Configuration d'un tunnel IPSec entre un parefeu Cisco Secure PIX Firewall et un pare-feu Checkpoint NG

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Diagramme du réseau Conventions **Configurer le PIX** Configurer le contrôleur NG Vérification Vérification de la configuration PIX Afficher l'état du tunnel sur Checkpoint NG Dépannage Dépannage de la configuration PIX Récapitulation de réseau Afficher les journaux NG du point de contrôle Informations connexes

Introduction

Ce document explique comment configurer un tunnel IPsec avec des clés pré-partagées pour communiquer entre deux réseaux privés. Dans cet exemple, les réseaux de communication sont le réseau privé 192.168.10.x à l'intérieur du pare-feu Cisco Secure PIX Firewall et le réseau privé 10.32.x.x à l'intérieur du pare-feu de nouvelle génération ^{CheckpointTM}.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Le trafic de l'intérieur du PIX et de l'intérieur du ^{CheckpointTM} NG vers Internet (représenté ici par les réseaux 172.18.124.x) doit circuler avant de commencer cette configuration.
- Les utilisateurs doivent être familiarisés avec la négociation IPsec. Ce processus peut être divisé en cinq étapes, dont deux phases IKE (Internet Key Exchange).Un tunnel IPSec est

lancé par un trafic intéressant. Le trafic est considéré comme intéressant quand il transite entre les homologues IPSec.Dans la phase 1 d'IKE, les homologues IPSec négocient la stratégie d'association de sécurité IKE. Une fois que les homologues sont authentifiés, un tunnel sécurisé est créé en utilisant Internet Security Association and Key Management Protocol (ISAKMP).Dans la phase 2 d'IKE, les homologues IPSec utilisent le tunnel authentifié et sécurisé pour négocier des transformations d'association de sécurité IPSec. La négociation de la stratégie partagée détermine comment le tunnel IPSec est établi.Le tunnel IPSec est créé et les données sont transférées entre les homologues IPSec en fonction des paramètres IPSec configurés dans les jeux de transformations IPSec.Le tunnel IPSec se termine quand les associations de sécurité IPSec sont supprimées ou quand leur durée de vie expire.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel PIX version 6.2.1
- Pare-feu 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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Configurer le PIX

Cette section vous présente les informations permettant de configurer les fonctionnalités décrites dans ce document.

Configuration 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

Configurer le contrôleur NG

Les objets et les règles réseau sont définis sur le NG ^{CheckpointTM} pour constituer la stratégie relative à la configuration VPN à configurer. Cette stratégie est ensuite installée à l'aide de l'Éditeur de stratégie ^{CheckpointTM} NG pour compléter le côté NG ^{CheckpointTM} de la configuration.

 Créez les deux objets réseau pour le réseau Checkpoint et le réseau PIX Firewall qui chiffrent le trafic intéressant.Pour ce faire, sélectionnez Manage > Network Objects, puis New > Network. Entrez les informations réseau appropriées, puis cliquez sur OK.Ces exemples montrent un ensemble d'objets réseau appelé CP_Inside (réseau interne de ^{CheckpointTM} NG) et PIXINSIDE (réseau interne 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 Prope	ties - PIXINSIDE		×
General NAT]		
<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:			
Broadcas <u>I</u> nclud	address: ed <u>O No</u> t included		
	OK Cancel	Help	

2. Créez des objets de station de travail pour le NG et le PIX ^{CheckpointTM}. Pour ce faire, sélectionnez Manage > Network Objects > New > Workstation.Notez que vous pouvez utiliser l'objet de station de travail ^{CheckpointTM} NG créé lors de la configuration initiale de ^{CheckpointTM} NG. Sélectionnez les options pour définir la station de travail en tant que passerelle et périphérique VPN interopérable, puis cliquez sur OK.Ces exemples montrent un ensemble d'objets appelés ciscocp (CheckpointTM NG) et 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

Workstation Properties -	PIX			×
General — Topology	General			
- NAT	<u>N</u> ame:	PIX		
- Advanced	IP <u>A</u> ddress:	172.18.124.158	<u>G</u> et address	
	<u>C</u> omment:	PIX Firewall		
	Color:			
	Туре:	⊂ <u>H</u> ost ⊙ Gate <u>w</u> ay		
	Check Point F	Products		
	Check Po	int products installed: Version NG	Get Version	
	□VPN-1 & F □FloodGate □Policy Ser □Managem	ïreWall-1 ⊶1 ver ent Station	▲ ▼	
	Object Manaç	gement		
	C Managed	by this Management Server (Interna	el)	
	C Managed	by another Management Server (E)	demal)	
	Interope	rable ⊻PN Device		
		ОК	Cancel	Help

3. Sélectionnez Manage > Network Objects > Edit pour ouvrir la fenêtre Workstation Properties pour la station de travail ^{CheckpointTM} NG (ciscocp dans cet exemple).Sélectionnez Topologie dans les choix situés à gauche de la fenêtre, puis sélectionnez le réseau à chiffrer. Cliquez sur Modifier pour définir les propriétés de l'interface.

Workstation Properties - o	iscocp				×
General Topology NAT	Topology <u>G</u> et Interfaces				
VPN	Name	IP Address	Network Mask	IP Addresses behind	
- Authentication	E100B0	10.32.50.50	255.255.128.0	CP_inside	
⊡-Advanced	E100B1	172.18.124.157	255.255.255.0	External	
	•				
	<u>A</u> dd	Edit	<u>R</u> emove	how	
	Show all IPs behin	d Gateway			
	VPN Domain				
	 All IP Addresses information. 	<u>b</u> ehind Gateway ba	ased on Topology	Show	
	C <u>M</u> anually Defined	± [¥	Sho <u>w</u>	
	Exportable for Se	ecuRemote			
,			ок с	ancel Help	

4. Sélectionnez l'option permettant de désigner la station de travail comme interne, puis spécifiez l'adresse IP appropriée. Click OK.Dans cette configuration, CP_inside est le réseau interne du NG ^{CheckpointTM}. Les sélections de topologie indiquées ici désignent la station de travail comme interne et spécifient l'adresse comme

Interface Properties
General Topology QoS
Topology
External (leads out to the internet)
Internal (leads to the local network)
IP Addresses behind this interface:
◯ <u>N</u> ot Defined
Network defined by the interface IP and Net Mask
Anti-Spoofing
Perform Anti-Spoofing based on interface topology
Spoof Tracking: 🔿 N <u>o</u> ne 💿 Log 🔿 Alert
OK Cancel Help

- CP_inside.
- 5. Dans la fenêtre Propriétés de la station de travail, sélectionnez l'interface externe du NG CheckpointTM qui mène à Internet, puis cliquez sur **Modifier** pour définir les propriétés de l'interface. Sélectionnez l'option pour désigner la topologie comme externe, puis cliquez sur

Interface Properties	×
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 Ma	sk.
C Specific:	~
Anti-Spoofing	_
Spoof Tracking: O None O Log O Alert	
here a Fed a Fierd	
OK Cancel Help	

- OK.L
- 6. Dans la fenêtre Propriétés de la station de travail sur ^{CheckpointTM} NG, sélectionnez **VPN** dans les choix situés à gauche de la fenêtre, puis sélectionnez les paramètres IKE pour les algorithmes de chiffrement et d'authentification. Cliquez sur **Edit** pour configurer les propriétés IKE.

Workstation Properties - o	iscocp			×
General Topology NAT VPN Authentication Management € Advanced	VPN Encryption schemes	set default <u>I</u> KE pro	operties	
	Nickname DN	Edit	Certificate Authority Eemove	

 Configurez les propriétés IKE :Sélectionnez l'option de chiffrement 3DES afin que les propriétés IKE soient compatibles avec la commande isakmp policy # encryption 3des.Sélectionnez l'option pour MD5 afin que les propriétés IKE soient compatibles avec la commande crypto isakmp policy # hash

General Support key exchange encryption with: □ ⊠ DES □ ⊠ CAST □ ⊠ 3DES □ SHA1 Support authentication methods: □ Pre-Shared Secret □ Public Key Signatures	
Support key exchange encryption with: Image: DES Image: CAST Image: SDES Image: Support authentication methods: Image: Pre-Shared Secret Image: Public Key Signatures Support Support authentication	
□ 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	
□ Image: CAST □ Image: Shared Secret □ SHA1 □ Support authentication methods: □ SHA1 □ Pre-Shared Secret Edit Secrets □ Public Key Signatures Specify	
Support authentication methods: Pre-Shared Secret Public Key Signatures Specify	
Support authentication methods: Pre-Shared Secret Edit Secrets Public Key Signatures Specify	
Image: Support authentication methods: Image: Pre-Shared Secret Image: Public Key Signatures Specify	
Public Key Signatures Specify	
Public Key Signatures Specify	
PN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)
Advanced	
	_
OK Cancel Help	

8. Sélectionnez l'option d'authentification pour les secrets pré-partagés, puis cliquez sur Modifier les secrets pour définir la clé pré-partagée comme compatible avec la commande PIX isakmp key key address address netmask netmask. Cliquez sur Modifier pour entrer votre clé comme indiqué ici et cliquez sur Définir,

Share	ed Secret		
_ ⊂ S	ihared Secrets List:		
	Peer Name	Shared Secret	
	PIX	****	<u>E</u> dit
			<u><u>H</u>emove</u>
	Enter secret: loise	sortal Sat	
	ОК	Cancel	Help
	5.0		

9. Dans la fenêtre des propriétés IKE, cliquez sur **Avancé...** et modifiez ces paramètres :Désélectionnez l'option **Support agressif mode**.Sélectionnez l'option d'**échange de clés de support pour les sous-réseaux**.Cliquez sur **OK lorsque vous avez**

Advanced IKE properties			×
Use <u>U</u> DP encapsulation	UDP VPN1_IPSE	EC_encapsi 🔽	
Support Diffie-Hellman groups	,		
	Group 1 (768	bit)	
	Group 2 (102-	4 bit) 6 bit)	
		,	
Rekeying Parameters			
Renegotiate IKE security associ	ations	1440 🕂	Minutes
Renegotiate IPSEC Security ass	ociations every	3600 🕂	Seconds
Renegotiate IPSEC Security	associations every	50000 🚍	KBytes
Mise	· Client		
Support in <u>compression</u> for a	ecureclient		
Support by exchange for su	Ibnets		
OK	Cancel	<u>H</u> elp	

10. Sélectionnez Manage > Network Objects > Edit pour ouvrir la fenêtre Workstation Properties pour le PIX. Sélectionnez Topologie dans les choix situés à gauche de la fenêtre pour définir manuellement le domaine VPN.Dans cette configuration, PIXINSIDE (réseau interne de PIX) est défini comme domaine VPN.

Workstation Properties - PI	x				×
General	Topology				
- Topology - NAT	<u>G</u> et Interfaces				
VPN Advanced	Name	IP Address	Network Mask		
	<u></u>	<u>E</u> dit	Bemove S	Show	
	S <u>h</u> pw all IPs beh	ind Gateway			
	VPN Domain				_
	C All IP Addresse information.	s <u>b</u> ehind Gateway b	ased on Topology	Show	
	Manually Define		•	Sho <u>w</u>	
	Egportable for S	SecuRemote			
			ОК С	Cancel Help	

11. Sélectionnez **VPN** dans les choix situés à gauche de la fenêtre, puis sélectionnez IKE comme schéma de cryptage. Cliquez sur **Edit** pour configurer les propriétés IKE.

Workstation Properties -	PIX		×
General Topology NAT Advanced	VPN Encryption schemes Image: Image		
		Hel	P

12. Configurez les propriétés IKE comme indiqué ici :Sélectionnez l'option de chiffrement 3DES afin que les propriétés IKE soient compatibles avec la commande isakmp policy # encryption 3des.Sélectionnez l'option pour MD5 afin que les propriétés IKE soient compatibles avec la commande crypto isakmp policy # hash

IKE Properties	×
General	
Support key exchange encryption with:	Support data integrity with:
DES DES	✓ MD5
Support authentication methods:	
Pre-Shared Secret	Edit <u>S</u> ecrets
Public Key Signatures Ma	atching Criteria
✓PN-1 & FireWall-1 authentication	for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
OK Cancel	

md5.

13. Sélectionnez l'option d'authentification pour les secrets pré-partagés, puis cliquez sur Modifier les secrets pour définir la clé pré-partagée comme compatible avec la commande PIX isakmp key key address address netmask netmask. Cliquez sur Modifier pour entrer votre clé, puis cliquez sur Définir,

Shar	ed Secret		×
<u>ح</u>	Shared Secrets List:		
	Peer Name	Shared Secret	
	ciscocp	****	Edit
			<u><u>H</u>emove</u>
	1		
	OK	Cancel	<u>H</u> elp

14. Dans la fenêtre des propriétés IKE, cliquez sur Avancé... et modifiez ces paramètres.Sélectionnez le groupe Diffie-Hellman approprié aux propriétés IKE.Désélectionnez l'option Support agressif mode.Sélectionnez l'option d'échange de clés de support pour les sous-réseaux.Cliquez sur OK, OK lorsque vous avez

Advanced IKE properties			×
Use UDP encapsulation			
	UDP VPN1_IPSE	EC_encapsi 💌	
Support Diffie-Hellman groups			
	Group 1 (768	bit)	
	Group 2 (102)	4 bit) C Lao	
		6 DI()	
Rekeying Parameters			
Renegotiate IKE security associa	ations	1440 🕂	Minutes
Benegotiate IPSEC Security ass	nciations everu	3600	Seconds
		, E0000	KDutes
Renegotiate institution security	associations every	100000 🖃	NDytes
Misc			
Support IP compression for S	ecureClient		
Support aggresive mode			
Support key exchange for <u>s</u> u	bnets		
ОК	Cancel	<u>H</u> elp	

15. Sélectionnez Rules > Add Rules > Top pour configurer les règles de chiffrement de la stratégie.Dans la fenêtre Éditeur de stratégie, insérez une règle avec une source CP_inside (réseau interne du Checkpoint TM NG) et PIXINSIDE (réseau interne du PIX) sur les colonnes source et de destination. Définissez des valeurs pour Service = Any, Action = Encrypt et Track = Log. Lorsque vous avez ajouté la section Action de chiffrement de la règle, cliquez avec le bouton droit sur Action et sélectionnez Modifier les propriétés.

CISCOCP - Check Point Policy Editor	- Standar	d			1010111		
File Edit View Manage Rules Policy	Topology	Search Window H	leip				
日の X 白 略 4 極 夜	A	• • • • • •	🐁 🗏 🔹 🖉	5 a 🕹 🖓			
1 📽 🛅 😫 🖉 🤌 🗛 🗍 🗛 🤇	1 9 0	२ 🖬 📏 👘	9				
\$ < < @ B & Ø %	Sec.	urity - Standard 🔠	Address Translation - St	andard 🙀 QoS - S	tandard 🛅 Desktop S	ecurity - Standard	
Retwork Objects B Workstation	NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
	1	+ CP_inside + PIXINSIDE	부 POINSIDE 부 CP_inside	🛪 Any	Edit prop	erties	🔝 Gateway:
-++ O inside	2	+ CP_inside	* Any	* Any		por	Gateway:
Domain OSE Device Embedded Device					 accept drop reject 		
Group					🕒 User Av 😑 Client A	uth	
- C Gateway Custer					😑 Session	Auth	
Dynamic Object	Nan	ne su	IP.	Conment	Encrypt		
	Cisc	ocp	172.18.1	24.157 Chedipoir 24.158 PDX Firew	st External I 🙆 Client Er	norypt	
					Query Ci Clear Qu	ary	

16. Lorsque IKE est sélectionné et mis en surbrillance, cliquez sur

E	ncryptio	n Properties			×
	General Encr	yption <u>s</u> chemes de Marcelle IKE Marcelle FVVZ Edit	efined:		
ər		OK	Cancel	Help	

17. Dans la fenêtre Propriétés IKE, modifiez les propriétés pour qu'elles correspondent aux transformations IPsec PIX dans la commande crypto ipsec transformer-set rtptac esp-3des esp-md5-hmac.Définissez l'option Transform sur Encryption + Data Integrity (ESP), définissez Encryption Algorithm sur 3DES, définissez Data Integrity sur MD5 et définissez la passerelle d'homologue autorisée pour qu'elle corresponde à la passerelle PIX externe (appelée PIX ici). Click

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

 Après avoir configuré ^{CheckpointTM} NG, enregistrez la stratégie et sélectionnez Policy > Install pour

l'activer.							
TISCOCP - Check Point Policy	Editor - Standard						
File Edit View Manage Rules	Policy Topology Search Window	Help					
🖬 Ə X ୩ 🛍 👫	Verify Install	*= = × 🗣	54 X 147				
Pie 📰 📰 🌮 🛃 🕴	Uninstall	9					
\$ € 4 0 8 8 8 0	Access Lists	Address Translation - Standard 🗱 QoS - Standard 🛅 Desktop Security - Standard					
Vetwork Objects Workstation	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL	
ciscocp PIX	Global Properties	부 PXINSIDE 부 CP_inside	* Any	Encrypt	E Log	Gateway:	
-→ Network	2 4 CP_inside	* Any	* Any	G eccept	E Log	Gateway:	
Domain							
- B Embedded Device							
Group							
					1		
Gateway Cluster		a and inclusion	ana a ar				
Dynamic Object	Name	1	Comment		<u></u>		
_	ciscocp	172.18.1	24.157 Checkpoir	nt External IP			
	PD(172.18.1	24.158 PEX Firew	al			
	CP_inside	10.32.0.	O OPINSIDE				
	PIXINSIDE	192.168	10.0 Poinside				

La fenêtre d'installation affiche les notes de progression lors de la compilation de la stratégie.



e la fenêtre d'installation indique que l'installation de la stratégie est terminée. Cliquez sur **Fermer** pour terminer la

 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

Vérification

Vérification de la configuration PIX

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'<u>Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines</u> <u>commandes show.</u> Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**. Lancez une requête ping de l'un des réseaux privés vers l'autre réseau privé pour tester la communication entre les deux réseaux privés. Dans cette configuration, une requête ping a été envoyée du côté PIX (192.168.10.2) au réseau interne ^{CheckpointTM} NG (10.32.50.51).

• show crypto isakmp sa—Affiche toutes les IKE SA actuelles chez un homologue.

```
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 — Affiche les paramètres utilisés par les SA.

 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:
```

Afficher l'état du tunnel sur Checkpoint NG

Accédez à l'Éditeur de stratégie et sélectionnez **Fenêtre > État du système** pour afficher l'état du tunnel.

🐺 CISCOCP - Check Point System Status			
<u>File View M</u> odules <u>P</u> roducts <u>T</u> ools <u>W</u> indow <u>H</u> elp			
) 🖸 🗉 🗛 🔢 🔦 🎫 🇞 📾 🚅 🍥 😪	1 ;7		
Modules IP Address	VPN-1 Details		
	Status: Ol	к	
E ciscocp 172.18.124.157	Packets		
FireWall-1	Encrypted: 20)	
FloodGate-1	Decrypted: 20		
Management	Errors		
SVN Foundation	Encryption errors: 0		
MFIN-1	Decryption errors: 0		
	IKE events errors: 0		
	Hardware		
	HW Vendor Name: no	one	
	HW Status: no	one	

Dépannage

Dépannage de la configuration PIX

L'<u>Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines</u> <u>commandes show.</u> Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Remarque : Consulter les <u>renseignements importants sur les commandes de débogage</u> avant d'utiliser les commandes de **débogage**.

Utilisez ces commandes pour activer les débogages sur le pare-feu PIX.

- debug crypto engine Affiche les messages de débogage sur les moteurs de chiffrement, qui effectuent le chiffrement et le déchiffrement.
- debug crypto isakmp—Affichage de messages d'événements 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 OM 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

Récapitulation de réseau

Lorsque plusieurs réseaux internes adjacents sont configurés dans le domaine de chiffrement sur le point de contrôle, le périphérique peut automatiquement les résumer en fonction du trafic intéressant. Si la liste de contrôle d'accès de chiffrement (ACL) sur le PIX n'est pas configurée pour correspondre, le tunnel risque d'échouer. Par exemple, si les réseaux internes 10.0.0.0 /24 et 10.0.1.0 /24 sont configurés pour être inclus dans le tunnel, ils peuvent être résumés sur 10.0.0.0 /23.

Afficher les journaux NG du point de contrôle

	CISCOCP - 0	Check Poi	nt Log Vie	wer -	oLw]]	a] ·		51		-ilii	ē-+iH+-H		
64	e Mode Ed	ik Selecti	on Yiew	<u>I</u> oois	Mind	ow He	þ						
Ó	9 🤹 骗	Log	*	*	A 1	F 🛓	۵ ک	% 👼	📑 🚟 🛱	🇞 🔛 😘	80	đ	
	Date	Time	Product		fili	Inter.	Orig	Туре	Action	Source	Destina		lafo.
0	23Aug2002	2 17:32:47	VPN-1	8 Fird	Wall	🕒 da.	ciscoop	🔳 log	Ow key install	POC	olscoop		KE: Mein Mode completion.
1	23Aug2002	17:32:47	VPN-4	8 Fire	Wall	🕒 de.	ciscocp	📕 log	D-w key install	POC	ciscocp		IKE: Quick Mode Received Notification from Peer: Initial Contact
2	23Aug2002	17:32:47	VPN-1	& Fee	Wall	🕒 da.	ciecocp	🔳 log	Dre key install	PIX	ciscocp		IKE: Quick Mode completion IKE IDs: subnet: 10.32.0.0 (mesk+ 255.25
з	23Aug2000	17:32:48	VPN-1	& Fire	(Val	C 11.	ciscoop	🔳 log	😡 decrypt	192:168 10:2	10.32.50.51	0	iomp-type 0 iomp-code 0
4	23Aug2002	2 17:32:48	WE VEN-1	å Fire	Wall	🕒 E1	ciscoop	📕 log	🞑 decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0
5	23Aug2002	17:32:48	R VPN-1	8.Fre	Well	🕒 E1	clecoop	Iog	😡 decrypt	192:168:10:2	10.32.50.51	0	icmp-type 0 icmp-code 0
6	23Aug2002	2 17:32:48	VPN-1	8 Fire	Nal	🖻 🖬	ciscoop	🔳 log	🚘 decrypt	192.168.10.2	10.32.50.51	0	ionp-type 8 ionp-code 8

Sélectionnez **Fenêtre > Visionneuse de journaux** pour afficher les journaux.

Informations connexes

- Logiciels pare-feu Cisco PIX
- <u>Références des commandes du pare-feu Cisco Secure PIX</u>
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques Cisco Systems