ASA 8.2: Redirección de puerto (expedición) con nacional, global, estático, y comandos access-list que usan el ASDM

Contenido

Introducción prerrequisitos Requisitos **Componentes Utilizados Convenciones** Diagrama de la red Permita el Acceso de Salida Permita el Acceso de los Hosts Internos a las Redes Externas con el NAT No prohiba a host interiores el acceso a las redes externas con la PALMADITA Limita el acceso de los Hosts Interiores a las Redes Externas Permita el tráfico entre las interfaces con el mismo nivel de seguridad Permita el Acceso de los Hosts no Confiables a los Hosts de su Red de Confianza Inhabilite NAT para los Hosts/Redes Específicos Redirección (Reenvío) de Puerto con Estático Limite la Sesión TCP/UDP con Estático Lista de Acceso Basada en el Tiempo Información Relacionada

Introducción

Este documento describe cómo funciona la redirección de puertos en Cisco Adaptive Security Appliance (ASA) mediante ASDM. Se ocupa del control de acceso del tráfico mediante el ASA y de cómo funcionan las reglas de traducción.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Descripción general de NAT
- PIX/ASA 7.X: Redirección de puerto

Componentes Utilizados

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

- Versión de ASA 8.2 de las Cisco 5500 Series
- Cisco ASDM versión 6.3

Nota: Esta configuración trabaja muy bien de la versión de software 8.0 a 8.2 de Cisco ASA solamente, porque no hay cambios importantes en la funcionalidad de NAT.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco</u> para obtener más información sobre las convenciones del documento.

Diagrama de la red



Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Permita el Acceso de Salida

El acceso de salida describe las conexiones de una interfaz de mayor nivel de seguridad a una interfaz de menor nivel de seguridad. Esto incluye las conexiones desde el interior al exterior, interior hacia las zonas desmilitarizadas (DMZ) y DMZ hacia el exterior. Esto también puede incluir las conexiones de una DMZ a otra, mientras la interfaz de la fuente de conexión tiene un mayor nivel de seguridad que el destino.

Ninguna conexión puede pasar a través del dispositivo de seguridad sin una regla de traducción configurada. Esta característica se llama <u>NAT control</u>. La imagen mostrada aquí representa cómo inhabilitar esto con el ASDM para permitir las conexiones con el ASA sin ninguna traducción de la dirección. Sin embargo, si usted hace cualquier regla de traducción configurar, después inhabilitar esta característica no sigue siendo válido para todo el tráfico y usted necesitará eximir

explícitamente las redes de la traducción de la dirección.

* Type Source Destination Service Inf	-	Turne	Original			Tran
	#	туре	Source	Destination	Service	Inte
			Tell			
	<					

Permita el Acceso de los Hosts Internos a las Redes Externas con el NAT

Usted podría permitir que un grupo de host interiores/de redes acceda el mundo exterior configurando las reglas dinámicas NAT. Para lograr esto, usted necesita seleccionar a la dirección real de los host/de las redes para ser dados el acceso y entonces tienen que ser asociadas a un pool de los IP Addresses traducidos.

Complete estos pasos para no prohibir a los host interiores el acceso a las redes externas con el NAT:

1. Vaya a la **configuración** > al **Firewall** > a las **reglas NAT**, el tecleo **agrega**, y después elige la opción **dinámica de la regla del agregar NAT** para configurar una regla dinámica

Home 🖧 Configuration 📝 Moni	toring 🔚 Save 🔇 Refresh 🔇 Back 🔘 🕫
Device List 🗇 🕀 🗡	Configuration > Firewall > NAT Rules
🗣 Add <u>î</u> Delete 🚿 Connect	🔂 Add 🗸 📷 Edit 🏢 Delete 🔶 🗲 🐇 🖡
Firewall 라우×	Add Static NAT Rule
En Firewal	Add Dynamic NAT Rule
	Add NAT Exempt Rule
Remote Access VPN	Add Static Policy NAT Rule
Site-to-Site VPN	Add Dynamic Policy NAT Rule
inc.	👷 Insert.,.
1.2	Tinsert After
Device Management	dan dan

NAT.

2. Elija el nombre de la interfaz con la cual los host reales están conectados. Elija el IP Address real de los host/de las redes usando el **botón Details Button** en el campo de **fuente**

terrace:	nside		
urce:			
	ñ		
slated —	1 10 1 11		
lect a glot	al pool for dynamic translat	ion,	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	

3. En este ejemplo, se ha seleccionado la *red interna* entera. Haga Click en OK para completar la

selección.

Name 1 IP Address Netmask Description Object NAT IPv4 Network Objects - IPv4 Network						
Import Network Objects Import Network Objects Import Inside Import Inside Insid	Name	A.1	IP Address	Netmask	Description	Object NAT
Image 0.0000 255.255.255.0 Imanage 10.77.241.64 255.255.255.192 Imanage 209.165.200.0 255.255.255 Imanage 201.1.10 255.255.255 Imanage 172.16.11.1 255.255.255 Imanage 172.16.11.1 255.255.255 Imanage 172.16.11.10 255.255.255 Imanage 109.165.200.10 255.255.255 Imanage 209.16 209.165.200.10 255.255.255	E-IPv4 Net	work Obje	o o o o	0000		
Istoretti. Iteration Iteration Imanage 10.77.241.64 255.255.255.192 Imanage 209.165.200.0 255.255.255.255 Imanage 201.1.10 255.255.255 Imanage 172.16 172.16.11.10 255.255.255 Imanage 172.16.11.10 255.255.255 Imanage Imanage 172.16.11.10 255.255.255 Imanage Imanage 172.16.11.10 255.255.255 Imanage Imanage 172.16.11.10 255.255.255 Imanage Imanage 172.16.12.2 255.255.255.255 Imanage Imanage 209.165.200.10 255.255.255.255 Imanage	- Q a	ny ddae	172 16 11 0	255 255 255 0		
Image Instruction Costastastructure Image 209.165.200.0 255.255.255 Image Image 20.1.1.10 20.1.1.10 255.255.255 Image Image 172.16 172.16.11.1 255.255.255 Image Image Image 172.16 172.16.11.10 255.255.255.255 Image Image Image 172.16 172.16.12.2 255.255.255.255 Image Image Image 172.16 172.16.12.2 255.255.255.255 Image Image Image 209.16 209.165.200.10 255.255.255.255 Image Image		anana	10 77 241 64	255 255 255 192		
Image: Solution in control of solution in the solution of the solution in the solution of the solution		utside.	209.165.200.0	255,255,255,224		
Image: Strain		0.1.1.10	20.1.1.10	255,255,255,255		
Image: style="text-align: center;">Image: style: style="text-align: center;">Image: style=		72.16	172.16.11.1	255.255.255.255		
■ 172.16 172.16.12.2 255.255.255 ■ 209.16 209.165.200.10 255.255.255	1	72.16	172.16.11.10	255.255.255.255		
209.16 209.165.200.10 255.255.255	1	72.16	172.16.12.2	255.255.255.255		
	- 18 2	09.16	209.165.200.10	255.255.255.255		

4. El tecleo **maneja** para seleccionar el pool de los IP Addresses a las cuales la red real será asociada.

nerrace.			
ource:	nside-network/24		
nslated —			
slect a glob	al pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
-0	(inbound)	Same as original address (identity)	E
			Manage
			<u> </u>
	Fallings		

5. El tecleo agrega para abrir la ventana de la agrupación global de direcciones del

Pool ID	Interface	Addresses Pool	

agregar.

6. Elija la opción del **rango** y especifique los IP Addresses que comienzan y de terminaciones junto con la interfaz de egreso. También, especifique un pool único ID y el tecleo **agregan** para agregar éstos a la agrupación de direcciones. Haga Click en OK para volver a la ventana de la agrupación global del manejo.

nterface:	outside		*		
ool ID:	10				
IP Addre	esses to Add				Addresses Pool
Ran	ge	2			🛃 209.165.200.20 - 209.165.200.4
Starti	ng IP Address:	209.165.200.20			
Endin	g IP Address:	209.165.200.40			
Netm	ask (optional):	255.255.255.192		Add >>]
O Port	Address Transi	lation (PAT)		<< Delete	
IP Ad	dress:				J
Netm	ask (optional):				
O Port Add	Address Trans ress of the inte	lation (PAT) using IF rface			

7. Haga Click en OK para volver a la ventana dinámica de la regla del agregar

Pool ID	Interface	Addresses Pool
-10	outside	209.165.200.20 - 209.165.200.40

8. Haga Click en OK para completar la configuración dinámica de la regla NAT.

and a second			
ource: insid	de-network/24		
nslated			
elect a global p	pool for dynamic translati	on.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
-0	(inbound)	Same as original address (identity)	
10	outside	209.165.200.20 - 209.165.200.40	Manage

 El tecleo solicita los cambios para tomar el efecto.Nota: El tráfico del permiso con el Firewall sin la opción de la traducción de la dirección se desmarca

*	Turne	Original			Translated		
•	type	Source	Destination	Service	Interface	Address	Servio
insid	e						
	Dynamic	inside-network/24	1		outside	209.165.200.20 - 209.165.200.40	
1	P S Dynamic	g inside-network/24			lookside	De 209.165.200.20 - 209.165.200.40	

Éste es el CLI equivalente hecho salir para esta Configuración de ASDM:

nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0

Según esta configuración, los host en la red de 172.16.11.0 conseguirán traducidos a cualquier dirección IP del agrupamiento NAT, 209.165.200.20-209.165.200.40. Aquí, el agrupamiento NAT ID es muy importante. Usted podría asignar al mismo agrupamiento NAT a otra red interna/del dmz. Si el pool asociado tiene menos direccionamientos que el grupo real, usted podría ejecutarse de los direccionamientos si es la cantidad de tráfico más que esperada. Como consecuencia, usted podría intentar implementar la PALMADITA o usted podría intentar editar a la agrupación de direcciones existente para extenderla.

Nota: Mientras que hace cualquier modificación a la regla de la traducción existente, observe que usted necesita utilizar el <u>comando clear xlate</u> para que esas modificaciones tomen el efecto. Si

no, seguirá habiendo la conexión existente anterior allí en la tabla de conexiones hasta ellas descanso. Sea prudente al usar el **comando clear xlate**, porque termina inmediatamente las conexiones existentes.

No prohiba a host interiores el acceso a las redes externas con la PALMADITA

Si desea que los host internos compartan a una sola dirección pública para la traducción, use PAT. Si la **sentencia global** especifica una dirección, a esa dirección se le traduce el puerto. El ASA permite una traducción de puerto por los soportes de la interfaz y de esa traducción hasta 65,535 objetos de traducción activos a la sola dirección global.

Complete estos pasos para no prohibir a los host interiores el acceso a las redes externas con la PALMADITA:

1. Vaya a la **configuración** > al **Firewall** > a las **reglas NAT**, el tecleo **agrega**, y después elige la opción **dinámica de la regla del agregar NAT** para configurar una regla dinámica



 Elija el nombre de la interfaz con la cual los host reales están conectados. Elija el IP Address real de los host/de las redes usando el **botón Details Button** en el campo de **fuente**, y elija la **red interna**. El tecleo **maneja** para definir la información de dirección traducida.

Interface:	inside	·····	
Source:	inside-network/24		
inslated Select a gl	obal pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
in U	(outbound)	Same as original address (identity)	and the second s
	LIDDOUIDGI	Same as original address (identity)	F

3. Haga clic en Add

	🔹 Manage (Global Pool	
	Add	Edit 🏢 Delete	
	Pool ID	Interface	Addresses Pool
	-		
(Agregar).			

 Elija el Port Address Translation (PAT) usando la dirección IP de la Opción de interfaz, y el tecleo agrega para agregarla a la agrupación de direcciones. No olvide asignar un ID único para este conjunto de direcciones NAT.

iol ID: 20	
See Street and a second s	
P Addresses to Add Addresses Pool	
O Range	
Starting IP Address:	
Ending IP Address:	
Netmask (optional): Add >>	
Port Address Translation (PAT) << Delete	
IP Address:	
Netmask (optional):	
Port Address Translation (PAT) using IP	

5. Se muestra aquí el pool de la dirección configurada con la interfaz exterior como la única dirección disponible en ese pool. Haga Click en OK para volver a la ventana dinámica de la

	Cuit Delete	
Pool ID	Interface	Addresses Pool
20	outside	🔤 outside

OK.

nterface:	inside	<u> </u>	
ource:	inside-network/24		
nslated -			
elect a glo	bal pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
20	outside	outside	Manage
onnectio	n Settings		

7. La regla dinámica configurada NAT se muestra aquí en cristal la configuración > el Firewall > de las reglas NAT

	Time	Original	Translated			
	туре	Source	Destination	Service	Interface	Address
inside	9					
1	Dynamic	inside-network/24			outside	outside
11		1		1		

Éste es el CLI equivalente hecho salir para esta configuración de la PALMADITA:

```
global (outside) 20 interface
nat (inside) 20 172.16.11.0 255.255.255.0
```

Limita el acceso de los Hosts Interiores a las Redes Externas

Cuando no se define ningunas reglas de acceso, los usuarios de una interfaz de mayor seguridad pueden acceder cualquier recurso asociado a una interfaz de menor seguridad. Para restringir a los ciertos usuarios de acceder ciertos recursos, utilice las reglas de acceso en el ASDM. Este ejemplo describe cómo permitir que un único usuario acceda los recursos exteriores (con el FTP, el S TP, el POP3, el HTTPS, y el WWW) y restrinja todos los demás de acceder los recursos

exteriores.

Nota: Habrá un "implícito niega" la regla en el extremo de cada lista de acceso.

Complete estos pasos:

1. Vaya a la **configuración** > al **Firewall** > a las **reglas de acceso**, el tecleo **agrega**, y elige la opción <u>de la **regla de acceso del agregar** para crear un</u>a nueva entrada de lista de



acceso.

2. Elija la dirección IP de origen que debe ser permitida en el campo de **fuente**. Elija **ningunos** como el destino, **dentro** como de la interfaz, y **permita** como la acción. Pasado, haga clic el **botón Details Button** en el campo del servicio para crear a un grupo de servicios TCP para

🕵 Add Aco	ess Rule
Interface:	inside 💌
Action: 💿	Permit O Deny
Source:	172.16.10.100
Destination	any
Service:	ip 💽
Description:	
🗹 Enable L	ogging
Logging	Level: Default 👻
More Opt	ions
	OK Cancel

los puertos requeridos.

3. El tecleo agrega, y después elige la opción del grupo de servicios



4. Ingrese un nombre para este grupo. Elija cada uno de los puertos requeridos, y el tecleo **agrega** para moverlos a los miembros en el campo del

Existing Service/Service Group:		Members in Grou
Name		Name
- TCP Service Groups	~	ttp ftp
RDP		
-Predefined		
- 199> aol		
ter bgp		
150> chargen		
- Ke ofs	- Series	
- 100 otrix-ica	C 4415	
tiqbe	A00 >	
daytime	<< Rem	ove
100> discard		
102> domain		
techo		
102> exec		
finger		
199 ftp-data		
- 102- gopher	2	
O Carls and and have		
O Create new member:		
Port/Range:		

5. Usted debe ver todos los puertos seleccionados en el campo derecho. El Haga Click en OK para completar el servicio vira la selección hacia el lado de babor del

Group Name:	Permit-172.16.10.100		
Description:			
Existing S	ervice/Service Group;		Members in Gro
Name			Name
- 10	nfs	~	100> ftp
- 10	ento		- 100 ftp-dat
	pcanywhere-data		🗠 🚾 http
- 10	pim-auto-rp		🔤 🚾 https
10	pop2		pop3
10	ppto		to smtp
10	rsh		
10	rtsp	C ad	455
10	sip		
10	sginet	<<1	Remove
10	ssh	-	
	sunrpc		
10	tacacs		
10	⊧ talk	3	
10	telnet		
19	vucp		
10	> whois	~	
O Create ne	w member:		
Port /D por	a+		
Purcikang			

6. Usted puede ver al grupo de servicios configurado TCP aquí. Haga clic en OK.

-iter:					
Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description
😑 🐼 Permit-	1 tcp				
BE ftp	tcp	default (1-65535)	21		
TRE ftp-	data tep	default (1-65535)	20		
- top http	tcp	default (1-65535)	80		
- 👥 http	is top	default (1-65535)	443		
- KP pop	3 tcp	default (1-65535)	110		
TCP smt	p tcp	default (1-65535)	25		
E RDP	tcp				
- Predefined					
- 19> aol	tcp	default (1-65535)	5190		
- 19> bgp	tcp	default (1-65535)	179		
- 102 charge	n tcp	default (1-65535)	19		
- 100> cifs	tcp	default (1-65535)	3020		
- 10 citrix-ic	a tcp	default (1-65535)	1494		
- 19> ctiqbe	tcp	default (1-65535)	2748		
🗠 😥 daytime	e tcp	default (1-65535)	13		
- 100> discard	tcp	default (1-65535)	9		
- 100 domain	tcp	default (1-65535)	53		
- 100 echo	tcp	default (1-65535)	7		
- TOP exec	tcp	default (1-65535)	512		
alastid enable					

7. Haga Click en OK para completar la

interface:	inside 💉
Action: 💿	Permit O Deny
Source:	172.16.10.100
Destination	any 🕘
Service:	Permit-172.16.10.100
Description:	
🗹 Enable L	ogging
Logging	Level: Default 🔽

configuración.

 La regla del acceso configurado se puede considerar bajo interfaz interior en el cristal de la configuración > del Firewall > de las reglas de acceso.

🗭 Add	• 🕼 Edt (🖥 Delete 🛉 🐇 🐰	, 🗈 🏨 - 🛛 Q, Find 🖭	Diagram	Export •	Gear	Hits 🔲 S	5how Log 🧯	Q P
#	Enabled	Source	Destination	Service		Action	Hits	Logging	
i 🥵 i	nside (2 incom	ing rules)							
1	V	172.16.10.100	🐔 any	III Perr	nit-172.1	🎻 Permit			
2	1	🏟 any	any	IP ip	TCP Grou	p: Permit-17	72.16.10.1	00	
5	nside IPv6 (2 i	mplicit incoming rules)			TCP: ftp (21)	-		
1		🦚 any	Any less secure ne	IE- ID	TCP: ftp-o	data (20)			
2		🥥 any	any	It ip	TCP: http	(80) s (443)			
-54 r	nanage (2 imp	licit incoming rules)			TCP: pop	3 (110)			
1		any	Any less secure pe	TP, in	TCP: smtp	(25)			

 Para la facilidad de empleo, usted podría también editar al grupo de servicios TCP directamente en el panel derecho en los servicios que el tecleo de cuadro edita para modificar este grupo de servicios directamente.

> Fire	mail > Access Rules								Addresses Services Time Ranges	
Edt	î Delete 🛧 🗲 .	🕺 🛍 - 🔍 Find 🖽	DiagramExport	- 69 Clear	HRs 🔳	Show Log	Packet	Trace	Services d1 4	×
abled	Source	Destination	Service	Action	Hits	Logging	Time	Description	Add - C Edt Delete Q Where	Lised
(2 incor	ning rules)							Colore Construction of the	Filter: Filter	dear
2	172.16.10.100	et any	30 Permit-172.1	🖌 Pornit		Lansana	Louis	Surger and Street	Name	1
	any	any	.æ∕ip	O Deny			1	Implicit rule	G TCP Service Groups	~
Pv6 (2	implicit incoming rules)								Permit-172.16.10.100	
	any	Any less secure ne	.m. ip	🖌 Pernit				Implicit rule: Per	- 180 Pap	- 11
	any	i any	20 lp	(3 Deny				Implicit rule	- 100 Rp-data	
je (2 ing	plicit incoming rules)								- see http	
	any any	Any less secure ne	je ip	🖌 Pernit				Implicit rule: Per	- 👷 https	
	any	any	ze ip	O Deny				Implicit rule	- mp pop3	
10 IPv6	(2 implicit incoming rules)								the setp	
	any	Any less secure ne	18 ip	🖌 Pernit				Implicit rule: Per	B TR RDP	
	any any	any	je ip	(3 Deny				Implicit rule	Predefined	
t (2 inci	oming rules)								- 100 ad	
2	20.1.1.10	209.165.200.10	THE ROP	🖌 Pernit	S	0		A Station of the	- 189 bgp	
	any	any any	IF ID	O Deny				Implicit rule	- BB- chargen	

10. Reorienta otra vez a la ventana de grupo de servicios del editar TCP. Realice las modificaciones basadas en sus requisitos, y haga clic la **AUTORIZACIÓN** para salvar los cambios.

xisting Service/Service Group:		Members in Group:
Name		Name
-TCP Service Groups	~	r-100> ftp
RDP		- 👥 ftp-data
Predefined		- tee> http
- 100> aol		- 100> https
- 😰 bgp	=	тор рор3
- 📷 chargen		smtp
😰 cifs		
10> citrix-ica		
tiqbe	Add >	>>
- 10 daytime	<< Rem	nove
👷 discard	· · · · · · · · · · · · · · · · · · ·	
- 😥 domain		
10 echo		
to exec		
- 102 finger	IS COLDENTS MADE	
- 100 gopher		
- 100 h323		
- besterne		

11. Se muestra aquí una vista completa del ASDM:

Cisco ASDM 6.3 for ASA 10.77.	241.115										068
Sie Yeve Book Wigerds Window	Dep.							Look Fors			alada
🖞 Home 😪 Canfiguration 💽 Mont	urng 🕞 Save 🧿	Reliesh 🚫 Back (🔾 😵 Helo								CISCO
Device List 🚽 🕈 🛪	Configuration > First	wall > Access Rules						0	Ad	hesses Service	IS Time Ranges
🗣 Add 📋 Delete 🚿 Connect	🗣 Add - 📑 Edk	Debto + 4	1 12 11 · Q mit 1	Dagan ato	ort - 🔗 Char M	95 🛄 5hos	v Log 🔍 Pachet	Trace	Servic		47 Q ×
Firewall d a ×	# Enabled	Source	Destination	Service	Action	Hits La	agging Time	Description	* AH	- 🖪 EN 🔳	Delete G. Where Used
P. trond	🖯 🏓 inside (2 incar	sing rules)						-	Piker:		KerlCharl
CO.	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8, 172, 16, 10, 100	🗇 ary	St Perst-172.	L., Periot	States 2	NEWSCON STREET	in the second	Name		
Exercicite Access VPV	12	i any	🕲 HTY	18-ip	O Deny			Impleit rule	⊕ 1CP	Service Groups	A
<i>(</i> 9)	8 Pmanage (2 ing	slicit incoming rules)							=	Permb-172.16	10.100
Ske-to-Ske VPN	1	ary ary	Any less secure ne	20	📌 Pomit			Depkit rule : F		ion Rp	
1 IPS	<							>		as Rp-data	
30	Access Pule Type	Pot and Poli @ Po	+ Only O IPv6 Only							age http	
Device Management			and Orient							the hites	
			C Anti-	Recei 1	Ataval					- Kito paga	
					Harrenover.				Links	the ship	Y
	a a a a a a a a a a a a a a a a a a a	distances and an)	test 11			116	1/30/11 8:10:17 AM URC

Ésta es la configuración CLI equivalente:

```
object-group service Permit-172.16.10.100 TCP
port-object eq ftp
port-object eq ftp-data
port-object eq www
port-object eq pop3
port-object eq smtp
!
access-list inside_access_in extended permit TCP host 172.16.10.100 any
object-group Permit-172.16.10.100
!
access-group inside_access_in in interface inside
!
Para toda la información sobre implementar el control de acceso, refiéras
```

Para toda la información sobre implementar el control de acceso, refiérase <u>agregan o modifican</u> <u>una lista de acceso con el ASDM GUI</u>.

Permita el tráfico entre las interfaces con el mismo nivel de seguridad

Esta sección describe cómo habilitar el tráfico dentro de las interfaces que tienen los mismos niveles de seguridad.

Estas instrucciones describen cómo habilitar la comunicación de la intra-interfaz.

Esto será útil para el tráfico VPN que ingresa una interfaz, pero después se rutea hacia fuera la misma interfaz. El tráfico VPN pudo ser unencrypted en este caso, o puede ser que sea encriptado nuevamente para otra conexión VPN. Va a la **configuración** > la **configuración de dispositivo** > las **interfaces**, y elige el **tráfico del permiso entre dos o más host conectados con la misma Opción de interfaz**.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Redur
Ethernet0/0	outside	Yes	(209.165.200.2	255.255.255.192	No
Ethernet0/1	inside	Yes	100	172.16.11.10	255.255.255.0	No
Ethernet0/2	manage	Yes	90	10.77.241.115	255.255.255.192	No
Ethernet0/3		No				No
<						
Enable traffic betw	een two or more inter	faces which a s connected t	re configured o the same int	with same security le	vels	

Estas instrucciones describen cómo habilitar la comunicación de la inter-interfaz.

Esto es útil para permitir la comunicación entre las interfaces con los niveles de seguridad iguales. Va a la **configuración** > la **configuración de dispositivo** > las **interfaces**, y elige el **tráfico del permiso entre dos o más interfaces que se configuran con la misma** opción de los **niveles de seguridad**.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Redu
Ethernet0/0	outside	Yes	(209.165.200.2	255.255.255.192	No
Ethernet0/1	inside	Yes	100	172.16.11.10	255.255.255.0	No
Ethernet0/2	manage	Yes	90	0 10.77.241.115	255.255.255.192	No
Ethernet0/3		No				No
< Enable traffic between the second seco	een two or more inter	faces which a	re configured	with same security le	vels	

Éste es el CLI equivalente para ambas configuraciones:

same-security-traffic permit intra-interface
same-security-traffic permit inter-interface

Permita el Acceso de los Hosts no Confiables a los Hosts de su Red de Confianza

Esto se puede alcanzar con la aplicación de una traducción NAT estática y de una regla de acceso de permitir esos host. Usted requiere para configurar esto siempre que un usuario externo quisiera acceder cualquier servidor que se siente en su red interna. El servidor en la red interna tendrá un IP Address privado que no sea routable en Internet. Como consecuencia, usted necesita traducir ese IP Address privado a un IP Address público con una regla NAT estática.

Suponga que usted tiene un servidor interno (172.16.11.5). Para hacer este trabajo, usted necesita traducir este soldado IP del servidor a un IP del público. Este ejemplo describe cómo implementar el NAT estático bidireccional para traducir 172.16.11.5 a 209.165.200.5.

La sección en permitir que el usuario externo acceda a este servidor Web implementando una regla del acceso no se muestra aquí. Un snippet de la descripción CLI se muestra aquí para su comprensión:

access-list 101 permit TCP any host 209.165.200.5 Para más información, refiérase <u>agregan o modifican una lista de acceso con el ASDM GUI</u>.

Nota: Especificar la palabra clave "" permite que cualquier usuario del mundo exterior acceda este servidor. También, si no se especifica para ninguna puertos del servicio, el servidor se puede acceder en cualquier puerto del servicio mientras que eso estancia abierta. Tenga cuidado cuando usted implementa, y le aconsejan limitar el permiso al usuario externo individual y también al puerto requerido en el servidor.

Complete estos pasos para configurar el NAT estático:

1. Vaya a la configuración > al Firewall > a las reglas NAT, el tecleo agrega, y elige agrega la



regla NAT estática.

2. Especifique el IP Address original y la dirección IP traducida junto con sus interfaces asociadas, y haga clic la

Interfaces	inside
Interrace:	inside
Source:	172.16.11.5
Translated	
Interface:	outside
OUse IP Address:	209.165.200.5
O Use Interface IP	Address
Port Address Translation	n (PAT)
🔲 Enable Port Ad	dress Translation (PAT)
Protocol:	TCP UDP
Original Port:	
Translated Port	

3. Usted puede ver la entrada NAT estática configurada aquí. El tecleo **se aplica** para enviar esto al

-		Original			Translated	
#	Type	Source	Destination	Service	Interface	Address
insid	le (1 Static rules, 1 l	Dynamic rules)				
1	Static	S 172.16.11.5			outside	209.165.200.5
2	Dynamic	inside-network/24			outside	outside
81						

Esto es un ejemplo de la descripción CLI para esta Configuración de ASDM:

static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255

!

Inhabilite NAT para los Hosts/Redes Específicos

Cuando usted necesita eximir los host o las redes específicos del NAT, agregue una regla exenta NAT para inhabilitar la traducción de la dirección. Esto permite traducido y los host remotos para iniciar las conexiones.

Complete estos pasos:

1. Vaya a la configuración > al Firewall > a las reglas NAT, el tecleo agrega, y elige agrega la



regla exenta NAT.

2. Aquí, la red interna 172.18.10.0 se ha eximido de la traducción de la dirección. Aseegurese que se ha seleccionado la opción exenta. La dirección exenta NAT tiene dos opciones:Tráfico saliente a las interfaces de menor seguridadTráfico entrante a las interfaces de mayor seguridadLa opción predeterminada está para el tráfico saliente. Haga Click en OK para completar el

Original		
Interface:	inside	6
Source:	172.18.10.0	
Destination:	any	[
○ NAT Exe	mpt inbound traffic from interface	'inside' to higher se
Description -		

Nota: Cuando usted

elige **no exima la** opción, ese host determinado no será eximido del NAT y una regla de acceso separada será agregada con "niega" la palabra clave. Esto es útil en evitar los host específicos del NAT tan exenta que la subred completa, excepto estos host, estará NAT eximido.

3. Usted puede ver la regla exenta NAT para la dirección saliente aquí. El tecleo **se aplica** para enviar la configuración al

	1.100.00				translaced
	туре	Source	Destination	Service	Interface
inside	(1 Exempt rules, 1	1 Static rules, 1 Dynamic rule	es)		A State of the second
1	🚝 Exempt	172.18.10.0	🐔 any		(outbound)
2	1 Static	3 172.16.11.5		-	outside
3	Dynamic	📸 inside-network/24			outside
(2027 B				

es el CLI equivalente hecho salir para su referencia:

access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any !

nat (inside) 0 access-list inside_nat0_outbound

4. Aquí usted puede ver cómo editar la regla exenta NAT para su dirección. Haga Click en OK para que la opción tome el

Action:	Exempt O Do not exempt
Original	
Interface:	inside
Source:	172.18.10.0
Destination:	any
NAT Exe	mpt inbound traffic from interface 'inside' to higher security interfaces

5. Usted puede ahora ver que la dirección se ha cambiado a *entrante*.

rype	Source	Destination	Service	Interface	19 B 19
-				a teattant	
Exempt rules, 1	Static rules, 1 Dynamic rule	is)			
Exempt	B 172.18.10.0	🏟 any		(inbound)	
 Static 	172.16.11.5			outside	B
Dynamic	🛃 inside-network/24			outside	5
	ЦЦ				
	Exempt Static Dynamic	Exempt I 172.18.10.0 Static II 172.16.11.5 Dynamic II inside-network/24 Static II	Exempt Exempt Static Static Dynamic Jinside-network/24		Exempt Inside-network/24 ary (inbound) outside outside

nat (inside) 0 access-list inside_nat0_outbound outside

Nota: De esto, usted puede ver que una nueva palabra clave (afuera) se ha agregado para terminar del **comando nat 0**. Esta característica se llama un **NAT exterior**.

6. Otra manera de inhabilitar el NAT está con la implementación de la identidad NAT. La

identidad NAT traduce un host a la misma dirección IP. Aquí está un ejemplo de NAT estático regular de la identidad, donde el host (172.16.11.20) se traduce a la misma dirección IP cuando se accede del

Interface:	inside	*
Source:	172.16.11.20	
ranslated		
Interface:	outside	~
() Use IP Address:	172.16.11.20	
ort Address Translation Enable Port Add Protocol: Original Port: Translated Port	r (PAT) dress Translation (PAT)	
onnection Setting	5	8
	K Cancel Help	

Redirección (Reenvío) de Puerto con Estático

1

La expedición o la redirección de puerto del puerto es una función útil donde los usuarios externos intentan acceder a un servidor interno en un puerto específico. Para alcanzar esto, traducirán al servidor interno, que tiene un IP Address privado, a un IP Address público que a su vez no se prohiba el acceso para el puerto específico.

En este ejemplo, el usuario externo quiere acceder al servidor SMTP, 209.165.200.15 en el puerto 25. Esto se logra en dos pasos:

- 1. Traduzca al servidor de correo interno, 172.16.11.15 en el puerto 25, al IP Address público, 209.165.200.15 en el puerto 25.
- 2. Permita el acceso al mail server público, 209.165.200.15 en el puerto 25.

Cuando el usuario externo intenta acceder el servidor, 209.165.200.15 en el puerto 25, este tráfico será reorientado al servidor de correo interno, 172.16.11 15 en el puerto 25.

1. Vaya a la configuración > al Firewall > a las reglas NAT, el tecleo agrega, y elige agrega la

6	onfic	juration > Firewall > NAT Rules	
	💠 A	dd 🗸 🕝 Edit 📋 Delete 👌 🗲	X
	111	Add Static NAT Rule	
		Add Dynamic NAT Rule	
		Add NAT Exempt Rule	
	<u>م</u> .	Add Static Policy NAT Rule	P
	@	Add Dynamic Policy NAT Rule	
		Insert	2
	壶	Insert After	

regla NAT estática.

2. Especifique la fuente original y la dirección IP traducida junto con sus interfaces asociadas. Elija el **Port Address Translation (PAT) del permiso**, especifique los puertos que se reorientarán, y haga clic la

Interface:	inside	
Source:	172.16.11.15	
Translated		
Interface:	outside	
💿 Use IP Address:	209.165.200.15	
Port Address Translatis	no (PAT)	
Port Address Translatio	on (PAT) ddress Translation (PAT) TCP O UDP	
Port Address Translation	on (PAT) ddress Translation (PAT) TCP O UDP 25	
Port Address Translation Enable Port Ad Protocol: Original Port: Translated Por	on (PAT) ddress Translation (PAT) TCP OUDP 25 t: 25	

3. La regla configurada del PAT estático se considera aquí:

	Turne	Original			Translated		
	type	Source	Destination	Service	Interface	Address	Servic
1	😅 Exempt	172.18.10.0	any		(outbound)		1.5.5
2	🗐 No Exempt	3 172.20.10.10	any		(outbound)		
3	Static	172.16.11.15		RD smtp	outside	209.165.200.15	🐨 sm
4	• Static	3 172.16.11.5			outside	A 209.165.200.5	
							>

Esto es el CLI equivalente hecho salir:

4. Ésta es la regla de acceso que permite que el usuario externo acceda el servidor smtp del público en

					P Group: smtp-access P: smtp (25)
3		any	any	TRAID	C Denv
2	V	🌑 any	209.165.200.15	smtp-access	; 🖌 🖌 Permit
1	~	🖳 20.1.1.10	🖳 209.165.200.10	RDP	🖌 Permit
i 🥦 out	side (3 inc	oming rules)			
2		🇳 any	🏟 any	IP/ ip	🔇 Deny
09.165 1	.200.15:	🧼 any	Any less secure ne	IP> IP	V Permit

Nota: Aseegurese utilizar los host específicos en vez de usar la **cualquier** palabra clave en la fuente de la regla de acceso.

Limite la Sesión TCP/UDP con Estático

Usted puede especificar el número máximo de conexiones TCP/UDP usando la regla estática. Usted puede también especificar el número máximo de conexiones embrionarias. Una conexión embrionaria es una conexión que es un estado medio abierto. Un número más grande de éstos afectará al funcionamiento del ASA. La limitación de estas conexiones prevendrá ciertos ataques como el DOS y el SYN hasta cierto punto. Para la mitigación completa, usted necesita definir la directiva en el marco del MPF, que está fuera del alcance de este documento. Para más información sobre este tema, refiera a <u>atenuar los ataques a la red</u>.

Complete estos pasos:

1. Haga clic la lengueta de las **configuraciones de la conexión**, y especifique los valores para las cantidades máximas de conexiones para esta traducción

Interrace:	inside
Source:	172.16.11.15
Translated	
Interface:	outside
💽 Use IP Address:	209.165.200.15
O Use Interface IP	Address
Uriginal Port:	t: smtp
Connection Setting	
Connection Setting	is NS replies that match the translation rule

2. Estas imágenes muestran los límites de la conexión para esta traducción estática específica:

Original			Translated		
Source	Destination	Service	Interface	Address	Service
atic rules, 1 Dynamic i	rules)				
A 172.18.10.0	any		(outbound)		
172.20.10.10	any		(outbound)		
₿ 172.16.11.15		ter smtp	outside	209.165.200.15	tto smtp

DNS Rewrite Ma	X TCP Connections	Embryonic Limit	Max LIDB Coppositions	
			Max obe Connections	Randomize Sequer
	100	50	Unlimited	

Esto es el CLI equivalente hecho salir:

Lista de Acceso Basada en el Tiempo

Esta sección se ocupa de implementar las listas de acceso basadas en el tiempo usando el ASDM. Las reglas de acceso pueden ser aplicadas basadas el tiempo. Para implementar esto, usted necesita definir un tiempo-rango que especifique las sincronizaciones por el día/la semana/el mes/año. Entonces, usted necesita atar este tiempo-rango a la regla de acceso requerida. el Tiempo-rango se puede definir de dos maneras:

- 1. Absoluto Define un período de tiempo con Starting Time (Tiempo de inicio) y el tiempo de la conclusión.
- 2. Periódico También conocido como repetirse. Define un período de tiempo que ocurra en los intervalos especificados.

Nota: Antes de que usted configure el tiempo-rango, aseegurese que el ASA se ha configurado con las configuraciones de la fecha y horas correctas mientras que esta característica utiliza las configuraciones del reloj del sistema para implementar. Tener ASA sincronizado con el servidor NTP rendirá resultados mucho mejores.

Complete estos pasos para configurar esta característica con el ASDM:

1. Mientras que define la regla de acceso, haga clic el botón Details Button en el campo del

M Add Acc	inside
Action: 🔿	Permit 💿 Deny
Source:	172.16.10.50
Destination	any 🕘
Service:	ip 🖂
Description:	
🔽 Enable L	ogging
Logging	evel: Default
More Opt	ions
Enable	Rule
Traffic Dire	ection: 🔘 In 💿 Out
Source Ser	vice: (TCP or L
Logging In	terval: 300 seconds
Time Rang	•:
	OK Cancel Help
para crear u	in nuevo tiempo-
e Time Ran	ge
Edt 🏦	Delete

rango de tiempo. 2. El tecleo **agrega** p

ē	😫 Brows	e Time Rang	e	
	Add	🖬 Edit 🏦 De	elete	
	Name	Start Time	End Time	Recurri
rango.				

3. Defina el nombre del rango de tiempo, y especifique Starting Time (Tiempo de inicio) y el tiempo de la conclusión. Haga clic en OK.

me Kange Name: Restrict-Usage							
tart Time	End Time						
O Start now	O Never	end					
Start at	💿 End at	(inclusive)					
Month: February 💌 Day: 05 💌 Year: 2011 💌	Month:	February	*	Day:	06 💌	Year:	2011
Hour: 14 Vinute: 00 V	Hour:	16	V	Mouter	30 🗸		
ecurring Time Ranges You can further constrain the active time of this range by specifyin start and stop time specified.	ig recurring ranges.	The recurri	ng time	ranges	wil be ac	tive wit	hin the
ecurring Time Ranges You can further constrain the active time of this range by specifyin start and stop time specified.	ig recurring ranges.	The recurri	ng time	ranges	wil be ac	tive wit	hin the Add
ecurring Time Ranges You can further constrain the active time of this range by specifyin start and stop time specified.	ig recurring ranges.	The recurri	ng time	ranges	will be ac	tive wit	hin the Add Edit
ecurring Time Ranges You can further constrain the active time of this range by specifyin start and stop time specified.	ig recurring ranges.	The recurri	ng time	ranges	will be ac		hin the Add Edit Delete
ecurring Time Ranges You can further constrain the active time of this range by specifyin start and stop time specified.	ig recurring ranges.	The recurri	ng time	ranges	wil be ac		Add Edit Delete
ecurring Time Ranges You can further constrain the active time of this range by specifyin start and stop time specified.	ig recurring ranges.	The recurri	ng time	ranges	wil be ac		Add Edit Delete

4. Usted puede ver el rango de tiempo aquí. Haga Click en OK para volver a la ventana de la

Res	14:00 05 Fe	16:30 06 F	Kecurring Entries

regla de acceso del agregar.

5. Usted puede ahora ver que el rango de tiempo del Restringir-uso ha estado limitado a esta regla de

nterface:	inside 💌
vetion: O	Permit 💿 Deny
iource:	172.16.10.50
estination	any 🔄
iervice:	ip 🖂
)occirchine -	
vescripcion:	
🗹 Enable L	ogging
Logging	Level: Default 🔛
Logging More Opt	Level: Default 🔛
Logging More Opt	Level: Default 💌 ions : Rule
Logging More Opt	Level: Default ions Rule action: In Out
Logging More Opt I Enable Traffic Dire Source Ser	Level: Default Ions Rule ection: In Out (TCP or UDP servic
Logging More Opt Image District District Source Ser Logging In	Level: Default Ions Rule ection: O In O Out rvice: (TCP or UDP servic terval: 500 seconds

acceso.

esta configuración de la regla de acceso, han restringido al usuario en 172.16.10.50 de usar cualquier recurso de 05/Feb/2011 2 de la tarde a 06/Feb/2011 4.30 PM. Esto es el CLI equivalente hecho salir:

```
time-range Restrict-Usage
  absolute start 14:00 05 February 2011 end 16:30 06 February 2011
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

 Aquí está un ejemplo en cómo especificar un rango de tiempo que se repite. El tecleo agrega para definir un rango de tiempo que se repite.

bne			
(inclusive)			
March 💌	Day:	06 💌	Year: 2011
00	Minute:	30 💌	
	March No.	March V Day: 00 V Minute	March 🖌 Day: 06 🖌 00 🖌 Minute: 30 🖌

7. Especifique las configuraciones basadas en sus requisitos, y haga clic la AUTORIZACIÓN

	on which this recurring range will be active
For example, use this option when y Monday through Thursday, from 8:0	ou want the time range to be active every 0 through 16:59, only.
Days of the Week	
O Every day	
O Weekdays	
O Weekends	
(On these days of the week:	
Mon V Tue V Wed	V Thu V Fri Sat Sun
Daily Start Time	Daily End Time (Inclusive)
Hour 15 V Minute 00 V	Hour 🔯 🗹 Minute 00 🗸
Specify a weekly interval when this r	ecurring range will be active
 Specify a weekly interval when this r For example, use this option when y 	ecurring range will be active ou want the time range to be active
 Specify a weekly interval when this r For example, use this option when y continuously from Monday at 8:00 th 	ecurring range will be active ou want the time range to be active rough Friday at 16:59.
O Specify a weekly interval when this r For example, use this option when y continuously from Monday at 8:00 th Weekly Interval	ecurring range will be active ou want the time range to be active rough Friday at 16:59.
Specify a weekly interval when this is For example, use this option when y continuously from Monday at 8:00 th Weekly Interval From: Monday Y Hour:	ecurring range will be active ou want the time range to be active rough Friday at 16:59.

8. Haga Click en OK para volver de nuevo a la ventana del rango de tiempo.

🚳 Edit Time	e Range											
Time Range N	ame: Restric	ct-Usage										
Start Time						End Time						
Start now						O Never end						
 Start at 	:					💿 End at	(inclusive)					
Month:	February	Y Day:	05 🛩	Year:	2011 💌	Month:	March	~	Day:	06 💌	Year:	201
Hour:	00	Minut	e: 00 💙			Hour:	00	~	Minute:	30 💌		
You can fur start and st weekdays	ther constra top time spec 15:00 throug	in the active offied. offied.	time of th	is range b	y specifying (ecurring ranges.	The recur	ring tim	e ranges	will be ac		Add Edit
			(ОК		ncel H	lelp					

Según esta configuración, han negado el usuario en 172.16.10.50 el acceso a cualquier recurso a partir del 3 PM a 8 PM en todos los días laborables excepto sábado y domingo.

```
!
time-range Restrict-Usage
absolute start 00:00 05 February 2011 end 00:30 06 March 2011
periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

Nota: Si un **comando time-range** hace los valores absolutos y periódicos especificar, después evalúan solamente después que se alcanza la hora de inicio absoluta, y no son más futuros a los **comandos periodic** evaluados después del tiempo absoluto del final se alcanzan.

Información Relacionada

- Página de documentación de Cisco ASA
- Soporte Técnico y Documentación Cisco Systems