Ejemplo de Configuración del Túnel VPN IPsec PIX/ASA (Versión 7.x y Posterior) con Traducción de Dirección de Red

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados** Convenciones **Productos Relacionados** Configurar Diagrama de la red Configuraciones Configuración del Dispositivo de Seguridad PIX y la Lista de Acceso Configuración de PIX Security Appliance y MPF (Modular Policy Framework) Verificación Troubleshoot Comandos de Troubleshooting para Router IPsec Verificación de las asociaciones de seguridad Comandos de Troubleshooting para PIX Información Relacionada

Introducción

Esta configuración de ejemplo demuestra un túnel VPN IPsec a través de un firewall que realiza la Conversión de Dirección de Red (NAT). Esta configuración no funciona con la traducción de direcciones de puerto (PAT) si utiliza versiones del software Cisco IOS® anteriores a la 12.2(13)T, sin incluirla. Este tipo de configuración se puede utilizar para tunelizar el tráfico IP. Esta configuración no se puede utilizar para cifrar el tráfico que no pasa a través de un firewall, como IPX o actualizaciones de ruteo. La tunelización de encapsulación de routing genérico (GRE) es una opción más apropiada. En este ejemplo, los routers Cisco 2621 y 3660 son los extremos del túnel IPsec que se unen a dos redes privadas, con conductos o listas de control de acceso (ACL) en el PIX en medio para permitir el tráfico IPsec.

Nota: NAT es una traducción de direcciones de uno a uno, no debe confundirse con PAT, que es una traducción de varios (dentro del firewall) a uno. Para obtener más información sobre el funcionamiento y la configuración de NAT, consulte <u>Verificación del Funcionamiento de NAT y</u> <u>Troubleshooting de NAT Básico</u> o <u>Cómo Funciona NAT</u>. Nota: Es posible que IPsec con PAT no funcione correctamente porque el dispositivo de punto final del túnel exterior no puede gestionar varios túneles desde una dirección IP. Póngase en contacto con su proveedor para determinar si los dispositivos terminales de túnel funcionan con PAT. Además, en Cisco IOS Software Release 12.2(13)T y posteriores, la función NAT Transparency se puede utilizar para PAT. Para obtener más detalles, consulte <u>Transparencia</u> <u>IPSec NAT</u>. Consulte <u>Soporte para IPSec ESP a través de NAT</u> para obtener más información sobre estas funciones en Cisco IOS Software Release 12.2(13)T y posteriores.

Nota: Antes de abrir un caso con el Soporte Técnico de Cisco, consulte <u>Preguntas Frecuentes</u> <u>sobre NAT</u>, que tiene muchas respuestas a preguntas comunes.

Consulte <u>Configuración de un Túnel IPSec a través de un Firewall con NAT</u> para obtener más información sobre cómo configurar el túnel IPsec a través del firewall con NAT en la versión 6.x de PIX y anteriores.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

 Versión 12.0.7.T del software del IOS de Cisco (hasta la versión 12.2(13)T del software del IOS de Cisco, pero sin incluirla)

Para ver las versiones más recientes, consulte IPSec NAT Transparency.

- Cisco 2621 router
- Router Cisco 3660
- Cisco PIX 500 Series Security Appliance que ejecuta 7.x y superior.

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Productos Relacionados

Este documento también se puede utilizar con Cisco 5500 Series Adaptive Security Appliance (ASA), con la versión de software 7.x o posteriores.

Configurar

En esta sección se presenta la información que puede utilizar para configurar las funciones que describe este documento.

Nota: Para encontrar información adicional sobre los comandos que este documento utiliza, utilice la <u>Command Lookup Tool</u> (sólo<u>para</u> clientes<u>registrados</u>).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



10.3.3.2

Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de Cisco 2621
- <u>Configuración del 3660 de Cisco</u>
- <u>Configuración del Dispositivo de Seguridad PIX y la Lista de Acceso</u>
 - <u>Configuración avanzada de la GUI del administrador de dispositivos de seguridad</u> (ASDM)
 - Configuración de la interfaz de línea de comandos (CLI)
- <u>Configuración de PIX Security Appliance y MPF (Modular Policy Framework)</u>

```
Cisco 2621
<#root>
Current configuration:
 ļ
version 12.0
 service timestamps debug uptime
service timestamps log uptime
 no service password-encryption
 1
hostname goss-2621
 ip subnet-zero
ip audit notify log
ip audit po max-events 100
 isdn voice-call-failure 0
cns event-service server
 I
!--- The IKE policy.
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
 !
crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
crypto map mymap local-address FastEthernet0/1
!--- IPsec policy.
```

```
crypto map mymap 10 ipsec-isakmp
 set peer 99.99.99.2
 set transform-set myset
!--- Include the private-network-to-private-network traffic !--- in the encryption process.
match address 101
 1
controller T1 1/0
 interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 !
interface FastEthernet0/1
ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
!--- Apply to the interface.
crypto map mymap
Т
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
no ip http server
!--- Include the private-network-to-private-network traffic !--- in the encryption process.
access-list 101 permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
line con 0
 transport input none
line aux 0
line vty 0 4
 Т
no scheduler allocate
end
```

Cisco 3660

```
<#root>
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname goss-3660
 1
ip subnet-zero
 1
cns event-service server
 T
!--- The IKE policy.
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0
!--- The IPsec policy.
crypto map mymap 10 ipsec-isakmp
 set peer 99.99.99.12
 set transform-set myset
!--- Include the private-network-to-private-network traffic !--- in the encryption process.
match address 101
 I
interface FastEthernet0/0
ip address 99.99.99.2 255.255.255.0
```

```
no ip directed-broadcast
ip nat outside
 duplex auto
 speed auto
!--- Apply to the interface.
crypto map mymap
 1
interface FastEthernet0/1
ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
ip nat inside
 duplex auto
 speed auto
Т
interface Ethernet3/0
 no ip address
 no ip directed-broadcast
 shutdown
 1
interface Serial3/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 !
interface Ethernet3/1
 no ip address
 no ip directed-broadcast
interface Ethernet4/0
 no ip address
 no ip directed-broadcast
 shutdown
 1
interface TokenRing4/0
 no ip address
 no ip directed-broadcast
 shutdown
 ring-speed 16
 !
!--- The pool from which inside hosts translate to !--- the globally unique 99.99.0/24 network.
```

ip nat pool OUTSIDE 99.99.99.70 99.99.99.80 netmask 255.255.255.0

```
!--- Except the private network from the NAT process.
ip nat inside source route-map nonat pool OUTSIDE
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.1
no ip http server
!--- Include the private-network-to-private-network traffic !--- in the encryption process.
access-list 101 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 101 deny ip 10.3.3.0 0.0.0.255 any
!--- Except the private network from the NAT process.
access-list 110 deny
                     ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 110 permit ip 10.3.3.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
 T
line con 0
 transport input none
 line aux 0
line vty 0 4
 1
 end
```

Configuración del Dispositivo de Seguridad PIX y la Lista de Acceso

Configuración de ASDM 5.0

Complete estos pasos para configurar la versión 7.0 de Firewall PIX mediante ASDM.

1. Consola en el PIX. A partir de una configuración despejada, utilice los mensajes interactivos para habilitar la GUI del Administrador de dispositivos de seguridad avanzada (ASDM) para la administración del PIX desde la estación de trabajo 10.1.1.3.

Bootstrap de PIX Firewall ASDM

Pre-configure Firewall now through interactive prompts [yes]? yes Firewall Mode [Routed]: Enable password [<use current password>]: cisco 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: pix-firewall Domain name: cisco.com IP address of host running Device Manager: 10.1.1.3 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: 10.1.1.3 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

- 2. Desde Workstation 10.1.1.3, abra un explorador web y utilice ADSM (en este ejemplo, https://10.1.1.1).
- 3. Elija Yes en los mensajes de certificado e inicie sesión con la contraseña de habilitación según lo configurado en la <u>configuración de Bootstrap de ASDM de Firewall PIX</u>.
- 4. Si esta es la primera vez que se ejecuta ASDM en el PC, le preguntará si desea utilizar ASDM Launcher o ASDM como una aplicación Java.

En este ejemplo, se selecciona el punto de ejecución de ASDM e instala estos mensajes.

5. Vaya a la ventana de inicio de ASDM y seleccione la ficha Configuration.

Elsco ASDM 5.0 for PIX - 10.1.1.1 File Rules Bearch Options Tools Wizards Help	
Home Configuration Monitoring Back Forward Sear	Cisco Systems rch Refresh Seve Help
- Device Information	Interface Status
General License	Interface IP Address/Mask Line Link Current Kops
Host Name: pipfirewall risco com	inside 10.1.1.1/24 Oup Oup 1
PKVersion: 7.0(0)102 Device Uptime: 0d 0h 3m 53s	
ASDM Version: 5.0(0)73 Device Type: PIX 515E	
Firewall Mode: Routed Context Mode: Single	
Total Flash: 16 MB Total Memory: 64 MB	Deleter an interference of a status investment and a should film a
MDN Status	Traffic Status
IKE Tunnels: 0 IPSec Tunnels: 0	Connections Per Second Usage
System Resources Status CPU CPU Usage (percent) 03 020.28 Memory Memory Usage (MB) 04 48 1020.28 04	10.0 10.0
Syslog Disabled	Contigure ASDM System Filter
Device configuration loaded successfully.	admin> NA (15) 🔤 🙀 🔤 🔂 3/16/05 4:26:28 PM UTC

6. Resalte la Interfaz Ethernet 0 y haga clic en Editar para configurar la Interfaz Externa.

Elisco ASDM	5.0 for PIX - 10.1.1.1	Hain						_O×
Home	Configuration Monitoring	Back For	ward	Q Search	Refresh S	Save Help		Cisco Systems
Features	Configuration > Features > Inter	rfaces						
Interfaces			\$					
B .	Interface	Name E	Inabled	Security Level	IP Address	Subnet Mask	Management Only	MTU Add
Security Policy	Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	No 1	500 Edit
24	Ethernet0		No				No	Delete
VPN VPN Routing								
Device Administration Properties	Enable traffic between two	n or mare inter	fores wi	hich are co	nfigured with sam	me serurity levels		
Wizards -		e of more affier		Apply	Rei	set	A	

7. Haga clic en Aceptar en el indicador de la interfaz de edición.

📷 Warning					×
Æ	Editing interfact connectivity.	e Ethernet0 may caus	e tempora	ry or permanent lo	iss of
		OK			

8. Ingrese los detalles de la interfaz y haga clic en Aceptar cuando haya terminado.

🕵 Edit Interface		×
Hardware Port:	Ethernet0	Configure Hardware Properties
🔽 Enable Interface	🗖 Dedicate this interface to manag	ement only
Interface Name:	outside	
Security Level:	0	
IP Address		
 Use Static IP 	🔿 Obtain Address via DHCP	
IP Address: Subnet Mask:	99.99.99.1 255.255.255.0	
MTU: Description:	1500	
	OK Cancel	Help

9. Haga clic en Aceptar en el prompt Cambio de una Interfaz.



10. Haga clic en Apply para aceptar la configuración de la interfaz. La configuración también se envía al PIX. Este ejemplo utiliza rutas estáticas.

Eisco ASDM 5.0 File Rulas Bea) for arch	PIX - 10.1 Options	.1.1 Tools M	(izards	Help								_D×
Home C	onfie	Guration	Monitorin	<u>_</u>]	Back Fi	Orward	Q Search	Q Refresh	Seve	? Help			CISCO SYSTEMS
Features	Cor	figuration	> Features	: > Interfa	ices								
Interfaces	*	<u></u> 문 후		A CA		51991							
۵.			Interface		Name	Enabled	Security Level	IP Address	Sub	net Mask	Management Only	MTU	Add
Security Policy		Ethernet1			inside	Yes	100	10.1.1.1	255.2	\$5.255.0	No	1500	Edit
NAT		Ethernetü			outside	Yes	0	99.99.99.1	265.2	5.255.0	No	1500	Delete
426 Routing													
Ruiking Blocks													
Device Administration													
Froperties		•										•	
		Enable	traffic betw	een two	or more int	erfaces wi	hich are co	onfigured with sa	ame seci	urity levels			
							Annalis		a not	1			
Wizards /							verta y	R	esei				
							ŀ	admin> N	A (15)	1		3/16/05	4:28:18 PM UTC

11. Haga clic en Routing en la pestaña Features , resalte Static Route y haga clic en Add.



12. Configure la puerta de enlace predeterminada y haga clic en Aceptar.



13. Haga clic en Agregar y agregue las rutas a las redes internas.



14. Confirme que las rutas correctas estén configuradas y haga clic en Apply.



15. En este ejemplo, se utiliza NAT. Quite la marca en la casilla Enable traffic through the firewall without address translation y haga clic en Add para configurar la regla NAT.



16. Configure la red de origen (en este ejemplo se utiliza any). Luego haga clic en Administrar Pools para definir el PAT.

📬 Add Address Ti	ranslation R	ule						x
Use NAT	ΟU	se Policy NAT						
-Source Hos	WNetwork-							7
		Interface:	inside		•			
		IP Address:	0.0.0.0		_			
		Mask:	0.0.0		-			
			10.0.0.0					
			Browse.					
							NAT Options	1
Translate Add	iress on Inter	rface: outsid	le 🔻			-		_
- Translate A	ddress To —							
C ala	Static	IP åddrage:			-			
	Redirect p	ort	1					
	C TOP	Original parts		Translated	(nort:			
	C UDP	onginai port.		Translated	i puit.			
• 📲	Dynamic	Address Pool:	same addr	ess 💌	Man	age Pools.		
	Pool ID		Ado	dress				
	N/A	No address poo	defined					
		OK	Cano	el	Help			

17. Seleccione la interfaz externa y haga clic en Agregar.

📫 Manage Global Ad	dress Pools			x
Global Address P	ools			
Global Address P addresses.	ools are used to	configure Dynamic Network Addr	ress Translatio	n (NAT)
Interface	Pool ID	IP Address(es)		
inside				Add
0010100				Edit
				Delete
	OK	Cancel	Help	

Este ejemplo utiliza una PAT que utiliza la dirección IP de la interfaz.

🚰 Add Global Pool Item	×
Interface: outside 💌 Pool ID: 1	
C Range	
O Port Address Translation (PAT)	
Port Address Translation (PAT) using the IP address of the interface	
IP Address:	
Network Mask (optional):	
OK Cancel Help	

18. Haga clic en Aceptar cuando la PAT esté configurada.

🕵 Manage Global Ad	dress Pools						×
Global Address P	ools						
Global Address Po addresses.	ools are used i	to config	ure Dynamic Net	work Addres:	s Translati	on (NAT)	
Interface	Pool ID		IP Addres	s(es)			
inside outside	1 (99.99.99	.1 (interface PAT)			Add	
						Edit	
						Delete	
	OK	1	Cancel	1 н	ein (
			Cancel		eih		

19. Haga clic en Agregar para configurar la traducción estática.

🔁 Add Address 1	Franslation R	Je				x
Use NAT	r cu	se Policy NAT				
Source Ho	st/Network-					
				_		
		Interface:	inside	<u> </u>		
		IP Address:	0.0.0.0			
		Mask	0.0.0.0	-		
			Browse			
					NAT Options	
Translate Ad	dress on Inte	face: outsid	ie 💌	-		
Translate /	Address To —					
0.11	Static	IP Address:	T]		
	🗖 Redirect p	ort		-		
	C UDP	Original port:	Translated p	ort:		
• 📲	Dynamic	Address Pool:	same address 💌	Manage Pools		
	Pool ID		Address			
	1	99.99.99.1 (inter	face PAT)			
	1					
		ок	Cancel	Help		
	_					

20. Seleccione inside en el menú desplegable Interface (Interfaz) y, a continuación, introduzca IP address 10.1.1.2, subnet mask 255.255.255.255, choose Static (Dirección IP) y, en el campo IP Address (Dirección IP), escriba outside address (Dirección externa) 99.99.99.12. Haga clic en Aceptar cuando haya terminado.

🔂 Add Address Translatio	on Rule				x
O Use NAT	C Use Policy NAT				
Source Host/Netwo	rk				
	Interface:	inside	1		
	IP Address:	10.1.1.2	1		
	Mask:	255 255 255 255	I		
		230.200.200.200	1		
		Browse			
				NAT Options	ĺ
Translate Address on	Interface: outsi	de 💌	-		1
- Translate Address 1	Го —				
• 1 Static	IP Address:	99 99 99 12			
□ Redir	ect port	00.00.00.12			
© TO	CP Original port:	Translated port			
C 🖞 Dynamic	Address Pool:	same address 💌	Manage Pools.		
Pool	D	Address		_	
		1001000			
	OK	Cancel	Help		

21. Haga clic en Apply para aceptar la configuración de la interfaz. La configuración también se envía al PIX.



22. Seleccione Política de seguridad en la pestaña Funciones para configurar la regla de Política de seguridad.

File Rules Sea) for PIX - 1(arch Option	0.1.1.1 ns Too	is Wiza	irds Hel	p								_0 ×
Home C	onfiguration	h Mon	j iloring	Back	Forw	and	Q Search	Q Refresh	Seve	nel Hel)	Cos	CO SYSTEMS
Features	Configurati	ion > Fea	atures > 1	Security P	olicy > Acc	ess Rul	es	-	-	-	_	_	
	C Acces	P 🗹 SS Rules	<u>ц</u> іа Са	A Bules	C Filter	sa i Rules	C Seni	ce Policy Ri	ules				
Interfaces	Show Ru	ules for ir	nterrace:	All Intert	laces	-	Show All	1	012.0				
Escurity Policy	¥ F	Rule Enabled	Action	Soc Hor	urce sbīNetwork		Desti Hosti	Li nation Network	Rule A To Tra	applied Mic	Interface	Service	Add
i des	-		1	🧆 any		•	🏟 any				inside (outbourd)	🚥 ip	Edit
											(ourseling)		Delete
VPN													
*23													
Routing													
Building Blocks													
2													
Device Administration													
Properties													
	I Allo	ow traffic		Deny	traffic					€ sh	ow Summary	C Show Detail	
Witardo					Ap	iply	1	Reset		Advar	nced		
Theards 7	1						<3	dmin>	NA (15)		B	🔒 3/1 6/05 4:4	7:48 PM UTC

23. Haga clic en Agregar para permitir el tráfico esp y haga clic en Aceptar para continuar.

🔂 Add Access Rule	x
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface ▼	Time Range
Source Host/Network	Destination Host/Network
Interface: Outside 💌	Interface: inside 💌
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255.255	Mask: 255.255.255.255 💌
Rule applied to traffic incoming to B 99.99.99.2 Allow t	o source interface
Protocol and Service	
C TCP C UDP C ICMP © IP IP Protocol IP protocol: esp	Manage Service Groups
Please enter the description below (optional):	
Access Rule to Allow ESP traffic	
ОК Са	ncel Help

24. Haga clic en Agregar para permitir el tráfico ISAKMP y haga clic en Aceptar para continuar.

📧 Edit Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range Time Range: Not Applied 💌 New
Source Host/Network	Destination Host/Network
	IP Address C Name C Group
Interface: outside	Interface: Inside
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255.255	Mask: 255.255.255.255
99.99.99.2 outside	affic
Protocol and Service	
C TCP © UDP C ICMP C IP Source Port © Service = Isakmp	Manage Service Groups Destination Port Service = any
C Service Group	C Service Group
Please enter the description below (optional):	
Access Rule to allow ISAKMP to host 99.99.99.12	×
OK Can	icel Help

25. Haga clic en Add para permitir el tráfico del puerto UDP 4500 para NAT-T y haga clic en OK para continuar.

🔁 Edit Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range Time Range: Not Applied 💌 New
Source Host/Network	Destination Host/Network
	CIP Address C Name C Group
Interface: Outside 💌	Interface: inside
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255.265	Mask: 255.255.255.255
99.99.99.2 outside	99.99.99.12
Protocol and Service	
C TCP C UDP C ICMP C IP Source Port Service = 4500	Manage Service Groups Destination Port Service = any Service Group
Please enter the description below (optional):	
Access Rule to allow 4500 to host 99.99.99.12	×
OK Car	Help

26. Haga clic en Apply para aceptar la configuración de la interfaz. La configuración también se envía al PIX.

E Cisco ASDM 5.0 for PIX - 10.1.1.1 File Rules Search Options Tools Wizards Help			
Image: Second	ISCO SYSTEMS		
Features Configuration > Features > Security Policy > Access Rules			
* * * III IIII IIII IIIIIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII			
Hierfaces Chow Bules for Interfaces Chow Bules for Interfaces Chow Bules Chow Bules for Interfaces Chow Bules			
	- And -		
Security Policy # Rule Action Source Destination Rule Applied Interface Service	ADO		
NAT · · · · · · · · · · · · · · · · · · ·	Edit		
1 🔽 🖌 🗟 99.99.99.2 🗟 99.99.99.12 🖓 incoming outside 🍱 esp	Delete		
VPN Z Z A State St	8		
Rouing Rouing Building Blocks Device Administration Image: Second state of the second			
Apply Reset Advanced			
Wizards ∧ → → → → → → → → →	54:59 PM UTC		

27. La configuración ha finalizado.

Elija File > Show Running Configuration in New Window para ver la configuración de CLI.

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		

Configuración de Firewall de PIX

Firewall PIX
<#root>
pixfirewall#
show run
: Saved
: PIX Version 7.0(0)102
names !
interface Ethernet0
nameif outside
security-level 0 in address 99 99 99 1 255 255 0
!
interface Ethernet1
nameif inside

```
security-level 100
 ip address 10.1.1.1 255.255.255.0
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
ftp mode passive
access-list outside_access_in remark Access Rule to Allow ESP traffic
access-list outside_access_in
            extended permit esp host 99.99.99.2 host 99.99.99.12
access-list outside_access_in
            remark Access Rule to allow ISAKMP to host 99.99.99.12
access-list outside_access_in
            extended permit udp host 99.99.99.2 eq isakmp host 99.99.99.12
access-list outside_access_in
            remark Access Rule to allow port 4500 (NAT-T) to host 99.99.99.12
access-list outside_access_in
                    extended permit udp host 99.99.99.2 eq 4500 host 99.99.92.12
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask 255.255.255.255
access-group outside_access_in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.3 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
I
```

```
class-map inspection_default
match default-inspection-traffic
ļ
policy-map asa_global_fw_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
ļ
service-policy asa_global_fw_policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e
: end
```

Configuración de PIX Security Appliance y MPF (Modular Policy Framework)

En lugar de la lista de acceso, utilice el comando inspect ipsec-pass-thru en MPF(Modular Policy Framework) para pasar el tráfico IPsec a través de los dispositivos de seguridad PIX/ASA.

Esta inspección está configurada para abrir agujeros de conexión para el tráfico ESP. Se permiten todos los flujos de datos ESP cuando existe un flujo de reenvío y no hay límite en el número máximo de conexiones que se pueden permitir. AH no está permitido. El tiempo de espera inactivo predeterminado para flujos de datos ESP está establecido de forma predeterminada en 10 minutos. Esta inspección se puede aplicar en todas las ubicaciones en las que se pueden aplicar otras inspecciones, lo que incluye los modos de comando class y match. La inspección de aplicación de paso a través de IPSec proporciona una cómoda travesía del tráfico ESP (protocolo IP 50) asociado a una conexión IKE UDP puerto 500. Evita la larga configuración de la lista de acceso para permitir el tráfico ESP y también proporciona seguridad con tiempo de espera y conexiones máximas. Utilice los comandos class-map, policy-map y service-policy para definir una clase de tráfico, para aplicar el comando inspect a la clase y para aplicar la política a una o más interfaces. Cuando está habilitado, el comando inspect IPSec-pass-thru permite tráfico ESP ilimitado con un tiempo de espera de 10 minutos, que no es configurable. Se permite el tráfico XAT y no NAT.

<#root>

hostname(config)#

access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#
class-map test-udp-class
hostname(config-cmap)#
match access-list test-udp-acl
hostname(config)#
policy-map test-udp-policy
hostname(config-pmap)#
class test-udp-class
hostname(config-pmap-c)#
inspect ipsec-pass-thru
hostname(config)#
service-policy test-udp-policy interface outside

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta <u>Output Interpreter</u> (sólo para clientes registrados) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

- show crypto ipsec sa-Muestra las asociaciones de seguridad de fase 2.
- show crypto isakmp sa Muestra las asociaciones de seguridad de la fase 1.
- show crypto engine connections active—Muestra los paquetes cifrados y descifrados.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos de Troubleshooting para Router IPsec

Nota: Consulte Información importante sobre los comandos de depuración antes de utilizar este tipo de comandos.

- · debug crypto engine: muestra el tráfico que está cifrado.
- debug crypto ipsec Muestra los IPSec Negotiations de la Fase 2.

• debug crypto isakmp: muestra las negociaciones de la fase 1 del Protocolo ISAKMP (Internet Security Association and Key Management Protocol).

Verificación de las asociaciones de seguridad

- clear crypto isakmp: borra las asociaciones de seguridad de Intercambio de claves de Internet (IKE).
- clear crypto ipsec sa: borra las asociaciones de seguridad IPsec.

Comandos de Troubleshooting para PIX

La herramienta <u>Output Interpreter</u> (sólo para clientes registrados) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

Nota: Consulte Información importante sobre los comandos de depuración antes de utilizar este tipo de comandos.

- logging buffer debugging—Muestra las conexiones que se establecen y las que se deniegan a los hosts que atraviesan el PIX. La información se almacena en el buffer de registro PIX y el resultado se puede ver usando el comando show log.
- ASDM se puede utilizar para habilitar el registro y también para ver los registros como se muestra en estos pasos.
- 1. Elija Configuration > Properties > Logging > Logging Setup > Enable Logging y luego haga clic en Apply.

File Rules Se.	D for PIX - 10.1.1.1 arch Options Tools Wizards	Help	_0×
Home C	onfiguration Montoring	Sack Forward Search Refresh Save Help	ÖYSTENS
Features	Configuration > Features > Prop	erties > Logging > Logging Setup	
Interfaces Security Policy NAT Security Policy NAT Security Routing Building Blocks Device Activities		Example 1 Sector Enable logging Enable logging Enable logging on the failover standby unit Send debug messages as systags Send systags in EMBLEM format Logging to Internal Buffer Specify the size of the internal buffer to which systags will be saved. When the buffer fills up, it was a convertible. Buffer Size: 4095 bytes You can choose to save the buffer contents before the buffer is overwritten. Save Buffer To: FTP Server Configure FTP Settings Flash Configure FIP Settings ASDM Logging Specify the size of the queue for systags intended for viewing in ASDM.	d orili
Properties		Queue Size: 100	
Wizards /	Priority Gueue	Apply Reset	
		≪admin> NA (15) 🚑 🔂 🔒 3/1 8/05 5:03:38	PM UTC

2. Elija Monitoring > Logging > Log Buffer > On Logging Level > Logging Buffer, a continuación, haga clic en View.



Este es un ejemplo de Log Buffer.

Log But This scri	ter een shows syslog mess	es in ASDM logging buffer as of now.		
Find text	in messages below.	Find Next	t	
Severity	Time			
<mark>4</mark> 6	Mar 16 2005 17:06:11	05005: Login permitted from 10.1.1.3	3/1247 to inside:10.1.1.1/https for user "enable	
<u>i</u> 6	Mar 16 2005 17:05:47	09001: Built local-host inside:10.1.1.	2	
<u>i</u> 6	Mar 16 2005 17:05:47	09001: Built local-host outside:99.99	.99.2	
<u>i</u> 6	Mar 16 2005 17:05:47	05005: Login permitted from 10.1.1.3	3/1220 to inside:10.1.1.1/https for user "enable	
<u>i</u> 6	Mar 16 2005 17:05:47	302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t		
<u>i</u> 6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10.		
<u>i</u> 6	Mar 16 2005 17:05:47	605005: Login permitted from 10.1.1.3/1221 to inside:10.1.1.1/https for user "enable"		
<u>i</u> 6	Mar 16 2005 17:05:47	302013: Built inbound TCP connection 50 for inside:10.1.1.3/1221 (10.1.1.3/1221) t		
<u>i</u> 6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 48 for inside:10.1.1.3/1220 to NP Identity Ifc:10.		
<u>a</u> 4	Mar 16 2005 17:05:47	106023: Deny udp src outside:99.99.99.2/4500 dst inside:99.99.99.12/4500 by acce		
<u>i</u> 6	Mar 16 2005 17:05:47	302015: Built inbound UDP connection 49 for outside:99.99.99.2/500 (99.99.99.2/5)		
<u>i</u> 6	Mar 16 2005 17:05:47	609001: Built local-host inside:10.1.1.2		
<u>i</u> 6	Mar 16 2005 17:05:47	09001: Built local-host outside:99.99	.99.2	
<u>i</u> 6	Mar 16 2005 17:05:47	05005: Login permitted from 10.1.1.3	3/1220 to inside:10.1.1.1/https for user "enable	
16	Mar 16 2005 17:05:47	02013: Built inbound TCP connection	n 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t	
<u>i</u> 6	Mar 16 2005 17:05:47	02014: Teardown TCP connection 47	7 for inside:10.1.1.3/1219 to NP Identity Ifc:10.	
<u>i</u> 6	Mar 16 2005 17:05:46	05005: Login permitted from 10.1.1.3	3/1219 to inside:10.1.1.1/https for user "enable	
έ.6	Mar 16 2005 17:05:46	02013: Built inbound TCP connection	n 47 for inside:10.1.1.3/1219 (10.1.1.3/1219) t	
<u>i</u> 6	Mar 16 2005 17:05:46	02014: Teardown TCP connection 46	6 for inside:10.1.1.3/1218 to NP Identity Ifc:10.	
16	Mar 16 2005 17:05:46	05005: Login permitted from 10.1.1.3	3/1218 to inside:10.1.1.1/https for user "enable	
<u>i</u> 6	Mar 16 2005 17:05:46	02013: Built inbound TCP connection	n 46 for inside:10.1.1.3/1218 (10.1.1.3/1218) t	
<u>i</u> 6	Mar 16 2005 17:05:46	02014: Teardown TCP connection 45	5 for inside:10.1.1.3/1217 to NP Identity Ifc:10.	
<u>i</u> 6	Mar 16 2005 17:05:46	05005: Login permitted from 10.1.1.3	3/1217 to inside:10.1.1.1/https for user "enable	
<u>i</u> 6	Mar 16 2005 17:05:46	302013: Built inbound TCP connection 45 for inside:10.1.1.3/1217 (10.1.1.3/1217) t		
<u>1</u> 6	Mar 16 2005 17:05:46	02014: Teardown TCP connection 44	4 for inside:10.1.1.3/1216 to NP Identity Ifc:10.	
<u>1</u> 6	Mar 16 2005 17:05:46	05005: Login permitted from 10.1.1.3	3/1219 to inside:10.1.1.1/https for user "enabl	
•			Þ	
	1			
1	Refresh Save	g As Clear	Close Help	

Información Relacionada

- Página de Soporte de IPSec Negotiation/IKE Protocols
- Página de Soporte de PIX
- Referencias de Comando PIX
- Página de Soporte de NAT
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).