# PIX/ASA 7.x e mais tarde: Conectando redes internas múltiplas com o exemplo de configuração do Internet

# Índice

Introdução **Pré-requisitos** Requisitos **Componentes Utilizados Produtos Relacionados** Convenções Configurar Informações de Apoio Diagrama de Rede Configurações Configuração de PIX usando o ASDM Configuração de PIX usando o CLI Verificar Troubleshooting Comandos para Troubleshooting Procedimento de Troubleshootina Incapaz de alcançar por nome Web site Informações Relacionadas

# Introdução

Este documento fornece uma configuração de exemplo do PIX/ASA Security Appliance, versão 7.x e posteriores, com redes internas múltiplas conectadas à Internet (ou a uma rede externa) que usam a interface de linha de comando CCLI) ou o Security Device Manager (ASDM) 5.x e versões posteriores.

Consulte <u>para estabelecer e pesquisar defeitos a Conectividade através do dispositivo do Cisco</u> <u>Security</u> para obter informações sobre de como estabelecer e pesquisar defeitos a Conectividade com o PIX/ASA.

Refira a <u>utilização nat, global, estática, a conduíte, e os comandos access-list e a porta</u> <u>Redirection(Forwarding) no PIX</u> para obter informações sobre dos comandos pix comuns.

**Nota:** Algumas opções em outras versões ASDM podem parecer diferentes das opções em ASDM 5.1. Consulte a <u>documentação do ASDM</u> para obter mais informações.

# Pré-requisitos

### **Requisitos**

Quando você adiciona mais de uma rede interna atrás de um PIX Firewall, mantenha estes pontos na mente:

- O PIX não apoia o endereçamento secundário.
- Um roteador tem que ser usado atrás do PIX a fim conseguir o roteamento entre a rede existente e a rede recentemente adicionada.
- O gateway padrão de todos os anfitriões precisa de apontar ao roteador interno.
- Adicionar uma rota padrão no roteador interno esses pontos ao PIX.
- Cancele o esconderijo do Address Resolution Protocol (ARP) no roteador interno.

Consulte <u>Permitindo o Acesso HTTPS para o ASDM</u> para permitir que o dispositivo seja configurado pelo ASDM.

### **Componentes Utilizados**

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

- Ferramenta de segurança 515E PIX com versão de software 7.1
- ASDM 5.1
- Roteadores Cisco com Software Release 12.3(7)T de Cisco IOS®

**Nota:** Este documento recertified com versão de software 8.x PIX/ASA e Cisco IOS Software Release 12.4.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

### **Produtos Relacionados**

Esta configuração pode igualmente ser usada com versão 7.x e mais recente da ferramenta de segurança de Cisco ASA.

### **Convenções**

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

## **Configurar**

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

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

Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

### Informações de Apoio

Nesta encenação, há três redes internas (10.1.1.0/24, 10.2.1.0/24 e 10.3.1.0/24) a ser conectadas ao Internet (ou a uma rede externa) com o PIX. As redes internas são conectadas à interface interna do PIX. A conectividade de Internet é através de um roteador que seja conectado à interface externa do PIX. O PIX tem o endereço IP de Um ou Mais Servidores Cisco ICM NT 172.16.1.1/24.

As rotas estáticas são usadas para distribuir e vice-versa os pacotes das redes internas ao Internet. Em vez de usar as rotas estáticas, você pode igualmente usar um protocolo de roteamento dinâmico tal como o Routing Information Protocol (RIP) ou o Open Shortest Path First (OSPF).

Os host internos comunicam-se com o Internet traduzindo as redes internas no PIX usando NAT dinâmico (pool dos endereços IP 172.16.1.5 a 172.16.1.10). Se o pool dos endereços IP de Um ou Mais Servidores Cisco ICM NT é esgotado, o PIX PANCADINHA (que usa o endereço IP 172.16.1.4) os host internos alcançará o Internet.

Refira <u>indicações PIX/ASA 7.x NAT e de PANCADINHA</u> para obter mais informações sobre do NAT/PAT.

**Nota:** Se o NAT estático usa o endereço IP (global\_IP) externo para traduzir, isso poderia causar uma tradução. Assim, use a palavra chave **interface** em vez do endereço IP na tradução estática.

### Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



O gateway padrão dos hosts na rede 10.1.1.0 aponta para o RoteadorA. Uma rota padrão no roteadorB é adicionada que aponte ao roteadorA. O roteador A tem uma rota padrão que aponta para a interface dentro do PIX.

### **Configurações**

Este documento utiliza as seguintes configurações:

- Configuração do Roteador A
- <u>Configuração do roteador B</u>
- <u>Configuração da ferramenta de segurança 7.1 PIXConfiguração de PIX usando o</u> <u>ASDMConfiguração de CLI da ferramenta de segurança PIX</u>

```
Configuração do Roteador A
RouterA#show running-config Building configuration...
Current configuration : 1151 bytes ! version 12.4
service config service timestamps debug uptime service
timestamps log uptime no service password-encryption !
hostname RouterA ! interface Ethernet2/0 ip address
10.2.1.1 255.255.255.0 half-duplex ! interface
Ethernet2/1 ip address 10.1.1.2 255.255.255.0 half-
duplex ! ip classless ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3 ! ! line con 0
line aux 0 line vty 0 4 ! end RouterA#
Configuração do roteador B
RouterB#show running-config Building configuration..
Current configuration : 1132 bytes ! version 12.4
service config service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption ! hostname RouterB ! interface
FastEthernet0/0 ip address 10.1.1.3 255.255.255.0 speed
auto ! interface Ethernet1/0 ip address 10.3.1.1
255.255.255.0 half-duplex ! ip classless ip route
0.0.0.0 0.0.0.0 10.1.1.2 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! end RouterB#
```

Se você quer usar o ASDM para a configuração da ferramenta de segurança PIX, mas não amarrou o dispositivo, termine estas etapas:

- 1. Console no PIX.
- 2. De uma configuração esclarecida, use as alertas interativas a fim permitir o ASDM para o Gerenciamento do PIX da estação de trabalho 10.1.1.5.

Configuração da ferramenta de segurança 7.1 PIX
Pre-configure Firewall now through interactive prompts
[yes]? yes
Firewall Mode [Routed]:
Enable password [ <use current="" password="">]: cisco</use>
Allow password recovery [yes]?
Clock (UTC):
Year [2005]:
Month [Mar]:
Day [15]:
Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5
The following configuration will be used:

```
Enable password: cisco
         Allow password recovery: yes
         Clock (UTC): 14:45:00 Mar 15 2005
         Firewall Mode: Routed
         Inside IP address: 10.1.1.1
         Inside network mask: 255.255.255.0
         Host name: OZ-PIX
         Domain name: cisco.com
         IP address of host running Device Manager:
10.1.1.5
Use this configuration and write to flash? yes
         INFO: Security level for "inside" set to 100 by
default.
         Cryptochecksum: a0bff9bb aa3d815f c9fd269a
3f67fef5
965 bytes copied in 0.880 secs
        INFO: converting 'fixup protocol dns maximum-
length 512' to MPF commands
        INFO: converting 'fixup protocol ftp 21' to MPF
commands
        INFO: converting 'fixup protocol h323_h225
1720' to MPF commands
        INFO: converting 'fixup protocol h323_ras 1718-
1719' to MPF commands
        INFO: converting 'fixup protocol netbios 137-
138' to MPF commands
        INFO: converting 'fixup protocol rsh 514' to
MPF commands
        INFO: converting 'fixup protocol rtsp 554' to
MPF commands
        INFO: converting 'fixup protocol sip 5060' to
MPF commands
        INFO: converting 'fixup protocol skinny 2000'
to MPF commands
        INFO: converting 'fixup protocol smtp 25' to
MPF commands
        INFO: converting 'fixup protocol sqlnet 1521'
to MPF commands
         INFO: converting 'fixup protocol sunrpc_udp
111' to MPF commands
        INFO: converting 'fixup protocol tftp 69' to
MPF commands
        INFO: converting 'fixup protocol sip udp 5060'
to MPF commands
         INFO: converting 'fixup protocol xdmcp 177' to
MPF commands
Type help or '?' for a list of available commands.
        07-PTX>
```

### Configuração de PIX usando o ASDM

Termine estas etapas a fim configurar através do ASDM GUI:

- 1. Da estação de trabalho 10.1.1.5, abra um navegador da Web para usar o ADSM (neste exemplo, https://10.1.1.1).
- 2. Clique sim nas alertas do certificado.
- 3. Início de uma sessão com a senha da possibilidade, como configurada previamente.

- 4. Se isto é a primeira vez o ASDM está executado no PC, você é alertado usar a launcher ASDM ou o ASDM como um App das Javas. Neste exemplo, a launcher ASDM é selecionada e instalada.
- 5. Vá à janela ASDM Home e clique a

<i>c</i>	~
configu	iracao
	n ayao.

Device Information			Interface Stat	us			
General License			Interface	IP Address/Mask	Line	Link	Current Kb
Lingthlows: whether	swall default damain imm	15.4	inside	10.1.1.1/24	🗿 up	🗿 up	1
PIVVersion: 7.1/1	Device Untim	nia o: 44d Sh Ann Ae					
ACDM Marcian 5 1/1	Device Type:	DIV 6460					
Eirewall Mode: Boute	d Context Mode	Single					
Total Flach: 16 ME	Total Momon	64 MB	Calculation intervi	and the start formula in	d and and the		
MDN Status	i total methor		Traffic Status	ace to view input an	a output Koj	15	
IKE Tunnels: 0	IPSec Tunne	្នា	Connections	Per Second Usage			
13 17.48.40 Memory Memory	19 Usage (MB)		17-58-0 UDP: 0 'inside' Interfa	TCP: 0		fotal: D	
0840 3840 16 17:58:10			0.5 17.58.19 Input Kbp	s 0 📕	Output Kbps	: 1	
Latest ASDM Syslog M	essages				<u>C</u>	nfigure AS	SDM Syslog Filt
	Syslog Disab	led					

6. Escolha a **relação > editam** a fim configurar a interface externa.

Cisco ASDM	5.1 for PIX - 10.1.1.1				7 <u>8</u>	_ [] ×
File Rules s	Search Options Tools Wizard	s Help	0			Ciero Sverene
Home	Configuration Monitoring	Back Forward	Search Retresh	Save Help		
	Configuration > Interfaces					
Interfaces	************	e in				
Security Policy	Interface	Name Enable	d Security IP Addres	s Subnet Mask	Management MTU Only	Add
2 As	EthernetD	No		Ī	No	Edit
NAT	Ethernet1	inside Yes	10010.1.1.1	255.255.255.0	No 1500	Delete
3						
VPN						
Routing						
Robal Objects						
Distortion						
Properates						
	Enable traffic between t	wo or more interfaces (	which are configured with	same security levels		
			1000	Direct 1		
		_	0449Y	rteset		
	,		<admin></admin>	NA (15)	8 7/11/08	3 5:59:49 PM UTC

 Incorpore os detalhes da relação e clique a APROVAÇÃO quando você é feito.

🚰 Edit Interface		×
Hardware Port:	Ethernet0	Configure Hardware Properties
🔽 Enable Interface	Dedicate this interface to man	agement only
Interface Name:	outside	
Security Level:	0	
- IP Address	10 (A)	
Ose Static IP	C Obtain Address via DHCP	
IP Address:	172.16.1.1	
Subnet Mask:	255.255.255.0	
MTU:	1500	
Description:		
	OK Cancel	Help
Clique a <b>APROVAÇÃO</b>	<b>na</b> caixa de diálogo da mudança	do nível de
seyulaliya.		



9. O clique **aplica-se** para aceitar a configuração da interface. A configuração igualmente obtém empurrada no

8.

Cisco ASDM 5.1 File Rules Bea	for PIX - 10.1.1.1 rdh Options Tools Wizard	s Help							
Home Co	enfiguration Monitoring	Back F	orward	Q Search	Refresh	Save Help			Cisco Systems
Interfaces	Configuration > Interfaces • 👲 🏵 😰 💼 🕺 S	2 <b>6 6</b> i	5 <b>(</b> 9						
Security Policy	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU	Add
220	Ethernet0	outside	Yes	0	172.16.1.1	255.255.255.0	No	1500	Edit
NAT	Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	No:	1500	Delete
Routing Global Objects Properties									
	Enable traffic between th	wo ar more in	terfaces wi	hich are c Apply	onfigured with sa	me secunty levels		<u> </u>	

10. Escolha a **política de segurança na** aba das características a fim rever a regra da política de segurança usada. Neste exemplo, a regra interna do padrão é usada.

Cisco ASDM 5.1	I for PIX - 10.1.1.1	and Lion				
Home C	onfiguration Monitoring	Back Forward	Q Q Search Refresh	Save Help	Cis	CO SYSTEMS
Interfaces Security Policy NAT VPN Coloal Objects Froperties	Configuration - Security P	Access Rules	s C Semice Policy Ru Show All Destination Host/Network	Rule Applied To Traffic ins (ou (ou Advanced	Interface Service ide ibound) Summary C Show Detail 4	Add Edf Delete
			<admin></admin>	NA (15)	8 📉 🛛 🖄 7/11/06 6:01	1:49 PM UTC

11. Neste exemplo, o NAT é usado. Desmarcar o **tráfego da possibilidade com o Firewall sem** caixa de verificação da **tradução de endereços** e o clique **adiciona** a fim configurar a regra NAT.

Cisco ASDM S File Rules S	.1 for PIX - earch Optio	10.1.1.1 ons Tools Wiza	rds Help				X
S Home	Configuratio	n Monitoring	Back Forward S	Q Q Search Refresh	Save Help		CISCO SYSTEMS
Interfaces	Contigura	tion > NAT > Trans →	lation Rules Par IBA IBA IBA ISA ISA Ihe frewall without address C Translation Exemp	translation: tion Rules			
NAT	Show	Rules for Interface	All Interfaces Original	Show All	ļ	Translated	Add
VPN Routing Glabel Objects	Typ	e Interface	Source Network	Destination Network	Interface	Address	Defete
Properties	1						IJ
	1.8	ianic NAT 🦷	Dynamic NAT 4 Stat	Apply sadmin>	Reset	Manage Pools.	6:02:29 PM UTC

 Configurar a rede da fonte. Neste exemplo, 10.0.0.0 é usado para o endereço IP de Um ou Mais Servidores Cisco ICM NT, e 255.0.0.0 é usado para a máscara.Clique em Manage Pools para definir os endereços do pool de NAT.

oource i re	SUNCTION				
		Interface:	inside	<u> </u>	
		IP Address:	10.0.0		
		Mask:	255.0.0.0	*	
			Browse		
					NAT Options
anslate Ad	idress on Inte	inace: Jouts			
anslate Ad Translate C י י	Idress on Inte Address To – Static Redirect p	IP Address;		<b>T</b>	
anslate Ad Translate ( اب	Address on Inte Address To – Static Redirect p © TCP © UDP	IP Address; port Original port	Translati	ed port:	
anslate Ad Translate ۲۰۰۱	Address on Inte Address To – Static Redirect p © TCP © UDP Dynamic	IP Address; port Original port Address Pool:	Translati	ed port:	Pools
anslate Ad Translate C 1	Idress on Inte Address To – Static E Redirect p C TCP C UDP Dynamic Pool ID	IP Address; port Original port Address Pool:	Translati	ed port: Manage	Pools
anslate Ad Translate C 1	Idress on Inte Address To – Static Redirect p © TCP © UDP Dynamic Pool ID N/A	IP Address: port Original port Address Pool: No address po	Translati	ed port: Manage	Pools

13. Selecione a interface externa e o clique **adiciona**.

tside	
	Edit
	Delete

 Neste exemplo, o pool de uma escala e do endereço PAT é configurado. Configurar o endereço do conjunto NAT da escala e clique a APROVAÇÃO.

	Togrande		PoonD.	<u> </u>	
Range					
C Port Ad	idress Transla	ition (PAT)			
C Port Ad	idress Transla	ition (PAT) usin	g the IP addres	s of the interface	
IP A	ddress: 172	.16.1.5	– [*	172.16.1.10	
	NO.				
Netv	vork Mask (opti	ional): 25	5.255.255.0		

15. Selecione a interface externa em etapa 13 a fim configurar o endereço PAT. Clique em OK.

Hoorarobarr	ool Item	
Interface:	outside  Pool ID: 1	
C Range		
🖲 Port Ad	dress Translation (PAT)	
C Port Ad	dress Translation (PAT) using the IP address of the interface	
IP Ad	uress. 172.16.1.4 -	
IP Ad	ork Mask (optional): 255.255.255.0	
IP Ad	oress. 172.16.1.4 —   ork Mask (optional): 255.255.255.0	

Clique a APROVAÇÃO a fim

Pool ID	IP Address(es)	
		Add
1 172.10	0.1.4	
1 172.10	5.1.5-17Z.16.1.10	Edit
		Delete
	1 172.10 1 172.10	1 172.16.1.4 1 172.16.1.5-172.16.1.10

 No indicador da regra de tradução de endereço da edição, selecione o pool ID para ser usado pela rede da fonte configurada. Clique em OK.

OBE NAT	<b>O</b> U	se Policy NAT					
Source Ho:	st/Network						
		Interface: IP Address: Mask:	inside 10.0.0.0 255.0.0.0		Y		
anslate Add	dress on Inte	rface: outsi	Browse	]			NAT Options
Translate A	ddress To						
Translate A	Address To — Static E Redirect p	IP Address:			2		
Translate A C 1	Address To – Static Redirect p © TCP © UDP	IP Address: fort Original port		Translated	port.		
Translate A	Address To – Static Redirect p © TOP © UDP Dynamic	IP Address: fort Original port Address Pool:	1	Translated	port Manage	Pools	
Translate A	Address To – Static Redirect p © TOP © UDP Dynamic Pool ID	IP Address: ort Original port Address Pool:	1 Ac	Translated	port.	Pools	
Translate A	Address To – Static Redirect p © TCP © UDP Dynamic Pool ID	IP Address: ort Original port Address Pool: 172.16.1.4 172.16.1.5-177	1 1 16 1 10	Translated Idress	port Manage	Pools	

17. O clique **aplica-se** a fim empurrar a regra configurada NAT para o PIX.



 Neste exemplo, as rotas estáticas são usadas. Clique o roteamento, escolha a rota estática e o clique adiciona.

# 19. Configurar o gateway padrão e clique a

	Add Static Route		×
	Interface Name:	outside	
	IP Address:	0.0.0.0	
	Mask:	0.0.0.0	
	Gateway IP:	172.16.1.2	
	Metric	1	
	C Tunneled (Used	l only for default route)	
APROVAÇÃO.	ок	Cancel Help	1

10

20. O clique adiciona e adiciona as rotas às redes

	付 Add Static Rou	te			×
	Interface Na	ame:	inside	•	
	IP Address:		10.2.1.0		
	Mask:		255.255.255.0	•	
	Gateway IP:		10.1.1.2		
	Metric		1		
	C Tunneled	(Used o	nly for default rout	e)	
internas	ОК		Cancel	Help	
Add	Static Route			×	
I	nterface Name:	inside			
1	P Address:	10.3.1.	0		
1	Mask:	255.25	5.255.0 💌		
Q	Sateway IP:	10.1.1.	2		
Ģ	Metric	1			
C	Tunneled (Used o	nly for de	fault route)		
	ок	Cancel	Help		

21. Confirme que as rotas corretas estão configuradas e o clique **se** aplica.

Eisco ASDM File Rules S	5.1 for PIX - 10.1.1.1 earch Options Tools Wizan	ts Help				_
San Home	Configuration Monitoring	Back Forward :	Q Q Search Refresh	Save	🦻 Help	Cisco Systems
Interfaces Security Policy NAT Security Policy NAT Security Properties	Contiguration > Routing > Ro Contiguration > Routing >	uting > Static Route  Para Route  Static Route  Specify static routes.  Interface IP Addre  outside 0.0.0.0  inside 10.2.1.0  Inside 10.3.1.0	ISS Netmask 0.0.0.0 255.255.255.0 255.255.255.0	Gateway IP 172.16.1.2 10.1.1.2 10.1.1.3	Metric 1 1 1 1 Reset	Tunneler Add No N/A Edit N/A Delete
С	-		<admin></admin>	NA (15)	🛃 🔂	7/11/06 7:48:40 PM UTC

### Configuração de PIX usando o CLI

A configuração através do ASDM GUI está agora completa.

Você pode ver esta configuração através do CLI:

#### Ferramenta de segurança CLI PIX

pixfirewall(config)#write terminal PIX Version 7.0(0)102
names ! interface Ethernet0 nameif outside security-
level 0 ip address 172.16.1.1 255.255.255.0 ! interface
Ethernet1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! Assign name and IP address
to the interfaces enable password 2KFQnbNIdI.2KYOU
encrypted passwd 2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control ! Enforce a strict NAT for all the
traffic through the Security appliance global (outside)
1 172.16.1.5-172.16.1.10 netmask 255.255.255.0 !
Define a pool of global addresses 172.16.1.5 to
172.16.1.10 with ! NAT ID 1 to be used for NAT global
(outside) 1 172.16.1.4 netmask 255.255.255.0 ! Define
a single IP address 172.16.1.4 with NAT ID 1 to be used
for PAT nat (inside) 1 10.0.0.0 255.0.0.0 ! Define
the inside networks with same NAT ID 1 used in the
global command for NAT route inside 10.3.1.0
255.255.255.0 10.1.1.3 1 route inside 10.2.1.0
255.255.255.0 10.1.1.2 1 ! Configure static routes
for routing the packets towards the internal network
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 !

Configure static route for routing the packets towards
the Internet (or External network) 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 ! Enable the HTTP server on PIX for ASDM
access http 10.1.1.5 255.255.255.255 inside ! Enable
HTTP access from host 10.1.1.5 to configure PIX using
ASDM (GUI) ! ! Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end

Escolha **configuração running do arquivo > da mostra na nova janela** a fim ver a configuração de CLI no ASDM.

File Rules Search Options Tools Wizards Help
Refresh ASDM with the Running Configuration on the Device Reset Device to the Factory Default Configuration
Show Running Configuration in New Window
Save Running Configuration to Flash Save Running Configuration to TFTP Server Save Running Configuration to Standby Unit Save Internal Log Buffer to Flash
Print
Clear ASDM Cache Clear Internal Log Buffer
Exit

# **Verificar**

No momento, não há procedimento de verificação disponível para esta configuração.

# **Troubleshooting**

### Comandos para Troubleshooting

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

Nota: Consulte <u>Informações Importantes sobre Comandos de Depuração</u> antes de usar comandos **debug**.

• debug icmp trace - Exibe se as requisições de ICMP dos hosts alcançam o PIX. A fim

executar isto debugar, você precisam de adicionar o **comando access-list** permitir o ICMP em sua configuração.

 eliminação de erros do logging buffer — Mostra as conexões que são estabelecidas e negadas aos anfitriões que atravessam o PIX. A informação é armazenada no buffer de registro PIX e você pode ver a saída com o comando show log.

### Procedimento de Troubleshooting

O ASDM pode ser usado para permitir o registro, e para ver igualmente os logs:

1. Escolha a **configuração > as propriedades > instalação de registro > de registro**, a verificação **permite o registro**, e o clique **aplica-**

Se.						
Cisco ASDM 5.1 for PIX - 10 File Rules Search Option	ns Tools Wizards	Help				×
Home Configuration	Montoring	Back Forward	Q Retres	h Save	<b>?</b> Help	CISCO SYSTEMS
Image: Security Policy       Image: Security Policy         Image: Security Poli	on × Properties × Log Lup Wizard Setup Spoofing Update ificate ice Access ice Administrati 2P Services 3 Client over Imment ory Metrics udit ging ogging Setup Swant Lists Logging Setup State Limit Syslog Servers Syslog Setup rity Queue URPC Server Options	ging > Logging Setup ■ Setup ■ Enable logging ■ Enable logging ■ Send debug n ■ Logging to Intern Specify the size of be overwritten. Buffer Size: 40 You can choose t Save Buffer To: ASDM Logging Specify the size of Queue Size: 1	Image: set in the set in	pig E ps E s S to which syslogs ntents before the Configure FTF Configure FTA pigs Intended for v pily	nable logging on lend syslogs in El will be saved. Wh buffer is overwriti P Settings sh Usage tewing in ASDM. Reset	the failover standby unit MBLEM format ien the buffer fills up, it will ten.

 Escolha a monitoração > registrando > buffer de registro > nível de registro e escolha o logging buffer da lista de drop-down. Clique a vista.



3. Está aqui um exemplo do buffer de registro:

💁 Log Buf	fer Electron	
C Rema	esh 🔄 Save 🖙 Clea	r 🛄 Color Settings 📲 Create Rule 🔤 Brithw Rule Find:
This table	shows syslog messages	s in ASDM logging buffer as of now.
Severity	Time	Message ID: Description
<u>ê</u> 6	Jul 12 2006 13:08:11	605005: Login permitted from 10.1.1.5/1136 to inside:10.1.1.1/https for user "enable_15"
<u>4</u> 6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
<u>ê</u> 6	Jul 12 2006 13:08:11	725003: SSL client inside:10.1.1.5/1136 request to resume previous session.
<u>1</u> 6	Jul 12 2006 13:08:11	725001: Starting SSL handshake with client inside:10.1.1.5/1136 for TLSv1 session.
<u>ê</u> 6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1136) to NP Identity Ifc:10.
<u>1</u> 6	Jul 12 2006 13:08:10	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:10	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>4</u> 6	Jul 12 2006 13:08:10	110001: No route to 171.71.179.143 from 10.1.1.5
<u>i</u> 6	Jul 12 2006 13:08:09	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>4</u> 6	Jul 12 2006 13:08:09	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:08	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>1</u> 6	Jul 12 2006 13:08:08	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:07	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>*</u> 6	Jul 12 2006 13:08:07	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:06	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>4</u> 6	Jul 12 2006 13:08:06	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:05	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>*</u> 6	Jul 12 2006 13:08:05	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:04	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>4</u> 6	Jul 12 2006 13:08:04	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:03	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>4</u> 6	Jul 12 2006 13:08:03	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:02	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>4</u> 6	Jul 12 2006 13:08:02	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>4</u> 6	Jul 12 2006 13:08:01	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>∔</u> 6 ∢]	Jul 12 2006 13:08:01	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
0 Er	nergencies 🗿 Alerts	Critical e Errors A Warnings A Notifications A Informational O Debugging

### Incapaz de alcançar por nome Web site

Em determinadas encenações, as redes internas não podem alcançar os Web site do Internet usando o nome (trabalhos com endereço IP de Um ou Mais Servidores Cisco ICM NT) no navegador da Web. Esta edição é comum e ocorre geralmente se o servidor DNS não é definido, especialmente nos casos onde o PIX/ASA é o servidor DHCP. Também, isto pode ocorrer nos casos se o PIX/ASA é incapaz de empurrar o servidor DNS ou se o servidor DNS não é alcançável.

## Informações Relacionadas

- <u>Cisco PIX 500 Series Security Appliances</u>
- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Referências do comando Cisco Secure PIX Firewall</u>
- <u>Cisco Adaptive Security Device Manager</u>
- Troubleshooting e Alertas do Cisco Adaptive Security Device Manager (ASDM)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação Cisco Systems