# ASA 7.x/PIX 6.x e superior: Exemplo de configuração de abrir/bloquear portas

## Contents

Introduction Prerequisites Requirements Componentes Utilizados Produtos Relacionados Conventions Configurar Diagrama de Rede Bloqueando a configuração das portas Abrindo a configuração de portas Configuração por meio do ASDM Verificar Troubleshoot Informações Relacionadas

## **Introduction**

Este documento fornece uma configuração de exemplo para abrir ou bloquear as portas para vários tipos de tráfego, como http ou ftp, no Security Appliance.

**Observação:** os termos "abrindo a porta" e "permitindo a porta" têm o mesmo significado. Da mesma forma, "bloquear a porta" e "restringir a porta" também oferecem o mesmo significado.

## **Prerequisites**

#### **Requirements**

Este documento pressupõe que o PIX/ASA está configurado e funciona corretamente.

#### **Componentes Utilizados**

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

- Cisco 5500 Series Adaptive Security Appliance (ASA) que executa a versão 8.2(1)
- Cisco Adaptive Security Device Manager (ASDM) versão 6.3(5)

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.

#### Produtos Relacionados

Essa configuração também pode ser usada com o Cisco 500 Series PIX Firewall Appliance com o software versão 6.x e superior.

#### **Conventions**

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

## **Configurar**

Cada interface deve ter um nível de segurança de 0 (mais baixo) a 100 (mais alto). Por exemplo, você deve atribuir sua rede mais segura, como a rede do host interno, ao nível 100. Embora a rede externa conectada à Internet possa ser de nível 0, outras redes, como DMZs, podem ser posicionadas entre elas. Você pode atribuir várias interfaces ao mesmo nível de segurança.

Por padrão, todas as portas são bloqueadas na interface externa (nível de segurança 0) e todas as portas são abertas na interface interna (nível de segurança 100) do Security Appliance. Dessa forma, todo o tráfego de saída pode passar pelo Security Appliance sem nenhuma configuração, mas o tráfego de entrada pode ser permitido pela configuração da lista de acesso e dos comandos estáticos no Security Appliance.

**Observação:** em geral, todas as portas são bloqueadas da Zona de Segurança Inferior para a Zona de Segurança Superior e todas as portas são abertas da Zona de Segurança Superior para a Zona de Segurança Inferior, desde que a inspeção stateful seja habilitada para tráfego de entrada e de saída.

Esta seção é composta pelas subseções, conforme mostrado:

- Diagrama de Rede
- Bloqueando a configuração das portas
- <u>Abrindo a configuração de portas</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:



#### Bloqueando a configuração das portas

O Security Appliance permite qualquer tráfego de saída, a menos que ele seja explicitamente bloqueado por uma lista de acesso estendida.

Uma lista de acesso é composta por uma ou mais entradas de controle de acesso. Dependendo do tipo de lista de acesso, você pode especificar os endereços origem e destino, o protocolo, as portas (para TCP ou UDP), o tipo ICMP (para ICMP) ou o EtherType.

**Observação:** para protocolos sem conexão, como o ICMP, o Security Appliance estabelece sessões unidirecionais, portanto, você precisa de listas de acesso para permitir o ICMP em ambas as direções (pela aplicação de listas de acesso às interfaces de origem e de destino) ou precisa habilitar o mecanismo de inspeção do ICMP. O mecanismo de inspeção ICMP trata as sessões ICMP como conexões bidirecionais.

Conclua estes passos para bloquear as portas, que geralmente se aplicam ao tráfego originado do interior (zona de segurança mais alta) para o DMZ (zona de segurança mais baixa) ou o DMZ para o exterior.

1. Crie uma lista de controle de acesso de forma que você bloqueie o tráfego de porta especificado.

access-list

2. Em seguida, vincule a lista de acesso ao comando access-group para estar ativa.

access-group

#### **Examples:**

1. Bloquear o tráfego da porta HTTP: Para bloquear o acesso da rede interna 10.1.1.0 ao http (servidor web) com o IP 172.16.1.1 colocado na rede DMZ, crie uma ACL como mostrado: ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.1 eq 80 ciscoasa(config)#access-list 100 extended permit ip any any ciscoasa(config)#access-group 100 in interface inside

**Observação:** use **no** seguido pelos comandos da lista de acesso para remover o bloqueio de porta.

 Bloquear o tráfego da porta FTP: Para bloquear o acesso da rede interna 10.1.1.0 ao FTP (servidor de arquivos) com o IP 172.16.1.2 colocado na rede DMZ, crie uma ACL como mostrado:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
host 172.16.1.2 eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

Observação: consulte portas IANA para saber mais sobre atribuições de porta.

A configuração passo a passo para executar isso através do ASDM é mostrada nesta seção.

1. Vá para Configuration > Firewall > Access Rules. Clique em Adicionar regra de acesso para

<b>4</b>	dd 🕶 🖪 Edit	💼 Delete	+ + 2	🌾 🐚 💼 - 🛛 🔍 Find
4	Add Access Ru	le		Destination
*	Insert			
	Insert After		.10.100	🏟 any
1 -	147 - 11 - 44	vər arry	-1 <sup>5</sup>	🏈 any
ė 🗳	👆 inside (2 outg	oing rules)		
1		<b>I</b> 172.1	16.10.50	🏟 any
2		🏈 any		🏈 any
ė 4	🖈 manage (2 imp	olicit incomin	g rules)	
-		Tour Course Statutes		-

criar a lista de acesso.

 Defina a origem e o destino e a ação da regra de acesso junto com a interface à qual essa regra de acesso será associada. Selecione os detalhes para escolher a porta específica a ser

	🖆 Add Access Rule
	Interface: Inside
	Action: O Permit O Deny
	Source: (10.1.1.0)
	Destination 172,16,1,1
	Service: ip
	Description:
	🛃 Enable Logging
	Logging Level: Default 💟
	More Options
bloqueada.	OK Cancel Help

3. Escolha http na lista de portas disponíveis e clique em OK para voltar à janela Adicionar

iter:	States are rear					Filte
Name	Protocal	Source Ports	Destination Ports	ICMP Type	Description	
teo discard	top	default (1-65535)	9			
- 119- damam	top	default (1-65535)	53			
- me echo	top	default (1-65535)	7			
18 over	top	default (1-65535)	512			
10 finger	top	default (1-65535)	79			
at ftp	top	default (1-65535)	21			
18 ftp-data	top	default (1-65535)	20			
- 10 gopher	top	default (1-65535)	70			
10 h323	top	default (1-65535)	1720			
32 hostname	top	default (1-65535)	101			
an hito	top	default (1-65535)	160	N - 2	1	
III https	top	default (1-65535)	443			
10- ident	top	default (1-65535)	113			
- 10 inap4	top	default (1-65535)	143			
mire	top	default (1-65535)	194			
12 kerberos	top.	default (1-65535)	750			
ma-klogn	top	default (1-65535)	543			
m lahel	top	default (1-65535)	544			
- 302- Idap	top	default (1-65835)	289			
-ma-idaps	top	defauk (1-65535)	606			
Statute for state	- 30 <u>-</u>					

regra de acesso.

4. Clique em OK para concluir a configuração da regra de

🖆 Add Access Rule	
Interface: inside 🔽	
Action: 🔿 Permit 💿 Deny	
Source: 10.1.1.0	
Destination 172.16.1.1	
Service: tcp/http	
Description:	
Enable Logging	
More Options	
OK Cancel Help	
5. Clique em <b>Inserir após</b> para adicionar uma regra de acesso à mesma lista de	
Configuration > Firewall > Access Rules	

4	Add - 🕑 Edit	🗍 Delete 👌 🗲	🔜 💼 💼 - 🔍 Fi
4	Add Access Ru	le	Destination
4	Insert		
	Insert After		📕 172.16.1.1
	-		🏟 any
÷.	🔊 manage (2 imp	olicit incoming rules)	
	1	🏈 any	Any less secur
cesso.	2	🍅 any	🏈 any

6. Permita que o tráfego entre "any" e "any" para evitar a "negação implícita". Em seguida, clique em **OK** para concluir a adição desta regra de

Interface:	inside 🔽
Action: 💿	Permit 🔿 Deny
Source:	any
Destination	any
Service:	ip
Description:	
💌 Enable L	logging
Logging I	Level: Default 💽
More Opt	ions

 A lista de acesso configurada pode ser vista na guia Regras de acesso. Clique em Apply para enviar esta configuração para o Security Appliance

#	Enabled	Source	Destination	Service	Action	Hits
. <b>5</b> 9 i	nside (3 incom	ing rules)				
1		凰 10.1.1.0	團 172.16.1.1	100/ http	🔞 Deny	
2	<b>Z</b>	📌 any	<ta>any</ta>	TP ip	🧹 Permit	
3		any	any	<u>⊥r&gt;</u> ip	🕴 Deny	
) 🦊 (	manage (2 imp	licit incoming rules)				
1		🌍 any	Any less secure ne	💴 ip	🖌 Permit	
2		🌑 any	<li>any</li>	<mark>⊥e</mark> > ip	🔞 Deny	
- <b>5</b>	outside (1 impl	licit incoming rule)				
1		🌍 any	🏟 any	😐 ip	3 Deny	
31.						

A configuração enviada do ASDM resulta nesse conjunto de comandos na CLI (Command

Line Interface, interface de linha de comando) do ASA. access-list inside\_access\_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www access-list inside\_access\_in extended permit ip any any access-group inside\_access\_in in interface inside

Por meio dessas etapas, o exemplo 1 foi executado por meio do ASDM para impedir que a rede 10.1.1.0 acesse o servidor web, 172.16.1.1. O exemplo 2 também pode ser obtido da mesma forma para bloquear o acesso de toda a rede 10.1.1.0 ao servidor FTP, 172.16.1.2. A única diferença estará no ponto de escolher a porta.**Observação:** esta configuração de regra de acesso para o exemplo 2 é presumida como uma nova configuração.

8. Defina a regra de acesso para bloquear o tráfego FTP e clique na guia **Detalhes** para escolher a porta de

📧 Add Acc	ess Rule
Interface:	inside 💌
Action: 🚫 P	<sup>p</sup> ermit 💿 Deny
Source:	10.1.1,0
Destination	172.16.1.1
Service:	ip 💮
Description:	
💽 Enable L	ogging
Logging l	.evel: Default 💙
More Opti	ions
	OK Cancel Help

9. Escolha a porta **ftp** e clique em **OK** para voltar à janela Adicionar regra de acesso.

ter:					
Jame	Protocol	Source Ports	Destination Ports	ICMP Type	Description
100 cibrix-ica	tcp	default (1-65535)	1494		
tiqbe	tcp	default (1-65535)	2748		
- 100 daytime	tcp	default (1-65535)	13		
ter discard	top	default (1-65535)	9		
ter domain	tcp	default (1-65535)	53		
w echo	top	default (1-65535)	7		
to exec	top	default (1-65535)	512		
10 finger	tcp	default (1-65535)	79		
- to ftp	top	default (1-65535)	21		—
ttp-data	top	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
10 h323	tcp	default (1-65535)	1720		
- 100 hostname	tcp	default (1-65535)	101		
ter http	top	default (1-65535)	60		
- Re https	top	default (1-65535)	443		
ident	top	default (1-65535)	113		
10 imap4	tcp	default (1-65535)	143		
TO IC	tcp	default (1-65535)	194		
- rev kerberos	tcp	default (1-65535)	750		
and Marsha	hen.	dofout (1 cccoc)	E40		
lected Service —	_				

10. Clique em **OK** para concluir a configuração da regra de

🖆 Add Acc	ess Rule
Interface:	inside 💉
Action: 🔘 i	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	tcp/ftp
Description:	
💽 Enable L	ogging
Logging l	Level: Default
More Opt	ions
	OK Cancel Help

11. Adicione outra regra de acesso para permitir qualquer outro tráfego. Caso contrário, a regra Negar implícito bloqueará todo o tráfego nessa

	🖆 Insert A	fter Access Rule
	Interface:	inside 😽
	Action: 💿 i	Permit 🔿 Deny
	Source:	any
	Destination	any
	Service:	ip 🔄
	Description:	
	💽 Enable Li	ogging
	Logging l	Level: Default 💉
	More Opt	ions
interface.		OK Cancel

12. A configuração completa da lista de acesso é semelhante a esta na guia Regras de acesso.

#	Enabled	Source	Destination	Service	Action
in 🤧 in	iside (3 incom	ing rules)			
1	¥	凰 10.1.1.0	172.16.1.1	🚾 ftp	🕴 Den
2		👘 any	👘 any	🌮 ip	🖌 Perr
3		🧼 any	🏟 any	🤊 ip	🕴 Den
n 🍋 🗧	anage (2 imp	licit incoming rules)			
1		🧼 any	Any less secure ne	₽ ip	🛹 Perr
2		🌍 any	🧼 any	10 ip	🕴 Den
- <b>M</b> o	utside (1 impli	icit incoming rule)			
1		🥥 any	🥥 any	😕 ip	🙆 Den
3					

13. Clique em **Apply** para enviar a configuração para o ASA. A configuração de CLI equivalente é semelhante a esta:

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp access-list inside_access_in extended permit ip any any access-group inside_access_in in interface inside
```

#### Abrindo a configuração de portas

O Security Appliance não permite nenhum tráfego de entrada, a menos que seja explicitamente permitido por uma lista de acesso estendida.

Se quiser permitir que um host externo acesse um host interno, você pode aplicar uma lista de acesso de entrada na interface externa. Você precisa especificar o endereço traduzido do host interno na lista de acesso porque o endereço traduzido é o endereço que pode ser usado na rede externa. Conclua estes passos para abrir as portas da zona de segurança inferior para a zona de segurança superior. Por exemplo, permita o tráfego de fora (zona de segurança inferior) para a interface interna (zona de segurança superior) ou DMZ para a interface interna.

 O NAT estático cria uma tradução fixa de um endereço real para um endereço mapeado. Esse endereço mapeado é um endereço que hospeda na Internet e pode ser usado para acessar o servidor de aplicativos na DMZ sem a necessidade de saber o endereço real do servidor.

```
static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
    access-list access_list_name | interface}
```

Consulte a seção <u>NAT estático da</u> <u>referência de comando para PIX/ASA</u> para saber mais. 2. Crie uma ACL para permitir o tráfego de porta específico.

```
access-list
```

3. Vincule a lista de acesso ao comando access-group para estar ativa.

```
access-group
```

#### **Examples:**

1. Abra o tráfego da porta SMTP: Abra a porta tcp 25 para permitir que os hosts de fora (Internet) acessem o servidor de e-mail colocado na rede DMZ.O comando Static mapeia o endereço externo 192.168.5.3 para o endereço DMZ real 172.16.1.3. ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit tcp any host 192.168.5.3 eg 25

```
ciscoasa(config)#access-group 100 in interface outside
```

2. Abra o tráfego da porta HTTPS: Abra a porta tcp 443 para permitir que os hosts externos (Internet) acessem o servidor web (seguro) colocado na rede DMZ.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
netmask 255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
any host 192.168.5.5 eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **Permitir o tráfego DNS:** Abra a porta **udp 53** para permitir que os hosts externos (Internet) acessem o servidor DNS (seguro) colocado na rede DMZ.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
netmask 255.255.255
ciscoasa(config)#access-list 100 extended permit udp
any host 192.168.5.4 eq 53
ciscoasa(config)#access-group 100 in interface outside
```

Observação: consulte portas IANA para saber mais sobre atribuições de porta.

#### Configuração por meio do ASDM

Nesta seção, uma abordagem passo a passo para executar as tarefas acima mencionadas através do ASDM é mostrada.

1. Crie a regra de acesso para permitir o tráfego smtp para o servidor



2. Defina a origem e o destino da regra de acesso e a interface com a qual essa regra se vincula. Além disso, defina a Ação como

🖆 Add Ao	cess Rule
Interface: Action: 🧿	Outside V Permit O Deny
Source:	(any )
Destination	192.168.5.3
Service:	ip 💽
Description	n:
🔽 Enable	Logging
Logging	g Level: Default
More Op	otions
it	OK Cancel Help

3. Escolha SMTP como a porta e clique em

Filter:					
Name	Protocol	Source Ports	Destination Ports	ICMP Type	Descripti
Me hhit	han a	defects (1 constant)	E76-0	1	
100 rsn	COD	derauk (1-00030)	514		
- no risp	top	default (1-65535)	504		
- Bo sp	- Iten	default (1+65555)	3060		
Los sucp	- boo	default (1 65535)	1521		
- Boy sqinec	han .	default (1-65555)	1021		
550	top	default (1-65535)	111		
sunrpc	top	default (1-65535)	10		
se tacacs	cop hos	default (1+65535)	49 E17		
taik.	ccp	derauk (1-05535)	317		
teinet	ccp	deraule (1-65535)	23		-
Nuch	ccp.	default (1-65535)	540		
- Minois	ccp	deraut (1-00000)	40		
Not view	Udp	derauc (0-05535)	512		
- Met bootpc	uap	derauc (0-65535)	66		
Her bootps	uap	default (0-65535)	67		
- IMP CITS	uap	deraut (0-65535)	3020		
www.discard	udp	default (0-65535)	9		
we disix	udp	default (0-65535)	195		
domain	udp	default (0-65535)	53		
Selected Service					
	2				

4. Clique em OK para concluir a configuração da regra de

📬 Add Acc	cess Rule
Interface:	outside 💌
Action: 💿	Permit 🔘 Deny
Source:	any
Destination	192.168.5.3
Service; (	tcp/smtp
Description:	
💽 Enable L	ogging
Logging	Level: Default
More Opt	ions
	OK Cancel

acesso.

5. Configure o NAT estático para converter 172.16.1.3 para 192.168.5.3Vá para **Configuration** > **Firewall > NAT Rules > Add Static NAT Rule** para adicionar uma entrada de NAT



estático.

Selecione a origem original e o

endereço IP traduzido juntamente com suas interfaces associadas e clique em **OK** para concluir a configuração da regra de NAT

🖆 Add Static NAT F	Rule	- 0
Original		
Interface:	DMZ	~
Source: (	172.16.1.3	
Translated		
Interface:	outside	~
💿 Use IP Address:	192.168.5.3	<u> </u>
🔘 Use Interface IP	Address	
Port Address Translatio	on (PAT)	
Enable Port Ad	Idress Translation (PAT)	
Protocol:		
Original Port:		
Translated Por	t:	
Connection Setting	js	*

imagem descreve as três regras estáticas listadas na seção Exemplos:

onfiq	uration > Firewa	all <u>&gt; NAT Rules</u> Delete ★ 🗲 👗 🛙	🖹 💼 - 🗌 Q, Find	📴 Diagram 🕯	💐 Packet Trace		
#	1	Original	Original			Translated	
	Type	Source	Destination	Service	Interface	Address	
DMZ	:						
1	• Static	3 172.16.1.3			outside	3 192.168.5.3	
2	• Static	<b>I</b> 172.16.1.5			outside	A 192.168.5.5	
3	Static	172.16.1.4			outside	192.168.5.4	

Esta imagem descreve as três regras de acesso listadas na seção Exemplos:

#	Enabled	Source	Destination	Service	Action
) 🦊 (	MZ (2 implicit	incoming rules)	Paste		
1		🧼 any	Any less secure ne	IP ip	🖌 Permit
2		🧼 any	any	IP/ ip	🕴 Deny
i 🥵 i	nside (2 implic	t incoming rules)			
1		🌍 any	Any less secure ne	IP/ ip	🖌 Permit
2		🧼 any	🏟 any	💷> ip	🔕 Deny
- 👎 n	manage (2 imp	licit incoming rules)			
1		🏟 any	Any less secure ne	IP ip	🖌 Permit
2		🏟 any	🏟 any	JE> ip	🕴 Deny
🚚 o	outside (4 inco	ming rules)			
1	¥	🧼 any	192.168.5.3	📧 smtp	🖌 Permit
2	$\checkmark$	🧼 any	192.168.5.5	10 https	🖌 Permit
3	Image: A start of the start	🦘 any	📕 192.168.5.4	🚥 domain	🧹 Permit
4		<ul> <li>any</li> </ul>	<ul> <li>any</li> </ul>	IP ip	🔞 Deny

## **Verificar**

Você pode verificar com determinados comandos show, como mostrado:

- show xlate exibe informações de conversão atuais
- show access-list exibir contadores de ocorrências para políticas de acesso
- show logging exibe os logs no buffer.

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.

## **Troubleshoot**

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- PIX/ASA 7.x: Ativar/Desativar Comunicação Entre Interfaces
- PIX 7.0 e Adaptive Security Appliance Port Redirection(Forwarding) com comandos nat, global, estático, conduit e access-list
- Usando comandos nat, global, estático, conduit e access-list e redirecionamento de porta (encaminhamento) no PIX
- PIX/ASA 7.x: Exemplo de Configuração de Habilitação de Serviços de FTP/TFTP
- <u>PIX/ASA 7.x: Exemplo de Configuração de Serviços de Habilitação de VoIP (SIP, MGCP, H323, SCCP)</u>
- PIX/ASA 7.x: Exemplo de Configuração de Acesso ao Servidor de Correio no DMZ

Suporte Técnico e Documentação - Cisco Systems