# ASA/PIX - Configurar um túnel IPsec LAN a LAN do roteador Cisco IOS

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Informações de Apoio Configurar Diagrama de Rede Configurações Configurações Configuração usando ASDM Verificar Troubleshoot Comandos para Troubleshooting Informações Relacionadas

### **Introduction**

Este documento demonstra como configurar um túnel de IPsec da um PIX Security Appliance 7.x ou posterior ou um Adaptive Security Appliance (ASA) com uma única rede interna para o roteador 2611 que executa a imagem crypto. As rotas estáticas são usadas por simplicidade.

Consulte <u>Configurando IPSec - Roteador para PIX</u> para obter mais informações sobre a configuração de um túnel LAN para LAN entre um roteador e o PIX.

Consulte <u>Túnel IPSec LAN a LAN entre o Cisco VPN 3000 Concentrator e o PIX Firewall Exemplo</u> para obter mais informações sobre a configuração de um túnel LAN a LAN entre o PIX Firewall e o Cisco VPN 3000 Concentrator.

Consulte o Exemplo de Configuração de Túnel IPsec Entre PIX 7.x e VPN 3000 Concentrator para saber mais sobre o cenário em que o túnel de LAN para LAN está entre o PIX e o VPN Concentrator.

Consulte o <u>Exemplo de Configuração de PIX/ASA 7.x Enhanced Spoke-to-Client VPN com</u> <u>Autenticação TACACS+</u> para saber mais sobre o cenário em que o túnel de LAN para LAN entre os PIXes também permite que um VPN Client acesse o PIX do spoke através do PIX do hub.

Consulte a <u>SDM: Exemplo de Configuração de VPN IPsec Site-to-Site entre ASA/PIX e um IOS</u> <u>Router</u> para saber mais sobre o mesmo cenário em que o PIX/ASA Security Appliance executa a versão de software 8.x. Consulte o <u>Configuration Professional: Exemplo de Configuração de VPN IPsec Site-to-Site entre</u> <u>ASA/PIX e um IOS Router</u> para saber mais sobre o mesmo cenário em que a configuração relacionada ao ASA é mostrada usando a GUI do ASDM e a configuração relacionada ao roteador é mostrada usando a GUI do Cisco CP.

### **Prerequisites**

### **Requirements**

Não existem requisitos específicos para este documento.

### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- PIX-525 com software PIX versão 7.0
- Roteador Cisco 2611 com Software Cisco IOS® versão 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**

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.</u>

# Informações de Apoio

No PIX, os comandos access-list e nat 0 trabalham juntos. Quando um usuário na rede 10.1.1.0 vai para a rede 10.2.2.0, a lista de acesso é usada para permitir que o tráfego da rede 10.1.1.0 seja criptografado sem a Tradução de Endereço de Rede (NAT). No roteador, os comandos **route-map** e **access-list** são usados para permitir que o tráfego de rede 10.2.2.0 seja criptografado sem NAT. No entanto, quando alguns desses usuários vão para algum outro lugar, eles são convertidos no endereço 172.17.63.230 por meio de Conversão de Endereço de Porta (PAT).

Estes são os comandos de configuração necessários no PIX Security Appliance para que o tráfego *não* seja executado através do PAT pelo túnel e o tráfego para a Internet seja executado através do 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

# <u>Configurar</u>

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

#### Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



#### **Configurações**

Esses exemplos de configuração são para a interface de linha de comando. Consulte a <u>seção</u> <u>Configuração usando o Adaptive Security Device Manager (ASDM)</u> deste documento se preferir configurar usando o ASDM.

- PIX da matriz
- Roteador da filial

#### PIX da matriz

```
HQPIX(config)#show run
PIX Version 7.0(0)102
names
!
interface Ethernet0
description WAN interface
nameif outside
security-level 0
ip address 172.17.63.229 255.255.240
!
interface Ethernet1
nameif inside
```

```
security-level 100
ip address 10.1.1.1 255.255.255.0
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname HOPIX
domain-name cisco.com
ftp mode passive
clock timezone AEST 10
access-list Ipsec-conn 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 Ipsec-conn
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 *
!
class-map inspection_default
match default-inspection-traffic
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
inspect http
1
service-policy asa_global_fw_policy global
Cryptochecksum: 3a5851f7310d14e82bdf17e64d638738
: end
SV-2-8#
```

Roteador da filial

```
BranchRouter#show run
Building configuration...
Current configuration : 1719 bytes
!
! 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
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
1
hostname BranchRouter
1
logging queue-limit 100
logging buffered 4096 debugging
1
username cisco privilege 15 password 0 cisco
memory-size iomem 15
clock timezone AEST 10
ip subnet-zero
1
1
1
ip audit notify log
ip audit po max-events 100
!
!
crypto isakmp policy 11
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 172.17.63.229
1
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
1
1
1
no voice hpi capture buffer
no voice hpi capture destination
1
1
mta receive maximum-recipients 0
!
!
```

```
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
1
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
route-map nonat permit 10
match ip address 130
!
call rsvp-sync
!
1
mgcp profile default
!
dial-peer cor custom
!
!
1
1
1
line con 0
line aux 0
line vty 0 4
login
!
1
end
```

# Configuração usando ASDM

Este exemplo demonstra como configurar o PIX usando a GUI do ASDM. Um PC com um navegador e o endereço IP 10.1.1.2 está conectado à interface interna e1 do PIX. Verifique se http está habilitado no PIX.

Este procedimento ilustra a configuração ASDM do PIX da matriz.

1. Conecte o PC ao PIX e escolha um método de download.

Cisco ASDM 5.0	adhoodhio
Cisco ASDM 5.0 provides an intuitive graphical user configure and manage your Cisco Security Applianc	r interface that makes it easy to set up, ces.
Cisco ASDM runs as either a local application or a 3	ava Applet.
Running Cisco ASDM as a local Application	
<ul> <li>Upgrades of the local application are perfected.</li> <li>You can invoke ASDM from desktop shorts</li> <li>One desktop shorts allows you to connected.</li> </ul> Download ASDM Launch	ormed automatically. cuts. No browser is required. ct to <i>multiple</i> Security Appliances. er and Start ASDM
Running Cisco ASDM as a Java Applet	
You can run Cisco ASDM as a Java applet that is which you connect.	dynamically downloaded from the device to
and the second	have Araba
Run ASDM as a	Java Applet

O ASDM carrega a configuração existente do PIX.

Device Information			Interface Stat	us		
General License			Interface	IP Address/Mask	Line Lin	k Current Kbps
Host Name: PDC Version: ASDM Version:	Device	Uptime:				
Firewall Mode: Total Flash:	Status				×	
VPN Status IKE Tunnels:	2	Please wait while ASDM is device.	loading the curren	t configuration from yo	ur	
- System Resources Status CPU		Initializing Monitor module	9	]	Total	
Memory Memory Usag						
			input Kbg	e 🗖 0	Jutput Klope:	

Essa janela fornece instrumentos e menus de monitoramento.

💼 Cisco ASDM 5.0 for PIX - 10.1.1.1	
File Rules Search Options Tools Wizards Help	
Home Configuration Monitoring Back Forward Search	Refresh Save Hep Cisco Stores
- Device Information	Interface Status
General License	Interface IP Address/Mask Line Link Current Kbps
Host Name SV-2-8 cisco.com	inside 10.1.1.1/24 O up O up 1
PIX 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
I/E Tunnale: 0 IPSec Tunnale: 0	Connections Per Second Usage
System Resources Status           CPU         CPU Usage (percent)           01         00           04:57:46         04:57:46           04:57:46         04:56:36           Memory         Memory Usage (MB)           67:48         250           102         125	0.5 01:50:50 UDP: 0 TCP: 0 Total: 0 Sincide" leterface Traffic Usage (Kbps)
0457.46 0458.36	nput Kbpz: 0 📕 Output Kbpz: 1
- Latest ASDM Syslog Messages	Configure ADDM System Filter
Sysiog Disabled	
Device configuration loaded successfully.	<admin> NA (15) 😡 😹 🔒 4/5/05 4:57:46 AM UTC</admin>

 Selecione Configuration > Features > Interfaces e selecione Add para novas interfaces ou Edit para uma configuração existente.

ures C	onfiguration + Features + In ♦ 👷 🏵   😰   📋 🐰	netacas Par IBA (B) A	60				-	-			
aces	Interface	Name	Enabled	Security	IP Address	Submet Mask	Management	MTU		D	Add
Policy	Ethernett	Inside	Yes	100	10.1.1.1	255.255.255.0	No.	1500			Ed
8	Ethernet0	outside	Yes	0	172.17.63.229	255 255 255 240	No	1500	WAN interface		Dele
u .	Ethernet2		No				No				
5	Ethernet3		No				No				
	Ethernet4		No.				No				
5	Ethernet5		No				No:				
ting B						Ŧ.					
trig Blocks Ree tration Torties											

3. Selecione as opções de segurança para a interface

#### interna.

11 F					Cisco St
Hone C	onfiguration Monitoring Bac	k Forward Search Refre	sh Save Help		allen
Features	Configuration > Features > Security i	Policy > Access Rules			
Eterisces	Access Rules	C Filter Rules C Service Poli	icy Rules		
600 Policy	Show Rules for Interface. All Inter	naces Show All Destination	Rule Applied Interface	Carries	Log Level /
34	Enabled Ho	stNetwork HostNetwor	rk To Traffic muenace	Bene	Interval
NAT NAT	1 🛛 🗸 🖓 🖬	• any	+ incoming inside	<b>2</b> 9	
0					
VPN					
Routing					
.80					
alding Blocks					
3					
Device dministration					
_					
Properties			[		
Properties	✓ Allow traffic ③ Deny	ាកណីខ		C Show Summary	C Show Detail

4. Na configuração de NAT, o tráfego criptografado é isento de NAT e todos os outros tráfegos são NAT/PAT para a interface

0		0 0	QQ	2 ?		Cu	ce Stotes
Home C	Configuration Montoring	Back Forward	Search Refresh	Save Help			(Baard))a
	• + 7 3 1						
interfaces	Enable traffic through	the firewall without addres	s translation				
6.	Transistion Rules	C Translation Exem	ption Rules				
ecurity Policy	Show Rules for Interface	E All Interfaces	Show All				
1 AL	Rule	Original			Translated		Add
C2	Type Interface	Source Network	Destination Network	Interface	Address	DNS Rewrite	Edit
VPN	1. inside	de 10.1.1.0/24	I any	outside	172 17 63 229 interface PAT)	No	Delete
and the second s							
Alding Blocks Device derivitivation Properties							
ulting Blocks Device strainestration Properties	*					v	

5. Selecione VPN >Geral > Grupo de Túneis e habilite um Grupo de Túneis



6. Selecione VPN > IKE > Parâmetros globais e ative IKE na interface

externa.	KO for P1X = 10.1.1.1 earch Options Tools Wizards Help		د اعالہ
Home	Configuration Montoring Back	O Q C G G Forward Search Refresh Save Help	Cisco Systems
Features Interfaces Security Policy MAT Security Policy MAT Security Policy MAT Security Policy NAT Security Policy NAT Securi	Configuration - Features - VPN> KE Configuration - Features - VPN> KE Configuration - Features Client Update Tunnel Group Client Update Tunnel Group Client Update - Policy - Policies - Policies - Policy - Poli	Olobal Parameters         Enable IKE         Interface         Value         Outside         Yes         Clobal PSec over NAT-T         Nat Transparency         Enable IPSec over NAT-T         Nat Science         Clobal Parameters         Enable IPSec over TCP         Enable IPSec over TCP         Enable IPSec over TCP         Enable IPSec over TCP         Identity to Be Sent to Peer         Identity:       Address         Koy Id String:         Disable inbound aggressive mode connections         Avert peers before disconnecting         Wait for all active sessions to voluntarily terminate before rebooting	
Wizards /		(1000 N8 (2) D 45 A 4900	2 30 05 PM ACCT

7. Selecione VPN > IKE > Policies e escolha as políticas de

IKE.

Carbon C	Construction account Data		and it is a set
estures	Contegeration = restures = with a loce =	P0804	_
Interfaces ourity Policy WPN VPN Routing Routing Blocks Device heritation	Client Update     VPN System Options     Client Update     Group Policy     Outron Group     Scottion     Scottion     Scottion     Scottion     Policy     Policy     Policy     Policy     Policy     Policy     Policy     Pre-Fragmentation     P Address Management     Pools     Pools	Policies         Configure specific Internet Key Exchange (KE) algorithms and parameters, within the IPSec Internet Security Association Key Management Protocol (IBAKMP) framework, for the AH and ESP IPSec protocols.         Priority # Encryption Hash D-H Group Authentication Lifetime(secs)         1       3das         2       pre-share         86400	
		Apply Reset	

8. Selecione VPN > IPsec > IPsec Rules e escolha IPsec para o túnel local e o endereçamento remoto.

Hone C	Configuration Monitoring Back	Forward	Search	Retresh Save	? Help		C	sco Sesteus
Features	Configuration + Features + VPN + IPSec	► IPSec Ru	les					
Interfaces Security Policy MAT	Ciert Update     General     General	IPSec R Use the	ules Rules menu, Action protect	the toolbar, or the right m PDC Side HostNotwork © 10.1.1.0/24	nouse button to add, edit or d Remote Side HostNotwork C 10.2.2.0/24	elete rutes. Service	Turnel Po	Add Edit Delete
Routing Building Blocks Building Blocks Administration Properties	Protes     Protes     Protes     Protect	1						
				anciv	(F SI	now Burnmary 🤇	Show Detail	

9. Selecione VPN > IPsec > Tunnel Policy e escolha a política de túnel.



10. Selecione VPN > IPsec > Transform Sets e escolha um Transform Set.

Cisco ASDM	5.0 for PDX - 10.1.1.1		-				_10 ×
File Rules 6	Search Options Tools Wizards Help						Cites Systems
Homo	Configuration Monitoring Back	Forward Search	Refresh	Save Help			dis die
Features Features Interfaces Security Policy MAT Security Policy MAT Properties Properties	Configuration > Foolures - VFN > PSoc Configuration > Foolures - VFN > PSoc Configuration > Foolures - VFN > PSoc Client Update - Client U	Zeschi     Zeschi     Zeschi     Zeschi     Zeschi     Transform Sets     Specify Transform Sets	Mode Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel	ESP Encryption DES DES JDES JDES AES-128 AES-128 AES-128 AES-128 AES-128 AES-128 AES-128 AES-128 AES-128 AES-128 AES-256	ESP Authentication MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5	AH Aufbentication None None None None None None None No	Add Edt Delete
Wizards -				Apply	Reset		

11. Selecione **Routing > Routing > Static Route** e escolha uma rota estática para o roteador do gateway. Neste exemplo, a rota estática aponta para o peer VPN remoto para simplificar.

Cisco ASDM S	.0 for PIX - 10.1.1.1	فالكنام والمحد						
File Rules in Home	Configuration Montoring	ands Help	Q Search R	etresh Save	? Help			Cisco Systems
Festures	Configuration = Fexures = + @ @ @ @ @ @ @ & @ % Routing - % RP - @ Proxy ARPs B % OSPF B % IGMP B * IGMP B * IGMP B * IGMP B * IGMP B * IGMP	Routing - Routing - Sis Ref & Sistic Route Specify static routh Interface outside	bc Route es. IP Address 00.00	Netmask 0.0.0.0	Gateway IP 172-17:63-230	Metric 1	Tunneled No	Add Edit Delete
without a	3.				cisco NA	0 6		05 3 39 36 PM AEST

# **Verificar**

Use esta seção para confirmar se a sua configuração funciona corretamente.

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

- show crypto ipsec sa Mostra as associações de segurança da fase 2.
- show crypto isakmp sa Mostra as associações de segurança da fase 1.

### **Troubleshoot**

Você pode usar o ASDM para ativar o registro e exibir os registros.

- Selecione Configuration > Properties > Logging > Logging Setup, escolha Enable Logging e clique em Apply para ativar o registro.
- Selecione Monitoring > Logging > Log Buffer > On Logging Level, escolha Logging Buffer e clique em View para exibir os logs.

### Comandos para Troubleshooting

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- debug crypto ipsec Mostra as negociações de IPsec da fase 2.
- debug crypto ipsec Exibe as negociações ISAKMP da fase 1.
- debug crypto engine Mostra o tráfego que está criptografado.
- clear crypto isakmp Limpa as associações de segurança relacionadas à fase 1.
- clear crypto sa Limpa as associações de segurança relacionadas à fase 2.
- debug icmp trace Mostra se as solicitações ICMP dos hosts acessam o PIX. Você precisa adicionar o comando access-list para permitir o ICMP em sua configuração para executar essa depuração.
- logging buffer debugging Mostra as conexões estabelecidas e negadas aos hosts que passam pelo PIX. As informações são armazenadas no buffer de log PIX e você pode ver a saída com o comando show log.

# Informações Relacionadas

- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- <u>Cisco PIX Firewall Software</u>
- <u>Referências do comando Cisco Secure PIX Firewall</u>
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)