monitor modules	<admin> NA (15)</admin>

This window provides monitoring instruments and menus.

Dendon Information		Interface Status
Coneral Lineare]		Interface Status
oenerar License		inside 10.1.1.1/24 Oup Oup 1
Host Name: SV-2-8.ciscou	com	
PDX Version: 7.0(0)102	Device Uptime: 0d 0h 24m 50s	
ASDM Version: 5.0(0)73	Device Type: PIX 525	
Firewall Mode: Routed	Context Mode: Single	
Total Flash: 16 MB	Total Memory: 256 MB	Select an interface to view input and output Kbps
VPN Status		Traffic Status
IKE Tunnels: 0	IPSec Tunnels: 0	Connections Per Second Usage
0 x 04 57 46 04 56 38	6	0.5 01:50:50 UDP: 0 TCP: 0 Tetal: 0 'inside' leterface Traffic Urage (Ospi)
Memory Memory Usage (M	8)	2211
67M8 041		24 16 04:00:26
		Input Kbps: 0 Output Kbps: 1
Latest ASDM Syslog Messages	5	Configure ASDM System Fill

2. Select **Configuration > Features > Interfaces** and select **Add** for new interfaces or **Edit** for an

existing configuration.

e Co	nfiguration Monitoring	Beck F	orward	Search	Refresh :	Save Help					allb
tures 0	configuration ► Features > In	nanaces Por por por s	51.001	_			_	-		-	_
l _o faces	- 2 M (1)										
5	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU		D	Ad
y Policy	Ethernet1	inside	Yes	100	10.1.1.1	255 255 255 0	No.	1500			Ed
k	Ethernet0	outside	Yes	0	172.17.63.229	255 255 255 240	No	1500	WAN interface		De
AT	Ethernet2		No				No				-
3	Ethernet3		No				No				
	Ethernet4		No				No				
3	Ethernet5		No				No				
Blocks Rece stration											
eruos	at										

3. Select the security options for the inside interface.

le Rules Se	arch Options Tools Wiz	cards Help		Contrast Contrast				
Home C	anfiguration Monitoring	Back Forward	Search Refresh	Save Help			Cis	ee Systems
Features	Configuration > Features >	Security Policy > Access	Rules					
	* • • • • • • •	1 10 10 10 10 10	l.					
Interfaces	(FAccess Rules)	AAA Rules C Filter Ru	les C Service Policy R	ules .				
<u>6.</u>	Show Rules for Interface	All Interfaces	Show All					
ecurity Policy	# Rule Action	Source	Destination	Rule Applied	Interface	Service	Log Level Interval	Add
245	1 🗹 🧭	🔹 any	🔹 any	al incoming in	side	10 to		Edit
NAT								Delete
93								
VPN								
1.0								
Routing								
.80								
elding Blocks								
3								
Device								
Properties								
	1							
	🖌 Allow traffic	O Deny traffic				Show Summary	C Show Detail	
		Apply	Reset	Advance	id			
Wizards <								

4. In the NAT configuration, encrypted traffic is NAT–exempt and all other traffic is NAT/PAT to the outside interface.

atures	Configuration - Featur	eo = NAT = Translation Rules S & Ro & Ro & S & S rough the Srewall without addres es	ss translation] nption Rules Show All				
NAT	Rule	Original			Translated		A
3	Type Interfa	ice Source Network	Destination Network	Interface	Address	DNS Rewrite	6
ng Blocks ng Blocks ence nubhation genties							

5. Select **VPN >General > Tunnel Group** and enable a Tunnel Group

204				à	Casco System
Home	Configuration Monitoring Back	Forward Search Rt	etrech Save He	la la	allowally
Features	Contiguration + Features + VPN + Ger	neral > Tunnel Group			
Electricos Security Policy NAT NAT CUPH Routing Building Blocks Device Administration	Clent Update Clent Update Clent Update Clent Update Clent Update Clent Update Clent Update Clent Update Clent Update Clent Carlo Coup Matching Clent ficate Group Matching Clent ficate Group Matching	Tunnel Geoup Tunnel Geoup Manage VPN tunnel ge IPBec connections. Name T217.62.00 DefaultRACroup Default.2LOrcup Specify the delimeter t are received when ture Group Delimiter	toups. A VPN tunnel group Type 1956-121 lipset-Ta lipset-121	P represents a connection spe Group Policy DitGropPolicy DitGropPolicy DitOrpPolicy	ctilc record for Add Eoit Detete

6. Select **VPN > IKE > Global Parameters** and enable IKE on the outside interface.



7. Select **VPN > IKE > Policies** and choose the IKE policies.

Home G	Configuration Monitoring Back	Forward 5	learch Re	fresh	Save He	ilp			استالس
Features	Configuration > Features > VFN > IKE	Policies	_	_			_	_	
Interfaces ourty Policy WPN ANT POLICY Routing Biory Biory Biory Device Device Device properties	Coneral Sofeneral Sofeneral	Policies Configure o Security Ass protocols.	Encryption 1)des	t Key Exch tanageme Hash sha	ange (IKE) alig est Protacel (IS D-H Group 2	orithms and paran Ak3dP) framework Authentication pre-share	neters, within the IPS for the AH and ESP Lifetime(secs) 86400	lec Internet IPSec Add Edit Delete	
					(App)		leset		

8. Select **VPN > IPsec > IPsec Rules** and choose **IPsec** for the local tunnel and remote addressing.

Features	Configuration + Features + VPN + IPSec	IPSec Ru	les				
Interfaces interfaces incurity Policy NAT Security Policy NAT Security Policy NAT Security Policy Properties	Conneral Client Updale Tunnel Group Group Policy Crefister Oroup Matching Policies Certificate Oroup Matching Policy Policies Certificate Oroup Matching Policy Policy Policy Policy Policy Construction Policy Polic	PSec R Use the	ules Rules menu, Action protect	the toolbar, or the right m PDC Side HostNetwork ≇ 10.111.024	rouse button to add, edit or de Remote Side HostNictwork 2010.2.2.074	elete rules. Service	Turmel Po Add

9. Select **VPN > IPsec > Tunnel Policy** and choose the tunnel policy.

Home Co	nfiguration Monitoring Back	Forward Search	h Refresh	Save Help				طاسختك
Festures	Configuration = Feromes = VEN = IRSec VEN System Options Clant Update UPN System Options Clant Update UPN System Options Clant Update UPN System Options Clant Update UPN System Options Definition Policy Policy Prolices Parameters Policy Prolices Parameters Policy Prolices Parameters Policy Prolices Parameters Policy Prolices Parameters	Tunnel Policy Specify Tunnel Policy Specify Tunnel Policy Interface outside t	Alicy Type & Priority (static - 21	Transform Set	Peer 172 17 63 230	Connection Type Bidirectional	SA 01 00 00 er	Add Edit Delete

10. Select **VPN > IPsec > Transform Sets** and choose a Transform set.

Homo d	Configuration Montoring Back	Forward Search	Refresh	Save Help			diad
Features	Configuration > Features > VPN > IPSec	> Transform Sets					
Interfaces Interf	General General Given Update Tunnel Group Giona Parametees Giobal Parametees Giob	Transform Sets Specify Transform Sets Specify Transform Sets ESP-DES-SNA ESP-DES-SNA ESP-AES-128-SNA ESP-AES-128-SNA ESP-AES-128-SNA ESP-AES-128-SNA ESP-AES-128-SNA ESP-AES-128-SNA ESP-AES-256-SNA ESP-AES-256-MD5	Node Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel	ESP Entryption DES DES 3DES 4ES-128 4ES-128 4ES-128 4ES-128 4ES-128 4ES-128 4ES-256 4ES-256	ESP Authentication MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5	AH Authentication None None None None None None None No	Add Edit Derete
				/oply	Reset		

11. Select **Routing > Routing > Static Route** and choose a static route to gateway router. In this example, the static route points to the remote VPN peer for simplicity.

Elsco ASDM SJ	0 for PIX - 10.1.1.1 Options Tools With	se Hielo	× 101×
Home C	Configuration Montoring	Dack Forward Search Ratech Save Hep	Cisco Station
Features Netraces Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Policy Policy Reading Dukting Blocks Administration Properties	Contiguration = Feedures = I Contiguration = Feedures = Feedures = I Contiguration = Feedures	outing - Routing - Static Route Batic Route Specify static routes. Interface IP Address Netmask Gateway outside 0.0.0 0.0.0 172.17.63.	IP Metric Tunneled Add 230 1 No Edit Delete
Wizards X	1	eiero	

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- show crypto ipsec sa Shows the phase 2 security associations.
- show crypto isakmp sa Shows the phase 1 security associations.

Troubleshoot

You can use ASDM to enable logging and to view the logs.

- Select Configuration > Properties > Logging > Logging Setup, choose Enable Logging and click Apply to enable logging.
- Select Monitoring > Logging > Log Buffer > On Logging Level, choose Logging Buffer, and click View to view the logs.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use debug commands.

- debug crypto ipsec Shows the IPsec negotiations of phase 2.
- debug crypto isakmp Shows the ISAKMP negotiations of phase 1.
- debug crypto engine Shows the traffic that is encrypted.
- clear crypto isakmp Clears the security associations related to phase 1.
- clear crypto sa Clears the security associations related to phase 2.
- **debug icmp trace** Shows whether ICMP requests from the hosts reach the PIX. You need to add the **access–list** command to permit ICMP in your configuration in order to run this debug.
- **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 you can see the output with the **show log** command.

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 PIX Firewall Software
- Cisco Secure PIX Firewall Command References
- Security Product Field Notices (including PIX)
- Requests for Comments (RFCs)
- Technical Support & Documentation Cisco Systems

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

Updated: Jan 18, 2006

Document ID: 63883