# نمآلا PIX ةيامح رادج نيب IPSec قفن نيوكت ققحتلا ةطقنل NG ةيامح رادجو Cisco نم

# المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات المكونات المستخدمة الرسم التخطيطي للشبكة الاصطلاحات تكوين PIX تكو<u>ين NG لنقطة التحقق</u> التحقق من الصحة التحقق من تكوين PIX <u>عرض حالة النفق على نقطة التحقق NG</u> استكشاف الأخطاء وإصلاحها <u>أستكشاف أخطاء تكوين PIX واصلاحها</u> تلخيص الشبكة <u>عرض سجلات NG لنقطة التحقق</u> معلومات ذات صلة

# <u>المقدمة</u>

يوضح هذا المستند كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للاتصال بين شبكتين خاصتين. في هذا المثال، شبكات الاتصال هي الشبكة الخاصة x.192.168.10 داخل جدار حماية Cisco Secure PIX والشبكة الخاصة x.x.10.32 داخل جدار حماية <sup>CheckpointTM</sup> من الجيل التالي (NG).

## <u>المتطلبات الأساسية</u>

### <u>المتطلبات</u>

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- يجب تدفق حركة المرور من داخل PIX ومن داخل <sup>CheckpointTM</sup> NG إلى الإنترنت (ممثلة هنا بشبكات x.172.18.124) قبل بدء هذا التكوين.
- يجب أن يكون المستخدمون على دراية بتفاوض IPsec. يمكن تقسيم هذه العملية إلى خمس خطوات، تتضمن مرحلتين من عملية تبادل مفتاح الإنترنت (IKE).يتم بدء نفق IPsec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين نظائر IPsec.في المرحلة الأولى من IKE، يتفاوض نظراء IPsec على سياسة اقتران أمان IKE (SA) التي تم إنشاؤها. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP).في المرحلة 2 من IKE، يستخدم نظراء IPsec

الآمن والمصدع للتفاوض على تحويلات IPsec SA. يحدد التفاوض على السياسة المشتركة كيفية إنشاء نفق IPsec.يتم إنشاء نفق IPsec ويتم نقل البيانات بين نظائر IPsec استنادا إلى معلمات IPsec التي تم تكوينها في مجموعات تحويل IPsec.ينتهي نفق IPsec عند حذف وحدات IPsec SAs أو عند انتهاء صلاحية مدة حياتها.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج PIX الإصدار 6.2.1 جدار حماية NG <sup>CheckpointTM</sup>

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة إلمُستخدمة في هذا المستند بتكوين ممسوح (افتراضيَ). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المُحتمل لأي امر.

### الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



### الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

# تکوین PIX

يقدم لك هذا القسم معلومات تكوين الميزات الموضحة في هذا المستند.

### تكوين 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<sup>™</sup> ---! 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 ipsec- ---! isakmp 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

# <u>تكوين NG لنقطة التحقق</u>

يتم تحديد كائنات الشبكة وقواعدها على NG <sup>CheckpointTM</sup> لتكوين السياسة المتعلقة بتكوين VPN الذي سيتم إعداده. يتم بعد ذلك تثبيت هذا النهج باستخدام محرر نهج NG <sup>CheckpointTM</sup> لإكمال جانب NG <sup>CheckpointTM</sup> من التكوين.

1. قم بإنشاء كائني الشبكة لشبكة نقطة التفتيش وشبكة جدار حماية PIX التي تقوم بتشفير حركة المرور المفيدة.للقيام بذلك، حدد **إدارة > كائنات الشبكة**، ثم حدد **جديد > الشبكة**. أُدخل معلومات الشبكة المناسبة، ثم انقر على **موافق**.تظهر هذه الأمثلة مجموعة من كائنات الشبكة تسمى CP\_Inside (داخل شبكة <sup>CheckpointTM</sup> NG) و Pixinside (داخل شبكة

Network Prop	erties - CP_inside		×
General NA	г		
<u>N</u> ame:	CP_inside		
IP <u>A</u> ddres:	s: 10.32.0.0		
Net <u>M</u> ask:	255.255.128.0		
<u>C</u> omment:	CPINSIDE		
Color:			
Broadca © <u>I</u> nclu	st address: ded <u>O No</u> t included		
		Halp	
		neip	(F

Network Proper	ties - PIXINSIDE	<u>×</u>
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	
Cojor:	<b>—</b>	
Broadcast	address: ed <u>O No</u> t included	
	OK Cancel	Help

2. إنشاء كائنات محطة العمل ل NG <sup>CheckpointTM</sup> و PIX. للقيام بذلك، حدد **إدارة > كائنات الشبكة > جديد >** محطة العمل.لاحظ أنه يمكنك إستخدام كائن محطة العمل NG <sup>CheckpointTM</sup> الذي تم إنشاؤه أثناء إعداد <sup>CheckpointTM</sup> الأولي. حدد الخيارات لتعيين محطة العمل كبوابة وجهاز VPN قابل للتشغيل البيني، ثم انقر فوق موافق.تظهر هذه الأمثلة مجموعة من الكائنات تسمى PIX NG (CheckpointTM NG) و PIX (جدار حماية (PIX).

Wo	rkstation Properties -	ciscocp			×
Wol	rkstation Properties - General Topology NAT VPN Authentication Management - Advanced	ciscocp General Name: IP <u>A</u> ddress: Cojor:	ciscocp 172.18.124.157 Checkpoint External IP	<u>G</u> et address	×
		Туре:	⊂ <u>H</u> ost . ເ⊂ Gate <u>w</u> ay		
		Check Point F	Products		
		Check Bo	int products installed: Version NG	▼ Giet Version	
		✓VPN-1 & F     ✓FloodGate     Policy Ser     ✓Primary Ma	ï <b>reWall-1</b> ⊷1 ver anagement Station	•	
		Object Manag	pement		
		Managed	by this Management Server (Interna	ŋ	
		C Managed	by another Management Server (Ex	temal)	
		Secure Intern	al Communication		
		Comm <u>unica</u>	ation DN: <b>cn=cp_mgmt,o=cisc</b> rable ⊻PN Device	ocppvzfoa	
			OK	Cancel	Help

Workstation Properties -	PIX			×
General	General			
- NAT	<u>N</u> ame:	PIX		
VPN Advanced	IP <u>A</u> ddress:	172.18.124.158	<u>i</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	FireWall-1 ⊶1 ver ent Station	×	
	Object Manag	gement		
	C Managed	by this Management Server (Internal)		
	C Managed	by another Management Server (Exter	nal)	
	✓ Interope	rable ⊻PN Device		
,		OK	Cancel	Help

3. حدد **إدارة>كائنات الشبكة>تحرير** لفتح نافذة خصائص محطة العمل ل C**heckpointTM** NG Workstation (CiscoP) في هذا المثال).حدد **المخطط** من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد الشبكة التي سيتم تشفيرها. انقر فوق **تحرير** لتعيين خصائص الواجهة.

Workstation Properties -	ciscocp				×
- General - Topology - NAT	Topology Get Interfaces				
Authoritization	Name	IP Address	Network Mask	IP Addresses behind	
Management	E100B0	10.32.50.50	255.255.128.0	CP_inside	
<ul> <li>Advanced</li> </ul>	E100B1	172.18.124.157	255.255.255.0	External	
	1				
	<u>A</u> dd S <u>h</u> ow all IPs behi VPN Domain ○ All IP Addresses information. ○ <u>M</u> anually Define Exportable for S	Edit	Remove S	Èhow Sh <u>o</u> w Sho <u>w</u>	
			ок с	Cancel Help	

4. حدد الخيار الخاص بتعيين محطة العمل كمحطة عمل داخلية، ثم حدد عنوان IP المناسب. وانقر فوق O**K**.في هذا تشكيل، cp\_inside هو الشبكة الداخلية من ال NG <sup>CheckpointTM</sup> NG. تعين تحديدات المخطط الموضحة هنا محطة العمل كمحطة عمل داخلية وتحدد العنوان كبروتوكول

Interface Properties 🛛 📉 🗙	
General Topology QoS	
Topology	
<u>External (leads out to the internet)</u>	
Internal (leads to the local network)	
IP Addresses behind this interface:	
◯ <u>N</u> ot Defined	
O Network defined by the interface IP and Net Mask	
Specific: + CP_inside	
Anti-Spoofing	
Perform Anti-Spoofing based on interface topology	
Spoof Tracking: ON <u>o</u> ne	
OK Cancel Help	СР

.5. من نافذة "خصائص محطة العمل"، حدد الواجهة الخارجية الموجودة على NG <sup>CheckpointTM</sup> التي تؤدي إلى الإنترنت، ثم انقر فوق **Edit"** لتعيين خصائص الواجهة. حدد الخيار لتعيين المخطط كمخطط خارجي، ثم انقر

Interface Properties
General Topology QoS
Topology
<ul> <li>External (leads out to the internet)</li> </ul>
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 Specific:
Anti-Spoofing
Perform Anti-Spoofing based on interface topology
Speef Tracking: C. None C. Lee, C. Alert
Spool Hacking. S None S Log S Alek
OK Cancel Help

من نافذة خصائص محطة العمل على NG <sup>CheckpointTM</sup> ، حدد VPN من الخيارات الموجودة على الجانب. الأيسر من النافذة، ثم حدد معلمات IKE لخوارزميات التشفير والمصادقة. انقر فوق **تحرير** لتكوين خصائص. IKE.

VPN Encryption schemes	set default <u>I</u> KE	properties	
Nickname E	)N	Certificate Authority	
		<u>R</u> emove	_
	VPN Encryption schemes	VPN Encryption gchemes	VPN         Encryption gchemes         Image: FWZ         Image: FWZ         Edit

7. تكوين خصائص IKE:حدد الخيار لتشفير **3DES** بحيث تكون خصائص IKE متوافقة مع الأمر **#** IKE crypto isakmp policy . حدد الخيار ل MD5 حتى تكون خصائص IKE متوافقة مع الأمر (# MD5.

IKE Properties			×
General			
Support key exchange encryption	with: Support dat	a integrity with:	
Support authentication methods:			
Pre-Shared Secret	Edit <u>S</u> ecrets		
Public <u>K</u> ey Signatures	Specify		
□ ⊻PN-1 & FireWall-1 authenti	cation for SecuRemote	, e (Hybrid Mode)	
		<u>A</u> dvanced	
OK	Cancel Help	5	

8. حدد خيار المصادقة للأسرار المشتركة مسبقا، ثم انقر فوق تحرير الأسرار لتعيين المفتاح المشترك مسبقا على أنه متوافق مع أمر PIX *عنوان مفتاح ISAKMP لعنوان قناع الشبكة* قناع الشبكة. طقطقة **يحرر** أن يدخل مفتاحك كما هو موضح هنا وطقطقة **محموعة،** 

Share	ed Secret		, j	×
<b>5</b>	Shared Secrets List: -	Shared Secret	1	
	PIX	****		t
			<u>R</u> emo	ove
	Enter secret: cisco	ortpS	et	
	ОК	Cancel	<u>H</u> elp	

9. من نافذة خصائص IKE، انقر على **خيارات متقدمة.**.. وقم بتغيير هذه الإعدادات:قم بإلغاء تحديد خيار **دعم الوضع المتداخل**.حدد الخيار **لتبادل مفتاح الدعم للشبكات الفرعية**.انقر فوق موافق عند

Advanced IKE properties			×
Use UDP encapsulation			
	UDP VPN1_IPSE	EC_encapsi 💌	
Support Diffie-Hellman groups			
	Group 1 (768	bit)	
	Group 2 (102)	4 bitj c.sa)	
		o Ditj	
Rekeying Parameters			
Renegotiate IKE security associal	tions	1440 🗧	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 🛨	Seconds
Renegotiate IPSEC Security a	associations every	50000 🚊	KBytes
Mise			
Support IP compression for Se	ecureClient		
Support aggresive mode			
Support key exchange for sub	onets		
	ancel	Help	

10. حدد **إدارة > كائنات الشبكة > تحرير** لفتح نافذة خصائص محطة العمل ل PIX. حدد **طوبولوجيا** من الخيارات الموجودة على الجانب الأيسر من النافذة لتعريف مجال VPN يدويا.في هذا التكوين، يتم تعريف Pixinside (داخل شبكة PIX) على أنه مجال VPN.

Workstation Properties - PIX					×
General	opology				
- Topology - NAT	<u>G</u> et Interfaces				
	Name	IP Address	Network Mask		1
Advanced					-
					-
					-
	, 	E-da	Remove I G	Show I	1
	<u>800</u>	Ealt	Tellove 2	271(319)	
	Show all IPs beh	ind Gateway			
	VPN Domain				-
	<ul> <li>All IP Addresse information.</li> </ul>	s <u>b</u> ehind Gateway b	ased on Topology	Sh <u>o</u> w	
	<u>Manually Definition</u>		-	Sho <u>w</u>	1
		1			'
	Exportable for 9	SecuRemote			
1				ancel Halr	

11. حدد **VPN** من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد IKE كمخطط تشفير. انقر فوق **تحرير** لتكوين خصائص IKE.

Workstation Properties -	PIX		×
General - Topology - NAT - Advanced	VPN         Incruption genemes         Image: Image		
		UK Lancel	нер

12. قم بتكوين خصائص IKE كما هو موضح هنا:حدد الخيار لتشفير **3DES** بحيث تكون خصائص IKE متوافقة مع الأمر **isakmp policy # encryption 3des**.حدد الخيار ل **MD5** حتى تكون خصائص IKE متوافقة مع الأمر crypto isakmp policy **# hash** 

riopercies	<u> </u>
ieneral	
Support key exchange encryption	n with:Support data integrity with:
Support authentication methods: -	
Pre-Shared Secret	Edit <u>S</u> ecrets
<ul> <li>Pre-Shared Secret</li> <li>Public Key Signatures</li> </ul>	Edit <u>S</u> ecrets Matching Criteria
Pre-Shared Secret Public Key Signatures VPN-1 & FireWall-1 authentic	Edit <u>S</u> ecrets <u>M</u> atching Criteria cation for SecuRemote (Hybrid Mode)
Public Key Signatures VPN-1 & FireWall-1 authentic	Edit <u>Secrets</u> <u>Matching Criteria</u> cation for SecuRemote (Hybrid Mode) <u>A</u> dvanced
Pre-Shared Secret     Public Key Signatures     VPN-1 & FireWall-1 authentic	Edit Secrets <u>Matching Criteria</u> cation for SecuRemote (Hybrid Mode) <u>Advanced</u>

13. حدد خيار المصادقة للأسرار المشتركة مسبقا، ثم انقر فوق تحرير الأسرار لتعيين المفتاح المشترك مسبقا كمتوافق مع أم<u>ر PIX **مفتاح** *عنوان* **قناع الشبكة</u> قناع الشبكة. انقر فوق <b>تحرير** لإدخال مفتاحك، ثم انقر فوق</u>

Shar	ed Secret			×
- ۲	Shared Secrets List: -			
	Peer Name	Shared Secret		
	ciscocp	****	<u>E</u> dit	
			<u>R</u> emove	
	OK	Cancel	<u>H</u> elp	
				تعيين، موافق 🦰

14. من نافذة خصائص IKE، انقر على **خيارات متقدمة.**.. وقم بتغيير هذه الإعدادات.حدد مجموعة -Diffie المناسبة لخصائص IKE.قم بإلغاء تحديد خيار **دعم الوضع المتداخل**.حدد الخيار **لتبادل مفتاح الدعم للشبكات الفرعية**.وانقر فوق **موافق، موافق** عند

Advanced IKE properties			×
Use UDP encapsulation			
	UDP VPN1_IPS	EC_encapsi 🔽	
Support Diffie-Hellman groups			
	Group 1 (768	3 bit)	
	Group 2 (102	24 bit) DC Fai	
		o uluj	
Rekeying Parameters			
Renegotiate IKE security associa	ations	1440 🗧	Minutes
Renegotiate IPSEC Security ass	ociations every	3600 🕂	Seconds
🔲 Renegotiate IPSEC Security	associations ever	y 50000 🚊	KBytes
Misc -	· CF		
Support iP compression for a	ecureulient		
Support key exchange for st	ibnete		
I ■ Support Key exchange for <u>s</u> u	ibiliets		
UK (	Jancel	<u>H</u> elp	

15. حدد **قواعد>إضافة قواعد>Top** لتكوين قواعد التشفير للنهج.في نافذة محرر النهج، قم بإدراج قاعدة بمصدر 15. حدد **قواعد>O**P\_Inside (داخل شبكة من نقطة التفتيش NG <sup>TM</sup>) و Pixinside (داخل شبكة PIX) على كل من أعمدة المصدر والوجهة. قم بتعيين قيم **للخدمة = أي، الإجراء = تشفير**، و**المسار = السجل**. عندما تقوم بإضافة قسم إجراء التشفير من القاعدة، انقر بزر الماوس الأيمن فوق **الإجراء** وحدد **تحرير** 

						الخصائص.
CISCOCP - Check Point Policy Editor	r - Standard					
File Edit View Manage Rules Policy	Topology Search Window He	np				
🖬 🕘 🐰 🔁 🛍 🛔 🤷 🦓	2 A 🛛 🗉 🖣 📲 👘	👞 🗏 🛶 🛛 👽	5 💦 🛛 🖓 👗			
1 18 🖬 💷 🌮 1 94 84 1 🖡 🤇	Q Q Q 🖸 🔪 🖻 I	9				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	🗱 Security - Standard 🧱 🗸	ddress Translation - 90	andard 🙀 QoS - Si	tandard 🕅 Desktop Secu	rity - Standard	
Retwork Objects	NO. SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
PIX	1 4 CP_inside 4 PIXINSIDE		🗙 Atty	Edit properti	es	🔝 Gateway:
-++ CP_inside	2 4 CP_inside	🛪 Any	🗙 Any	C acc Ecit Encrypt	07 07 9	Gateway:
+ PDONSIDE			1	accept	11.1	
g Domain				drap.		
OSE Device	11			C spinot		
Embedded Device					1 1 mar 1	
- W Logical Server	10			Oser Auer	1 3 m 1 1	
Address Range				Client Auth	and the second	1
Gateway Ouster				😑 Session Av	dh	
Dynamic Object	Name	IP	Conment	Encrypt		
_	ciscocp	172.18.1	24.157 Chedipoin	t External I 🙆 Client Encry	ppt	
	D PDX	172.18.1	24.158 PDX Pirewa	al Crumos Colum	La La martin	
	1			Clear Ouerv		
	11			Contra Cont h		

Encryption Properties			×
General			
Encryption <u>s</u> chemes defined:			
<u>E</u> dit			
OK Cano	el H	lelp	

crypto ipSec في أمر PIX IPsec 17. على نافذة خصائص الله من الخصائص لتوافق مع تحويلات PIX IPsec في أمر crypto ipSec قم بتعيين خيار التحويل إلى **التشفير + تكامل البيانات (Iransform-set rtptac esp-3des esp-md5-hmac**)، وتعيين خوارزمية التشفير إلى 3DES، وتعيين تكامل البيانات إلى MD5، وتعيين بوابة النظير المسموح بها لمطابقة بوابة PIX الخارجية (المعروفة باسم PIX هنا). وانقر فوق

IKE Properties	<u></u>		×
General			
Transform			
Encruption + Data Integ	ritu (ESP)		
C Data Integrity Only (AH)			
Encryption Algorithm:	3DES		-
<u>D</u> ata Integrity	MD5	•	-    - E-
<u>C</u> ompression method:	None	•	-
Allowed Peer Gateway:	PIX	ŀ	] [
Use Perfect Forward Secrecy	,		
Use DH <u>G</u> roup:	Group 1 (768 bit)		2
Perform IP Pool NAT			
OK (	Cancel Hel	P	
			Oł

18. بعد تكوين NG <sup>CheckpointTM</sup>، احفظ النهج وحدد **النهج** > Install

لتمكينه. CISCOCP - Check Point Policy Editor - Standard - O × le Edit View Manage Rules Policy Topology Search Window Help Verify... 54 %å& ₩ 日 ジ 当 前 前 条 Install... \*1: 🔲 📰 🏏 🛃 임류 Uninstall... 2 º 🔍 🔍 🛞 🖪 🙈 ⊘ Address Translation - Standard 🛛 🏭 QoS - Standard 🗖 Desktop Security - Standard Access Lists... Install Users Database... Retwork Objects SERVICE ACTION TRACK INSTALL DESTINATION 😑 🛄 Workstation Management High Availability Ciscoop + POONSIDE 🗇 Encrypt 🔳 Log 🖪 Gateway Global Properties. 🗙 Any + CP\_inside 😑 😽 Network 🗙 Any + OP\_inside 2 4 CP\_inside \* Any G eccept E Log Gateway: + PEGNSIDE 😭 Domain OSE Device Embedded Device Group Ungical Server 📙 Address Range × Gateway Cluster Name IP Comment 172.18.124.157 Checkpoint External IP 📙 ciscocp PIX CP\_inside 172.18.124.158 PEX Firewall **OPINSIDE** 10.32.0.0 + PIXINSIDE 192.168.10.0 Pixinside

تعرض نافذة التثبيت ملاحظات التقدم أثناء تحويل النهج

Install Polic	;y			×
Standard.W Standard: Compiled Ol	': Security Policy K.	Script generated	into Standard.pf	 <u> </u>
				_
			ort	

عندما تشير نافذة التثبيت إلى اكتمال تثبيت النهج. انقر فوق **إغلاق**" لإنهاء

Install Policy	×
Standard.W: Security Policy Script generated into Standard.pf Standard: Compiled OK.	<u>~</u>
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	

# <u>التحقق من الصحة</u>

# <u>التحقق من تكوين PIX</u>

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

بدء إختبار اتصال من إحدى الشبكات الخاصة إلى الشبكة الخاصة الأخرى لاختبار الاتصال بين الشبكتين الخاصتين. في هذا التكوين، تم إرسال إختبار اتصال من جانب PIX (192.168.10.2) إلى الشبكة الداخلية NG <sup>CheckpointTM</sup> NG 10.32.50.51)).

### • show crypto isakmp sa— يعرض جميع شبكات IKE الحالية في نظير.

show crypto isakmp sa : 1 Total Embryonic : 0 dst src state pending created QM\_IDLE 172.18.124.158 0 1 172.18.124.157 • show crypto ipSec—يعرض الإعدادات المستخدمة من قبل SAs الحالية. 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

### <u>عرض حالة النفق على نقطة التحقق NG</u>

انتقل إلى "محرر النهج" وحدد **نافذة > حالة النظام** لعرض حالة النفق.

📅 CISCOCP - Check Point System	status			
<u>File View M</u> odules <u>P</u> roducts <u>T</u> oo	ols <u>W</u> indow <u>H</u> elp			
) D 🕂 🗖 🖊 🗖 🖬	🎭 📾 🚅 🐵 🍨	<b>∖?</b>		
Modules	IP Address	VPN-1 Details		
		Status:	ок	
🖻 📲 ciscocp	172.18.124.157	Packets		
FireWall-1		Encrypted:	20	
FloodGate-1		Decrypted:	20	
Management		Errors		
SVIN Foundation		Encryption errors:	0	
		Decryption errors:	0	
		IKE events errors:	0	
		Hardware		
		HW Vendor Name:	none	
		HW Status:	none	

# استكشاف الأخطاء وإصلاحها

### أستكشاف أخطاء تكوين PIX وإصلاحها

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

**ملاحظة:** ارجع إلى <u>معلومات مهمة حول أوامر التصحيح</u> قبل إستخدام أوامر debug.

أستخدم هذه الأوامر لتمكين تصحيح الأخطاء على جدار حماية PIX.

• debug crypto engine—يعرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تقوم بالتشفير وفك التشفير.

• debug crypto isakmp—يعرض الرسائل المتعلقة بأحداث 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 = 0ISAKMP (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 = 0ISAKMP (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 = 0ISAKMP (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 4lifetime 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

#### <u>تلخيص الشبكة</u>

عندما يتم تكوين شبكات داخلية متجاورة متعددة في مجال التشفير على نقطة التحقق، قد يقوم الجهاز بتلخيصها تلقائيا فيما يتعلق بحركة المرور المفيدة. إذا لم يتم تكوين قائمة التحكم في الوصول إلى التشفير (ACL) على PIX للمطابقة، فمن المحتمل أن يفشل النفق. على سبيل المثال، إذا تم تكوين الشبكات الداخلية من 10.0.00 /24 و 24/ 10.0.10

### <u>عرض سجلات NG لنقطة التحقق</u>

حدد **نافذة > عارض السجل** لعرض السجلات.

	ISCOUP - C	heck Poir	ut Log Vier	wer - [lwJ	log]							
6le	Mode Ed	t Selecti	n yew	Icois Wr	ndow He	lp-						
69	🗳 🗞 🛛	Log	•	+ A	Ŧ 🛓	۵ ک	<b>%</b> 👼	· 📄 🗰 🛱	🇞 🔛 😘	80	1	
. (	Date	Time	Product	i fit fit	Inter.	Orig	Туре	Action	Source	Destina		Info.
0 3	23Aug2002	17:32:47	VPN-1	8 Find/Vall	. 💽 da.	. ciscocp	🔳 log	Ow key install	POC	ciscocp		KE: Main Mode completion.
t = 1	23Aug2002	17:32:47	VPN-1	8 Fire/Vall	. 🕞 de .	. ciscocp	📕 log	Oray key install	POC	ciscocp		IKE: Quick Mode Received Notification from Peer: Initial Contact
2 :	23Aug2002	17:32.47	WPN-1	& FireNvall	. 📻 da.	. ciscocp	🔳 log	Ore key install	PIX	ciscocp		IKE: Guick Mode completion IKE IDs: subnet: 10.32.0.0 (mest+ 255.25
з ;	23Aug2002	17:32:48	W VPN-1	& Firel/Vall	. 🕒 🛤.	. ciscoop	🔳 log	🚘 decrypt	192.168 10.2	10.32.50.51	0	iomp-type 0 iomp-code 0
4 3	23Aug2002	17:32:48	VPN-1	& Fire/Vall	🕒 E1	. ciscoop	📕 log	🚔 decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0
5 3	23Aug2002	17:32:48	R VPN-1	8.Farel/Val	. 🕒 🖬 .	. clecoop	Iog	😡 decrypt	192:168:10:2	10.32.50.51	0	icmp-type 8 icmp-code 8
6 :	23Aug2002	17:32:48	VPN-1	8 Firel/Val	🕞 🛤	ciscoop	🔳 log	🚘 decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 8

# <u>معلومات ذات صلة</u>

- <u>برنامج جدار حماية Cisco PIX</u>
- مراجعً أوامرً جدار حماية PIX الآمن من <u>Cisco</u>
- <u>الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)</u>
  - طلبات التعليقات (RFCs<u>)</u>
  - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما