Configuración de un túnel ISec entre un Firewall PIX de Cisco Secure y un Firewall NG de punto de control.

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Diagrama de la red **Convenciones** Configure el PIX Configuración del punto de control NG Verificación Verificar la configuración de PIX Ver el estado del túnel en el punto de control NG Troubleshoot Resolución de Problemas de la Configuración PIX Resumen de la red Ver registros NG de punto de control Información Relacionada

Introducción

Este documento muestra cómo configurar un túnel IPsec con claves previamente compartidas para comunicarse entre dos redes privadas. En este ejemplo, las redes que se comunican son la red privada 192.168.10.x dentro del Cisco Secure PIX Firewall y la red privada 10.32.x.x dentro del CheckpointTM Next Generation (NG) Firewall.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El tráfico desde dentro del PIX y dentro del NG ^{CheckpointTM} a Internet (representado aquí por las redes 172.18.124.x) debe fluir antes de iniciar esta configuración.
- Los usuarios deben conocer el IPSec Negotiation. Este proceso se puede dividir en cinco pasos, incluidas dos fases de intercambio de claves de Internet (IKE).Un túnel IPSec es

iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPSec.En la Fase 1 IKE, las entidades pares IPSec negocian la política establecida de la Asociación de seguridad (SA) IKE. Una vez que se autentican los pares, se crea un túnel seguro por medio de la Asociación de Seguridad en Internet y del Protocolo de administración de clave (ISAKMP).En la fase 2 de IKE, los pares IPSec usan el túnel autenticado y seguro para negociar las transformaciones de IPSec SA. La negociación de la política compartida determina el modo en que se establece el túnel IPSec.Se crea el túnel IPSec y los datos se transfieren entre los pares IPSec según los parámetros IPSec configurados en los conjuntos de transformaciones de IPSec.El túnel IPSec termina cuando los IPSec SAs son borrados o cuando caduca su vigencia.

Componentes Utilizados

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

- Versión 6.2.1 del software PIX
- Firewall NG CheckpointTM

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

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

Configure el PIX

Esta sección le presenta la información necesaria para configurar las funciones descritas en este documento.

Configuración de PIX
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100

enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname PIXRTPVPN domain-name cisco.com fixup protocol ftp 21 fixup protocol http 80 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol ils 389 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol smtp 25 fixup protocol sqlnet 1521 fixup protocol sip 5060 fixup protocol skinny 2000 names !--- Interesting traffic to be encrypted to the Checkpoint™ NG. access-list 101 permit ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0 !--- Do not perform Network Address Translation (NAT) on traffic to the Checkpoint™ NG. access-list nonat permit ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0 pager lines 24 interface ethernet0 10baset interface ethernet1 10full mtu outside 1500 mtu inside 1500 ip address outside 172.18.124.158 255.255.255.0 ip address inside 192.168.10.1 255.255.255.0 ip audit info action alarm ip audit attack action alarm pdm history enable arp timeout 14400 global (outside) 1 interface !--- Do not perform NAT on traffic to the Checkpoint™ NG. nat (inside) 0 access-list nonat nat (inside) 1 0.0.0.0 0.0.0.0 0 0 route outside 0.0.0.0 0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius aaa-server LOCAL protocol local no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable !--- Permit all inbound IPsec authenticated cipher sessions. sysopt connection permit-ipsec no sysopt route dnat !--- Defines IPsec encryption and authentication algorithms. crypto ipsec transform-set rtptac esp-3des esp-md5-hmac !--- Defines crypto map. crypto map rtprules 10 ipsecisakmp crypto map rtprules 10 match address 101 crypto map rtprules 10 set peer 172.18.124.157 crypto map rtprules 10 set transform-set rtptac !--- Apply crypto map on the outside interface. crypto map rtprules interface outside

isakmp enable outside
! Defines pre-shared secret used for IKE
authentication. isakmp key ******** address
172.18.124.157 netmask 255.255.255.255
! Defines ISAKMP policy. isakmp policy 1
authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5
: end

Configuración del punto de control NG

Los objetos y reglas de red se definen en el NG ^{CheckpointTM} para formar la política que pertenece a la configuración de VPN que se va a configurar. Esta política se instala luego mediante el Editor de políticas ^{CheckpointTM} NG para completar el lado ^{CheckpointTM} NG de la configuración.

 Cree los dos objetos de red para la red de punto de control y la red de firewall PIX que cifran el tráfico interesante.Para hacer esto, seleccione Manage > Network Objects, luego seleccione New > Network. Ingrese la información de red adecuada y luego haga clic en Aceptar.Estos ejemplos muestran una configuración de objetos de red llamados CP_Inside (red interna de ^{CheckpointTM} NG) y PIXINSIDE (red interna de

Network Properti	es - CP_inside		<u>×</u>
General NAT			
<u>N</u> ame:	CP_inside		
IP <u>A</u> ddress:	0.32.0.0		
Net <u>M</u> ask:	255.255.128.0]	
Comment:	PINSIDE		
Color:			
Broadcast a	ddress: I O N <u>o</u> t included]	
		-	
	OK Cancel	Help	

Network Proper	ties - PIXINSIDE	×
General NAT	1	
<u>N</u> ame:	PIXINSIDE	
IP <u>A</u> ddress:	192.168.10.0	
Net <u>M</u> ask:	255.255.255.0	
<u>C</u> omment:	Pixinside	
Color:		
■Broadcast	address: ed <u>O</u> N <u>o</u> t included	
	OK Cancel	Help

2. Cree objetos de estación de trabajo para el NG y PIX ^{CheckpointTM}. Para hacer esto, seleccione Manage > Network Objects > New > Workstation. Tenga en cuenta que puede utilizar el objeto de estación de trabajo NG ^{CheckpointTM} creado durante la ^{configuración NG} inicial de ^{CheckpointTM}. Seleccione las opciones para configurar la estación de trabajo como Gateway y dispositivo VPN interoperable y, a continuación, haga clic en Aceptar. Estos ejemplos muestran una configuración de objetos llamada ciscocp (CheckpointTM NG) y PIX (PIX

Firewall).

Workstation Properties - o	ciscocp			×
Workstation Properties - o General Topology NAT VPN Authentication Management I Advanced	ciscocp General Name: IP Address: Color: Type:	ciscocp 172.18.124.157 Checkpoint External IP C Host © Gateway	<u>G</u> et address	X
	Check Point	Products int products installed: Version NG ireWall-1 o-1 ver anagement Station	i 🔽 Get Version]]
	Object Managed Managed Secure Interr Communic	gement	al) xtemal) cocppvzfoa	
		ОК	Cancel	Help

W	orkstation Properties -	PIX			×
	General Topology	General			
	- NAT	<u>N</u> ame:	PIX		
	- VPN - Advanced	IP <u>A</u> ddress:	172.18.124.158	<u>G</u> et address	
		Comment:	PIX Firewall		
		Color:			
		Туре:	⊂ <u>H</u> ost ⊙ Gate <u>w</u> ay		
		Check Point F	Products		
		Check Po	int products installed: Version NG	i 💌 Get Version	
		□VPN-1 & F □FloodGate □Policy Ser □Managem	ireWall-1 -1 ver ent Station	×	
		Object Manaç	pement		
		C Managed	by this Management Server [Interna	al)	
		C Managed	by another Management Server (Ex	(temal)	
		✓ Interoper	rable ⊻PN Device		
			ОК	Cancel	Help

3. Seleccione Administrar > Objetos de red > Editar para abrir la ventana Propiedades de la estación de trabajo para la estación de trabajo CheckpointTM NG (ciscocp en este ejemplo).Seleccione Topology en las opciones del lado izquierdo de la ventana y luego seleccione la red que desea cifrar. Haga clic en Editar para establecer las propiedades de la interfaz.

Workstation Properties - ci	scocp				×
General Topology NAT VPN	G et Interfaces	Påddrass	Network Mask	IP åddresses behins	
- Authentication - Management ∙ Advanced	E100B0 1 E100B1 1	10.32.50.50 172.18.124.157	255.255.128.0 255.255.255.0	CP_inside External	
	▲dd	Edit	Bemove S sed on Topology	how Show Show	
	E <u>x</u> portable for Sec	cuRemote	ОК С	ancel Help	

4. Seleccione la opción para designar la estación de trabajo como interna y especifique la dirección IP adecuada. Click OK.En esta configuración, CP_inside es la red interna del ^{CheckpointTM} NG. Las selecciones de topología que se muestran aquí designan la estación de trabajo como interna y especifican la dirección como

1	Interface Properties 📉 🔀
	General Topology QoS
	Topology
	External (leads out to the internet)
	Internal (leads to the local network)
	IP Addresses behind this interface:
	C <u>N</u> ot Defined
	Network defined by the interface IP and Net Mask
	Specific: ↓ CP_inside
	Anti-Spoofing
	Perform Anti-Spoofing based on interface topology
	Spoof Tracking: O None I og O Alert
	OK Cancel Help

- CP_inside.
- 5. En la ventana Propiedades de la estación de trabajo, seleccione la interfaz exterior en el NG ^{CheckpointTM} que conduce a Internet y, a continuación, haga clic en **Editar** para establecer las propiedades de la interfaz. Seleccione la opción para designar la topología como externa y luego haga clic en

Interface Properties X
General Topology QoS
Topology
 External (leads out to the internet)
O Internal (leads to the local network)
IP Addresses behind this interface:
C Not Defined
C Network defined by the interface IP and Net Mask
O <u>S</u> pecific:
Anti-Spoofing
Spoof Tracking: O None 💿 Log O Alert
OK Cancel Help

Aceptar.
 6. En la ventana Propiedades de la estación de trabajo en el NG ^{CheckpointTM}, seleccione VPN de las opciones del lado izquierdo de la ventana y, a continuación, seleccione los parámetros IKE para los algoritmos de cifrado y autenticación. Haga clic en Edit para configurar las propiedades

IKE.

Workstation Properties -	ciscocp			×
General Topology NAT VPN Authentication Management € Advanced	VPN Encryption schemes	set default <u>I</u> KE pro	perties	
	Nickname DN ▲dd	Edit	ertificate Authority Eemove	

 Configure las propiedades IKE:Seleccione la opción para el cifrado 3DES para que las propiedades IKE sean compatibles con el comando isakmp policy # encryption 3des.Seleccione la opción para MD5 para que las propiedades IKE sean compatibles con el comando crypto isakmp policy # hash

General Support key exchange encryption with: DES CAST 3DES Support authentication methods: Pre-Shared Secret Edit Secrets Public Key Signatures Specify VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)	IKE Properties	
Support key exchange encryption with: Support data integrity with: DES MD5 CAST SHA1 Support authentication methods: Support authentication methods: Pre-Shared Secret Edit Secrets Public Key Signatures Specify VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)	General	
□ Image: DES Image: MD5 □ Image: CAST Image: MD5 Image: Support authentication methods: Image: SHA1 Image: Support authentication methods: Image: SHA1 Image: Pre-Shared Secret Edit Secrets Image: Public Key Signatures Specify	Support key exchange encryption	with:
□ Image: CAST □ SHA1 Image: Support authentication methods: Image: Shared Secret Image: Pre-Shared Secret Edit Secrets Image: Pre-Shared Secret Edit Secrets Image: Public Key Signatures Specify Image: WPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)	DES DES	
Support authentication methods: ✓ ✓ Pre-Shared Secret Edit Secrets ✓ Public Key Signatures ✓	CAST	
Support authentication methods: Pre-Shared Secret Edit Secrets Public Key Signatures Specify VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)		SHA <u>1</u>
✓ Pre-Shared Secret Edit Secrets □ Public Key Signatures Specify □ ⊻PN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)	Support authentication methods: -	J [
□ Public Key Signatures Specify □ ⊻PN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)	✓ Pre-Shared Secret	Edit Secrets
	Dublic Key Signatures	Gracific
L VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)		ogeory
		cation for SecuRemote (Hybrid Mode)
		<u>A</u> dvanced
<u>A</u> dvanced		Cancel Help
<u>A</u> dvanced OK Cancel Help		

8. Seleccione la opción de autenticación para Secretos Previamente Compartidos, luego haga clic en Editar Secretos para establecer la clave previamente compartida como compatible con el comando PIX **isakmp key key address** address address netmask netmask. Haga clic en Editar para introducir la clave como se muestra aquí y haga clic en Establecer,

Shar	ed Secret		2	×
Г ⁹	Shared Secrets List: -		,	
	Peer Name	Shared Secret		
		****	<u>E</u> dit	
			Berrau	
			<u><u>H</u>emove</u>	
		·····		
	Enter secret: cisco	ortpSet		
_	OK	Cancel	<u>H</u> elp	

Aceptar.

9. En la ventana de propiedades IKE, haga clic en **Avanzadas...** y cambie estos parámetros:Anule la selección de la opción **Support agresive mode**.Seleccione la opción para el **intercambio de claves Support para subredes**.Haga clic en **Aceptar** cuando haya

Advanced IKE properties			×
Use <u>U</u> DP encapsulation	UDP VPN1_IPSE	C_encapsi 🔽	
Support Diffie-Hellman groups	,		
	☐Group 1 (768 ✔Group 2 (1024 ☐Group 5 (1538	bit) 4 bit) 5 bit)	
Rekeying Parameters	, 		
Renegotiate IKE security associat	ions	1440 🚦	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 🗦	Seconds
Renegotiate IPSEC Security a	ssociations every	50000 🚊	KBytes
Misc Support IP <u>c</u> ompression for Se Support <u>agg</u> resive mode Support key exchange for <u>s</u> ub	ecureClient mets		
OK C	ancel	<u>H</u> elp	

- terminado.
- 10. Seleccione Administrar > Objetos de red > Editar para abrir la ventana Propiedades de estación de trabajo para el PIX. Seleccione Topology en las opciones del lado izquierdo de la ventana para definir manualmente el dominio VPN.En esta configuración, PIXINSIDE (red interna de PIX) se define como el dominio VPN.

Workstation Properties - PIX	k internet				×
General	Topology	1			
- NAT	<u>G</u> et Interfaces				
- VPN - Advanced	Name	IP Address	Network Mask		
	Add	Edit	<u>B</u> emove	Show	- -
	Show all IPs beh	ind Gateway es <u>b</u> ehind Gateway b	ased on Topology	Show	-
	 Manually Defin 		•	Show	
	Egportable for \$	SecuRemote			
			OK C	Cancel Help	

11. Seleccione **VPN** de las opciones del lado izquierdo de la ventana y luego seleccione IKE como esquema de encriptación. Haga clic en **Edit** para configurar las propiedades IKE.

Workstation Properties -	PIX			×
General Topology NAT Advanced	VPN Encryption gehemes IN IN INTERPORTED I			
		OK	Cancel Hel;	

12. Configure las propiedades IKE como se muestra aquí:Seleccione la opción para el cifrado 3DES para que las propiedades IKE sean compatibles con el comando isakmp policy # encryption 3des.Seleccione la opción para MD5 para que las propiedades IKE sean compatibles con el comando crypto isakmp policy # hash

IKE Properties	
General	
Support key exchange encryptic	on with: Support data integrity with:
DES DES	
CAST	
	I SHA <u>I</u>
Support authentication methods	[
✓ Pre-Shared Secret	Edit Secrets
Public Key Signatures	Matching Criteria
VPN 1.8 Firsty all 1 authors	Fighting Concerns (Hubrid Mode)
	tication for securitemote (Hybrid Mode)
	Advanced
	<u>A</u> dvanced
ОК	Cancel Help

13. Seleccione la opción de autenticación para Secretos Previamente Compartidos, luego haga clic en Editar Secretos para establecer la clave previamente compartida como compatible con el comando PIX isakmp key key address address netmask netmask. Haga clic en Editar para introducir la clave y luego haga clic en Establecer,

Shar	ed Secret		×
	Shared Secrets List:	Shared Secret	
	ciscocp	xxxx	<u>E</u> dit
			<u>R</u> emove
	(OK)	Cancel	<u>H</u> elp

Aceptar.

14. En la ventana de propiedades IKE, haga clic en Avanzadas... y cambie estos parámetros.Seleccione el grupo Diffie-Hellman adecuado para las propiedades IKE.Anule la selección de la opción Support agresive mode.Seleccione la opción para el intercambio de claves Support para subredes.Haga clic en Aceptar, OK cuando haya

Advanced IKE properties			×
Use UDP encapsulation			
Support Diffie-Hellman groups —		SEC_encapsi 💌	
	Group 1 (76 G roup 2 (10	8 bit))24 bit)	
	Group 5 (15	536 bit)	
Rekeying Parameters			
Renegotiate IKE security as	sociations	1440 🛨	Minutes
Renegotiate IPSEC Security	associations every	3600 🛨	Seconds
🔲 Renegotiate IPSEC Sec	urity associations eve	ery 50000 🚊	KBytes
Misc	for SecureClient		
Support aggresive mode	ion peouleolient		
Support key exchange f	or <u>s</u> ubnets		
Πκ	Cancel	Help	

15. Seleccione Rules > Add Rules > Top para configurar las reglas de cifrado para la política.En la ventana del Editor de políticas, inserte una regla con un origen de CP_inside (red interna del NG TM de punto de control) y PIXINSIDE (red interna del PIX) en las columnas de origen y de destino. Establecer valores para Servicio = Any, Action = Encrypt, y Track = Log. Cuando haya agregado la sección Acción de cifrado de la regla, haga clic con el botón derecho en Acción y seleccione Editar propiedades.

CISCOCP - Check Point Policy Editor	- Standa	rd i					1.		
File Edit View Manage Rules Policy	File Edit View Manage Rules Policy Topology Search Window Help								
🖬 🕹 🐰 🔁 🛍 💧 🏪 🕸 🤴									
1 📽 🛄 😫 🎦 🖓 84 🗍 📐		२ 🖬 📏 👘	9						
\$ < < ⊗ 8 8 0 %	Sec.	urity - Standard 🔠	Address Translation - St	andard 🙀 QoS - S	Standard 🗓	Desktop Securi	ky - Standard		
Retwork Objects B Workstation	NU.	SOURCE	DESTINATION	SERVICE	AC	TION	TRACK	INSTALL	
	1	+ CP_inside + PIXINSIDE		* Any	© Ere	Edit propertie	s	🔃 Gateway:	
	2	+ CP_inside	* Any	🗙 Any	000 🔂	Esit Enrypho	292	Gateway:	
OSE Device OSE Device Group VLogical Server Address Range Gateway Cluster			[10	Comment		accept drop reject User Auth Client Auth Session Aut	h	1	
Dynamic Object	L cisc PD	ocp	172.18.1 172.18.1	24.157 Chedipol 24.158 PDX Firew	nt External I , Ial	Query Column Clear Query Clear Query	st		

16. Con IKE seleccionado y resaltado, haga clic en

	Encryption Properties
	General Encryption schemes defined: C C R FVVZ
	<u>E</u> dit
Edit.	OK Cancel Help

17. En la ventana IKE Properties, cambie las propiedades para coincidir con las transformaciones PIX IPsec en el comando crypto ipsec transform-set rtptac esp-3des esp-md5-hmac. Establezca la opción Transform en Encryption + Data Integrity (ESP), establezca Encryption Algorithm en 3DES, establezca Data Integrity en MD5 y establezca Allowed Peer Gateway para que coincida con el gateway PIX externo (llamado PIX aquí).

IKE Properties		
General		
Transform		
Encryption + Data Integ	rity (ESP)	
🔿 Data Integrity Only (AH)		
Encryption Algorithm:	3DES 💌]
<u>D</u> ata Integrity	MD5]
<u>C</u> ompression method:	None	1
<u>A</u> llowed Peer Gateway:	PIX 💌]
Use Perfect Forward Secrecy	,	
Use DH <u>G</u> roup:	Group 1 (768 bit) 💌 💌]
Perform IP Pool NAT		
	Cancel Help	

18. Después de configurar el ^{CheckpointTM} NG, guarde la política y seleccione **Policy > Install** para

habilitarla.						
CISCOCP - Check Point Policy	Editor - Standard					
File Edit View Manage Rules	Policy Topology Search Window	Help				
日 〇 X 市 略 番	Verify Install	'e∃≪ ♥	5 a 🛛 🖓 🕹			
°ta 🔲 📰 🌮 対 84	Uninstall	9				
♀ � � @ 8 8 0	Access Lists	Address Translation - St.	andard 🙀 QoS - St	andard 🛅 Desktop S	iecurity - Standard	1 11 11
Network Objects Workstation	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
	Global Properties	부 PIXINSIDE 부 CP_Inside	* Ατιγ	Chcryst	E Log	Gateway:
P→ Network	2 ++ CP_inside	* Any	* Any	🔂 eccept	E Log	Gateway:
- Domain - OSE Device - Embedded Device - Embedded Cevice - Embed						
-B Address Range	* CONTRACTOR	i i i i andiine				
Gateway Cluster	Name	1P	Commert			
- M Dynamic Object	ciscocp	172.18.1	24.157 Checkpoint	t External IP		
	II PIX	172.18.1	24.158 PEX Firewa			
	+ PDUNSIDE	192.168	10.0 Poinside			
	1					

La ventana de instalación muestra las notas de progreso a medida que se compila la política.



o la ventana de instalación indica que la instalación de la política ha finalizado. Haga clic en **Cerrar** para finalizar el

p	rocedimiento.
1	Install Policy
	Standard.W: Security Policy Script generated into Standard.pf Standard: Compiled OK.
	Installing VPN-1/FireWall-1 policy On: ciscocp
	VPN-1/FireWall-1 policy installed successfully on ciscocp
	VPN-1/FireWall-1 policy Installation for all modules was successful
	Close

Verificación

Verificar la configuración de PIX

Use esta sección para confirmar que su configuración funciona correctamente.

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.

Inicie un ping desde una de las redes privadas a la otra para probar la comunicación entre las dos redes privadas. En esta configuración, se envió un ping desde el lado PIX (192.168.10.2) a la red interna ^{CheckpointTM} NG (10.32.50.51).

 show crypto isakmp sa — Muestra todas las asociaciones actuales de seguridad (SA) IKE de un par.

```
show crypto isakmp sa
 Total : 1
 Embryonic : 0
              dst.
                                       src
                                                               state
                                                                         pending created
   172.18.124.157 172.18.124.158 QM_IDLE
                                                     0
                                                                1

    show crypto ipsec sa — Muestra la configuración actual utilizada por las SA actuales

 PIX501A#show cry ipsec sa
 interface: outside
     Crypto map tag: rtprules, local addr. 172.18.124.158
    local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)
    current_peer: 172.18.124.157
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
     #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
     #send errors 1, #recv errors 0
      local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
      path mtu 1500, ipsec overhead 56, media mtu 1500
      current outbound spi: 6b15a355
      inbound esp sas:
       spi: 0xced238c7(3469883591)
         transform: esp-3des esp-md5-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 3, crypto map: rtprules
         sa timing: remaining key lifetime (k/sec): (4607998/27019)
         IV size: 8 bytes
         replay detection support: Y
      inbound ah sas:
      inbound pcp sas:
      outbound esp sas:
       spi: 0x6b15a355(1796580181)
         transform: esp-3des esp-md5-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 4, crypto map: rtprules
         sa timing: remaining key lifetime (k/sec): (4607998/27019)
         IV size: 8 bytes
         replay detection support: Y
      outbound ah sas:
      outbound pcp sas:
```

Ver el estado del túnel en el punto de control NG

Vaya al Editor de directivas y seleccione **Ventana > Estado del sistema** para ver el estado del

túnel.

🕎 CISCOCP - Check Point System Status						
<u>File View M</u> odules Products <u>T</u> ools <u>W</u> indow <u>H</u> elp						
) 🗩 🗉 🗛 🔢 🔦 🚥 🇞 📾 🚅 📀 😤	} ?					
Modules IP Address	VPN-1 Details					
	Status:	ок				
i iscocp 172.18.124.157	Packets					
FireWall-1	Encrypted:	20				
FloodGiate-1	Decrypted:	20				
Management	Errors					
SVN Foundation	Encryption errors:	0				
	Decryption errors:	0				
	IKE events errors:	0				
	Hardware					
	HW Vendor Name:	none				
	HW Status:	none				

Troubleshoot

Resolución de Problemas de la Configuración PIX

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.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

Utilice estos comandos para habilitar los debugs en el Firewall PIX.

- debug crypto engine: muestra los mensajes de depuración sobre los motores criptográficos, que realizan el cifrado y el descifrado.
- debug crypto isakmp Muestra mensajes acerca de eventos IKE.

VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share

```
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
ISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4 IPSEC(key_engine): got a
queue event...
IPSEC(spi_response): getting spi 0xced238c7(3469883591) for SA
from 172.18.124.157 to 172.18.124.158 for prot 3
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.158,
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0)
has spi 3469883591 and conn_id 3 and flags 4
lifetime of 28800 seconds
```

lifetime of 4608000 kilobytes outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0) has spi 1796580181 and conn_id 4 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157, dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0xced238c7(3469883591), conn_id= 3, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157, src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP_NO_ERROR

Resumen de la red

Cuando se configuran varias redes internas adyacentes en el dominio de cifrado en el punto de control, el dispositivo podría resumirlas automáticamente con respecto al tráfico interesante. Si la lista de control de acceso criptográfico (ACL) en el PIX no está configurada para coincidir, es probable que el túnel falle. Por ejemplo, si las redes internas de 10.0.0.0 /24 y 10.0.1.0 /24 están configuradas para ser incluidas en el túnel, se pueden resumir en 10.0.0.0 /23.

Ver registros NG de punto de control

Seleccione Window > Log Viewer para ver los registros.

🐺 CLSCOCP - Check Point Log Viewer - [fw.log]												
Elle Mode Edit Selection Yew Iools Window Help												
Ó	9 🤹 🖫	Log	*	* 🕺	Ŧ 🛓	۵ ک	1 2 👼	· 📄 🗰 📴	🇞 🔛 😘	80	Ø	
1	Date	Time	Product		Inter.	Orig	Туре	Action	Source	Destina		into.
0	23Aug2002	17:32:47	VPN-1	8 Fire/Val	💽 da.	ciscoop	📄 log	Ow key install	PDC	ciscoop		IKE: Main Mode completion,
1	23Aug2002	17:32:47	VPN-4	& Fire/Vall	🕞 de .	. ciscoop	📕 log	Ow key install	PX	ciscocp		IKE: Quick Mode Received Notification from Peer: Initial Contact
2	23Aug2002	17:32:47	VPN-1	& Fire/Vall	💽 da.	. ciscocp	🔳 log	D-e key install	PIX	ciscocp		IKÉ: Quick Mode completion IKE IDs: subnet: 10.32.0.0 (most+ 255.25
э	23Aug2000	17:32:48	WE VPN-1	& Fire/Val	💽 🛤	ciscoop	🔳 log	😡 decrypt	192.168.10.2	10.32.50.51	0	ionp-type 0 ionp-code 0
4	23Aug2002	17:32:48	R VPN-1	& Fire/Vall	- 🕒 E1	. ciscoop	📕 log	🚘 decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0
5	23Aug2002	17:32:48	WE VEN-1	& Fire/Val	🕒 🖬	clecoop	🔳 log	😡 decrypt	192:168:10:2	10.32.50.51	0	icmp-type 0 icmp-code 0
6	23Aug2002	17:32:48	VPN-1	8 Fire/Val	E [1	ciscoop	🔳 log	😡 decrypt	192.168 10.2	10.32.50.51	0	icmp-type 8 icmp-code 8

Información Relacionada

- <u>Cisco PIX Firewall Software</u>
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación Cisco Systems