# ASA 7.x/PIX 6.x y Versiones Posteriores: Ejemplo de Configuración para Abrir o Bloquear los Puertos

### Contenido

Introducción Prerequisites Requirements Componentes Utilizados Productos Relacionados Convenciones Configurar Diagrama de la red Configuración de Bloqueo de los Puertos Configuración de Apertura de los Puertos Configuración mediante ASDM Verificación Troubleshoot Información Relacionada

### **Introducción**

Este documento proporciona un ejemplo de configuración sobre cómo abrir o bloquear los puertos para diversos tipos de tráfico, tales como http o ftp, en el dispositivo Security Appliance.

**Nota:** Los términos "abriendo el puerto" y "autorizando el puerto" significan lo mismo. Del mismo modo, "bloqueando el puerto" y "restringiendo el puerto" también significan lo mismo.

### **Prerequisites**

#### **Requirements**

Este documento supone que PIX/ASA está configurado y funciona correctamente.

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

• Cisco 5500 Series Adaptive Security Appliance (ASA) que ejecuta la versión 8.2(1)

• Versión 6.3(5) de Cisco Adaptive Security Device Manager (ASDM)

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.

#### **Productos Relacionados**

Esta configuración también se puede utilizar con el Cisco 500 Series PIX Firewall Appliance con la versión de software 6.x o posteriores.

#### **Convenciones**

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

### **Configurar**

Cada interfaz debe tener un nivel de seguridad de 0 (más bajo) a 100 (más alto). Por ejemplo, debe asignar la red más segura, como la red host interna, al nivel 100. Mientras que la red externa conectada a Internet puede ser el nivel 0, otras redes, como las DMZ, pueden ubicarse entre sí. Puede asignar múltiples interfaces al mismo nivel de seguridad.

De forma predeterminada, todos los puertos se bloquean en la interfaz externa (nivel de seguridad 0) y todos los puertos se abren en la interfaz interna (nivel de seguridad 100) del dispositivo de seguridad. De este modo, todo el tráfico saliente puede pasar a través del dispositivo de seguridad sin necesidad de una configuración, pero el acceso del tráfico entrante debe autorizarse mediante la configuración de la lista de acceso y los comandos estáticos en el dispositivo de seguridad.

**Nota:** En general, todos los puertos se bloquean desde la Zona de Seguridad Más Baja a la Zona de Seguridad Más Alta y todos los puertos se abren desde la Zona de Seguridad Más Alta a la Zona de Seguridad Más Baja; siempre que esté habilitada la inspección de estado tanto para el tráfico entrante como saliente.

Esta sección comprende las siguientes subsecciones:

- Diagrama de la red
- <u>Configuración de Bloqueo de los Puertos</u>
- <u>Configuración de Apertura de los Puertos</u>

En esta sección encontrará la información para configurar las funciones descritas en este documento.

<u>Nota:</u> Utilice la herramienta <u>Command Lookup</u> (sólo para clientes <u>registrados</u>) para obtener más información sobre los comandos utilizados en esta sección.

#### Diagrama de la red

En este documento, se utiliza esta configuración de red:



#### Configuración de Bloqueo de los Puertos

El dispositivo de seguridad permite cualquier tráfico saliente, excepto que esté explícitamente bloqueado por una lista de acceso extendido.

Una lista de acceso está conformada por una o más Access Control Entries (ACE). Según el tipo de lista de acceso, usted puede especificar las direcciones de origen y destino, el protocolo, los puertos (para TCP o UDP), el tipo ICMP (para ICMP) o EtherType.

**Nota:** Para los protocolos sin conexión, como ICMP, el dispositivo de seguridad establece sesiones unidireccionales, de modo que usted necesita listas de acceso para autorizar el ICMP en ambas direcciones (mediante la aplicación de listas de acceso a las interfaces de origen y destino) o bien debe habilitar el motor de inspección del ICMP. El motor de inspección del ICMP trata las sesiones del ICMP como conexiones bidireccionales.

Siga estos pasos para bloquear los puertos, que generalmente se aplican al tráfico que se origina desde la zona interna (zona de seguridad más alta) a la DMZ (zona de seguridad más baja) o desde la DMZ a la zona externa.

1. Cree una Access Control List (ACL) de forma que bloquee el tráfico del puerto especificado.

access-list

2. Luego vincule la lista de acceso con el comando access-group para activarla.

```
access-group
```

#### **Examples:**

1. Bloqueo del tráfico del puerto HTTP: Para bloquear el acceso de la red interna 10.1.1.0 al http (servidor Web) con IP 172.16.1.1 ubicada en la red DMZ, cree una ACL como se indica a continuación:

```
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
```

**Nota:** Utilice **no** seguido de los comandos de la lista de acceso para eliminar el bloqueo del puerto.

 Bloqueo del tráfico del puerto FTP: Para bloquear el acceso de la red interna 10.1.1.0 al FTP (servidor de archivos) con IP 172.16.1.2 ubicada en la red DMZ, cree una ACL como se indica a continuación:

```
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
```

Nota: Consulte Puertos IANA para obtener más información sobre las asignaciones de puerto.

La configuración paso a paso para realizar esto a través del ASDM se muestra en esta sección.

1. Vaya a Configuration > Firewall > Access Rules. Haga clic en Agregar regla de acceso para



 Defina el origen y el destino y la acción de la regla de acceso junto con la interfaz a la que se asociará esta regla de acceso. Seleccione los detalles para elegir el puerto específico que desea

🖆 Add Aco	cess Rule
Interface: (	inside 💌
Action: 🔿	Permit 💿 Deny
Source: (	10.1.1.0
Destination	172.16.1.1
Service:	ip 🔄
Description:	
💽 Enable L	ogging
Logging	Level: Default
More Opt	ions
	OK Cancel Help

bloquear.

3. Elija **http** de la lista de puertos disponibles y, a continuación, haga clic en **Aceptar** para volver a la ventana Agregar regla de

Filter.		Shere's large read					Entrio
Nerr	e	Protocal	Source Ports	Destination Ports	ICMP Type	Description	1
	18 decard	top	default (1-65535)	9			
	11 daman	top	default (1-65535)	53			
	110 echo	top	default (1-65535)	7			
	18 exec	top	default (1-65535)	512			
	339 finger	top	default (1-65535)	79			
	at fip	top	default (1-65535)	21			
	12 ftp-data	top	default (1-65535)	20			
	- 18- gopher	top	default (1-65535)	70			
	10 h323	top	default (1-65535)	1720			
	38 hostname	top	default (1-65535)	101			
	ap htp	top.	default (1-65535)	10		E	
1	m Ntps	top	default (1-65535)	443			
	12-ident	top	default (1-65535)	113			
11	10 inap4	top	default (1-65535)	143			
	mire	top	default (1-65535)	194			
	12 kerberos	top.	default (1-65535)	750			
	ste slogn	top	default (1-65535)	543			
	m Johel	top	default (1-65535)	544			
	- 12- Idap	top	default (1-65835)	389			
	- me-lidaps	top	default (1-65535)	636			
-	ed Service		00	N			

acceso.

4. Haga clic en Aceptar para completar la configuración de la regla de

🖆 Add Acc	ess Rule
Interface:	inside 💌
Action: 🔿 I	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	tcp/http
Description:	
💽 Enable L	ogging
Logging I	Level: Default
More Opt	ions
	OK Cancel Help
ic en <b>Insertar</b> (	<b>después</b> para agregar una regla de acceso a la misma lista de

acceso.

5. Haga clic

4	Add - 🗹 E	dit <u>î</u> Delete 👌	+ +	- よ 🖻 💼 - 🔍 Fi
4	Add Acces	s Rule		Destination
4	Insert			1
	Insert Afte	er	)	📕 172.16.1.1
	- -		🕘 🧠 any	
÷.	🔊 manage (:	2 implicit incoming r	ules)	
	1	🏈 any		Any less secur
ceso	2	🍅 any		🏈 any

6. Permita que el tráfico pase de "cualquiera" a "cualquiera" para evitar la "negación implícita". A continuación, haga clic en Aceptar para completar la adición de esta regla de

oterface:	inside 🗸 🗸
Action: 💿	Permit O Deny
iource:	any
estination	any
-1104-145 - 1104-145	
ervice;	P
escription:	
🗸 Enable L	ogging
Logging	Level: Default
Logging	
More Opt	ions

acceso.

 La lista de acceso configurada se puede ver en la ficha Access Rules (Reglas de acceso). Haga clic en Aplicar para enviar esta configuración al dispositivo de seguridad.

¥ i	Enabled	Source	Destination	Service	Action	Hits
🥵 in	side (3 incom	ing rules)				
1		🖳 10.1.1.0	172.16.1.1	100 http	🕴 Deny	
2		any	Image: state	TP ip	🖌 Permit	
3	· · · · ·	🌍 any	🏟 any	<u>ль</u> ib	🕴 Deny	
🥵 m	anage (2 imp	licit incoming rules)				
1		🌍 any	Any less secure ne	IP ip	🖌 Permit	
2		🌑 any	🏟 any	1e> ip	3 Deny	
	itside (1 impl	licit incoming rule)		+		
1		🌍 any	<li>any</li>	IP ip	3 Deny	
80. – – –						
310 		o se se comencia de la comencia de l		_		

La configuración enviada desde el ASDM da como resultado este conjunto de comandos en

la interfaz de línea de comandos (CLI) del 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

A través de estos pasos, el ejemplo 1 se ha realizado a través de ASDM para bloquear el acceso de la red 10.1.1.0 al servidor web, 172.16.1.1. El ejemplo 2 también se puede lograr de la misma manera para bloquear el acceso de toda la red 10.1.1.0 al servidor FTP,

172.16.1.2. La única diferencia será en el punto de elegir el puerto. **Nota:** Se supone que esta configuración de regla de acceso, por ejemplo, 2, es una configuración nueva.

8. Defina la regla de acceso para bloquear el tráfico FTP y, a continuación, haga clic en la pestaña **Detalles** para elegir el puerto 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. Elija el puerto **ftp** y haga clic en **Aceptar** para volver a la ventana Agregar regla de acceso.

ter:					
Jame	Protocol	Source Ports	Destination Ports	ICMP Type	Description
100 cibrix-ica	tcp	default (1-65535)	1494		
TO ctiqbe	tcp	default (1-65535)	2748		
- 🚾 daytime	tcp	default (1-65535)	13		
ter-discard	top	default (1-65535)	9		
ter domain	top	default (1-65535)	53		
w echo	top	default (1-65535)	7		
TO exec	tcp	default (1-65535)	512		
100 finger	tcp	default (1-65535)	79		
- TOP ftp	top	default (1-65535)	21		—
ttp-data	tcp	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
10 h323	tcp	default (1-65535)	1720		
- 🚾 hostname	tcp	default (1-65535)	101		
ter http	top	default (1-65535)	60		
- KIP https	top	default (1-65535)	443		
- rep ident	top	default (1-65535)	113		
imap4	tcp	default (1-65535)	143		
TO IC	tcp	default (1-65535)	194		
- Rev kerberos	tcp	default (1-65535)	750		
and Marsia	hen	dofoult (1 cccoc)	E49		
lected Service					

10. Haga clic en Aceptar para completar la configuración de la regla de

🖆 Add Acc	ess Rule
Interface:	inside 🔽
Action: 🚫 P	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	tcp/ftp
Description:	
💌 Enable Lo	ogging
Logging L	.evel: Default
More Opti	ions
	OK Cancel Help

11. Agregue otra regla de acceso para permitir cualquier otro tráfico. De lo contrario, la regla Denegar implícita bloqueará todo el tráfico en esta

	🖆 Insert A	fter Access Rule
	Interface:	inside 😽
	Action: 💿 I	Permit 🔿 Deny
	Source:	any
	Destination	any
	Service:	ip
	Description:	
	💽 Enable L	ogging
	Logging I	Level: Default
	More Opt	ions
interfaz.		OK Cancel

12. La configuración completa de la lista de acceso es similar a esta en la pestaña Access Rules (Reglas de acceso).

#	Enabled	Source	Destination	Service	Action
🗟 🖊 i	nside (3 incom	ning rules)			
1	<b>V</b>		I72.16.1.1	🚾 ftp	😮 Den
2		🐔 any	🏟 any	🈰 ip	🗸 Perr
3		🧼 any	🧼 any	ip	🕴 Den
÷ 🥵	nanage (2 imp	licit incoming rules)			
1		🎱 any	Any less secure ne	🥦 ip	🛹 Perr
2		🌍 any	🧼 any	1º/ip	🙆 Den
- 🥦 i	outside (1 impl	licit incoming rule)			
1		🥥 any	any	19 ip	🔕 Den
• 11. 					

13. Haga clic en **Aplicar** para enviar la configuración al ASA. La configuración CLI equivalente tiene el siguiente aspecto:

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

#### Configuración de Apertura de los Puertos

El dispositivo de seguridad no permite ningún tráfico entrante, excepto que esté explícitamente autorizado por una lista de acceso extendido.

Si desea permitir el acceso de un host externo a un host interno, puede aplicar una lista de acceso entrante en la interfaz externa. Debe especificar la dirección traducida del host interno en la lista de acceso porque esta dirección es la que puede utilizarse en la red externa. Siga estos pasos para abrir los puertos desde la zona de seguridad más baja a la zona de seguridad más alta. Por ejemplo, permita el tráfico desde la interfaz externa (zona de seguridad más baja) a la interna (zona de seguridad más alta) o desde la DMZ a la interfaz interna.

1. La NAT estática crea una traducción fija de una dirección real a una dirección asignada. Esta dirección asignada es una dirección que los hosts en Internet pueden utilizar para acceder al servidor de la aplicación de la DMZ sin necesidad de conocer la dirección real del servidor.

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

Consulte la sección <u>NAT Estática</u> de <u>Referencia de comandos para PIX/ASA</u> para obtener más información.

2. Cree una ACL para permitir el tráfico del puerto específico.

```
access-list
```

3. Vincule la lista de acceso con el comando access-group para activarla.

```
access-group
```

#### **Examples:**

- 1. Apertura del tráfico del puerto SMTP: Abra el puerto tcp 25 para permitir que los hosts externos (Internet) accedan al servidor de correo ubicado en la red DMZ.El comando Static asigna la dirección externa 192.168.5.3 a la dirección 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 eq 25 ciscoasa(config)#access-group 100 in interface outside
- 2. Apertura del tráfico del puerto HTTPS: Abra el puerto tcp 443 para permitir que los hosts externos (Internet) accedan al servidor Web (seguro) ubicado en la red DMZ. ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5 netmask 255.255.255.255 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. Autorización del tráfico de DNS: Abra el puerto udp 53 para permitir a los hosts externos (Internet) acceder al servidor DNS (seguro) ubicado en la red DMZ. ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit udp any host 192.168.5.4 eq 53 ciscoasa(config)#access-group 100 in interface outside

Nota: Consulte Puertos IANA para obtener más información sobre las asignaciones de puerto.

#### Configuración mediante ASDM

En esta sección se muestra un enfoque paso a paso para llevar a cabo las tareas antes mencionadas mediante ASDM.

1. Cree la regla de acceso para permitir el tráfico smtp al servidor

Add -	f Edit 🏢 Delete 🛉 🗲
Add Ad	cess Rule.
🔹 Insert.	(s)
🐺 Insert	After
🖃 🥵 inside	(2 implicit incoming rules)
1	🇳 any
2	any

192.168.5.3.

2. Defina el origen y el destino de la regla de acceso y la interfaz con la que esta regla se vincula. Además, defina la acción como

	🖆 Add Access Rule
	Interface: Outside 💌
	Action: O Permit O Deny
	Source: any
	Destination 192.168.5.3
	Service: ip
	Description:
	Enable Logging
	Logging Level: Default 💉
	More Options
Permiso.	OK Cancel Help

3. Elija SMTP como puerto y luego haga clic en

575 BO						
Name		Protocol	Source Ports	Destination Ports	ICMP Type	Descripti
	r pp p	hop	default (1-65535)	514		
	rten	tro	default (1-65535)	554		
	sin	hop	default (1-65535)	5060		
	sete .	tro	(def.w.it (1-65535))	25		1
-	sabet	tro	default (1-65535)	1521		
	sch	top	default (1-65535)	22		
	suproc	tcp	default (1-65535)	111		
1.00	tacars	bon	default (1-65535)	49		
-1207	talk	top	default (1-65535)	517		
10	telast	top	default (1-65535)	23		
10	LUCD	top	default (1-65535)	540		
	whois	top	default (1-65535)	43		
100	hift	udo	default (0-65535)	512		
101	bootor	udp	default (0-65535)	68		
1 10	bootos	udp	default (0-65535)	67		
107	cife	udp	default (0-65535)	3020		
100	discard	udp	default (0-65535)	9		
100	distr	udp	default (0-65535)	195		
100	domain	udp	default (0-65535)	53		
	10.000	10 Geo	<ul> <li>A CARTER CONTRACTOR</li> </ul>			

4. Haga clic en **Aceptar** para completar la configuración de la regla de

🖆 Add Aco	ess Rule
Interface:	outside 🔽
Action: 💿	Permit 🔘 Deny
Source:	any
Destination	192.168.5.3
Service: (	tcp/smtp
Description:	
💽 Enable L	ogging
Logging I	Level: Default
More Opt	ions
	OK Cancel

5. Configure la NAT estática para traducir 172.16.1.3 a 192.168.5.3Vaya a Configuration > Firewall > NAT Rules > Add Static NAT Rule para agregar una entrada NAT



estática.

Seleccione el origen original y la

dirección IP traducida junto con sus interfaces asociadas y luego haga clic en **Aceptar** para finalizar la configuración de la regla NAT

Original		
Interface	DMZ	
Interrace,		
Source:	172.16.1.3	
Translated	na tu	
Interface: (	outside	~
💿 Use IP Address:	192.168.5.3	[-
O Use Interface IP	Address	
Port Address Translatic	on (PAT)	
Enable Port Ac	dress Translation (PAT)	
Protocol;		
Original Port:		
Translated Dev	+	
Translated Por		
Connection Setting	gs	1

imagen representa las tres reglas estáticas que se enumeran en la sección <u>Ejemplos</u>:

Config	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 imagen representa las tres reglas de acceso que se enumeran en la sección <u>Ejemplos</u>:

#	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	nside (2 implic	it incoming rules)			
1		🏟 any	Any less secure ne	IP/ ip	🖌 Permit
2		🧼 any	🏟 any	💷> ip	🔕 Deny
- <b>5</b>	manage (2 imp	licit incoming rules)			
1		🏟 any	Any less secure ne	IP ip	🖌 Permit
2		🏟 any	🌍 any	JE> ip	🕴 Deny
<b>, 54</b> o	outside (4 inco	ming rules)			
1	¥	🧼 any	192.168.5.3	📧 smtp	🖌 Permit
2	$\checkmark$	🍥 any	192.168.5.5	100 https	🖌 Permit
3		🥌 any	192.168.5.4	🚥 domain	💉 Permit
4		any	<ul> <li>any</li> </ul>	IP ip	🔞 Deny

## **Verificación**

Puede verificar con determinados comandos show, como se indica a continuación:

- show xlate: muestra la información de la traducción actual
- show access-list: muestra los contadores de aciertos para las políticas de acceso
- show logging: muestra los registros en el buffer

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

### **Troubleshoot**

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

### Información Relacionada

- PIX/ASA 7.x: Activar/desactivar la comunicación entre interfaces
- PIX 7.0 y Adaptive Security Appliance Port Redirection (Reenvío) con Comandos nat, global, static, conduit y access-list
- Uso de los Comandos NAT, global, static, conduit y access-list y Redirección de Puerto (Reenvío) en PIX
- PIX/ASA 7.x: Ejemplo de Configuración de Habilitar Servicios FTP/TFTP
- PIX/ASA 7.x: Ejemplo de Configuración de Habilitar Servicios VoIP (SIP, MGCP, H323, SCCP)
- PIX/ASA 7.x: Ejemplo de Acceso al Servidor de Correo en la Configuración de DMZ
- Soporte Técnico y Documentación Cisco Systems