# زكرم نيب IPSec قفن نيوكت Cisco VPN 3000 قفن نيوكت ققحتالا ةطقنل NG ةيامح رادجو

### المحتويات

المقدمة المتط<u>لبات الأساسية</u> المتطلبات المكونات المستخدمة الاصطلاحات الرسم التخطيطي للشبكة التكوينات تكوين مركز VPN 3000 <u>تكوين NG لنقطة التحقق</u> التحقق من الصحة <u>التحقق من اتصال الشبكة</u> عرض حالة النفق على نقطة التفتيش NG عرض حالة النفق على مركز VPN استكشاف الأخطاء وإصلاحها تلخيص الشبكة <u>تصحيح أخطاء NG لنقطة التفتيش</u> تصحيح أخطاء مركز VPN 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 مركز Cisco VPN 3000 والشبكة الخاصة x.x.10.32 داخل جدار حماية الجيل التالي لنقطة الوصول.

### <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

- يجب أن تتدفق حركة المرور من داخل مركز الشبكة الخاصة الظاهرية (VPN) ومن داخل نقطة التفتيش NG إلى الإنترنت - الممثلة 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 إنشاء نفق IPSec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين أقران IPSec.في المرحلة الأولى من IKE، يتفاوض نظراء IPSec على سياسة اقتران أمان IKE (SA) الراسخة. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP).في المرحلة 2 من IKE، يستخدم نظراء IPSec

والمصدق من أجل التفاوض على عمليات تحويل 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 أسماء IPSec أو عند انتهاء صلاحية عمرها الافتراضي.

#### <u>المكونات المستخدمة</u>

تم تطوير هذه التهيئة واختبارها باستخدام إصدارات البرامج والمكونات المادية التالية:

- مركز VPN 3000 Series Concentrator 3.5.2
  - جدار حماية NG لنقطة التحقق

#### <u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

#### <u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:



**ملاحظة:** مخطط عنونة IP المستخدم في هذا التكوين غير قابل للتوجيه بشكل قانوني على الإنترنت. هم rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

### <u>التكوينات</u>

### <u>تكوين مركز VPN 3000</u>

أتمت هذا steps in order to شكلت ال VPN 3000 مركز:

1. انتقل إلى **التكوين > النظام > بروتوكولات الاتصال النفقي > IPSec LAN إلى LAN** لتكوين جلسة عمل الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN). قم بتعيين الخيارات الخاصة بخوارزميات المصادقة والتشغيل الفوري للبروتوكول IKE والمفتاح المشترك مسبقا وعنوان IP للنظير والمعلمات المحلية والبعيدة للشبكة. طقطقة **يطبق**.في هذا التكوين، تم تعيين المصادقة على أنها ESP-MD5-HMAC وتم تعيين التشفير على 3DES.

Configuration   System   Tunneling Protocols   IPSec LAN-to	p-LAN   Modify
Modify an IPSec LAN-to-LAN connection.	
Name Checkpoint	Enter the name for this LAN-to-LAN connection.
Interface Ethernet 2 (Public) (172.18.124.131) 💌	Select the interface to put this LAN-to-LAN connection on.
Peer 172.18.124.157	Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital None (Use Preshared Keys) -	Select the Digital Certificate to use.
Certificate  Certi	Choose how to send the digital certificate to the IKE peer.
Preshared Key ciscortprules	Enter the preshared key for this LAN-to-LAN connection.
Authentication ESP/MD6/HMAC-128 💌	Specify the packet authentication mechanism to use.
Encryption 3DES-168	Specify the encryption mechanism to use.
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.
Routing None	Choose the routing mechanism to use.Parameters below are ignored if Network Autodiscovery is chosen.
Local Network	
Network List Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 192.168.10.0	Note: Enter a wildcard mark, which is the reverse of a subnet mark. A
Wildcard Mask 0.0.0.256	wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Remote Network	
Network List Use IP Address/Wildcard-mask below 💌	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 10.32.0.0 Wildcard Mask 0.0.127.255	Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match.
Apply Cancel	For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

2. انتقل إلى **التكوين > النظام > بروتوكولات الاتصال النفقي > IPSec > مقترحات IKE** وقم بتعيين المعلمات المطلوبة.حدد مقترح IKE-3DES-MD5 وتحقق من المعلمات المحددة للمقترح. طقطقة **يطبق** in order to شكلت ال LAN إلى LAN جلسة.هذه هي معلمات هذا

		التكوين:
Configuration   System   Tunneling Protocols   IPSec   IKE F	Proposals   Modify	
Modify a configured IKE Proposal.		
Proposal Name IKE-3DES-MD5	Specify the name of this IKE Proposal.	
Authentication Mode Preshared Keys	Select the authentication mode to use.	
Authentication Algorithm MD5/HMAC-128 -	Select the packet authentication algorithm to use.	
Encryption Algorithm 3DES-168 -	Select the encryption algorithm to use.	
Diffie-Hellman Group Group 2 (1024-bits)	Select the Diffie Hellman Group to use.	
Lifetime Measurement Time	Select the lifetime measurement of the IKE keys.	
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).	
Time Lifetime 86400	Specify the time lifetime in seconds.	
Apply Cancel		

#### Configuration | Policy Management | Traffic Management | Security Associations

Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IKE Proposals to negotiate IKE parameters.

Click Add to add an SA, or select an SA and click Modify or Delete.



#### هذه هي المعلمات ل

			:SA
Configuration   Policy Manag	gement   Traffic Management   S	Security Associations   Modify	
Modify a configured Securit	y Association.		
SA Name	L2L: Checkpoint	Specify the name of this Security Association (SA).	
Inheritance	From Rule ·	Select the granularity of this SA.	
IPSec Parameters			
Authentication Algorithm	ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.	
Encryption Algorithm	3DES-168 •	Select the ESP encryption algorithm to use.	
Encapsulation Mode	Tunnel -	Select the Encapsulation Mode for this SA.	
<b>Perfect Forward Secrecy</b>	Disabled •	Select the use of Perfect Forward Secrecy.	
Lifetime Measurement	Time •	Select the lifetime measurement of the IPSec keys.	
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).	
Time Lifetime	86400	Specify the time lifetime in seconds.	
IKE Parameters			
IKE Peer	172.18.124.157	Specify the IKE Peer for a LAN-to-LAN IPSec connection.	
Negotiation Mode	Main 💌	Select the IKE Negotiation mode to use.	
<b>Digital Certificate</b>	None (Use Preshared Keys) 💌	Select the Digital Certificate to use.	
Certificate Transmission	<ul> <li>Entire certificate chain</li> <li>Identity certificate only</li> </ul>	Choose how to send the digital certificate to the IKE peer.	
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use as IKE initiator.	
Apply Cancel			

#### <u>تكوين NG لنقطة التحقق</u>

يتم تحديد كائنات الشبكة وقواعدها على نقطة الوصول NG لإنشاء السياسة المتعلقة بتكوين شبكة VPN الذي سيتم إعداده. يتم بعد ذلك تثبيت هذا النهج مع محرر نهج NG الخاص بنقطة التحقق لإكمال جانب NG لنقطة التحقق من التكوين.

1. قم بإنشاء كائني الشبكة لشبكة NG نقطة الوصول وشبكة مركز VPN التي ستقوم بتشفير حركة المرور المفيدة.لإنشاء كائنات، حدد **إدارة > كائنات الشبكة**، ثم حدد **جديد > شبكة**. أدخل معلومات الشبكة المناسبة، ثم انقر على موافق.تظهر هذه الأمثلة مجموعة من كائنات الشبكة تسمى CP\_Inside (الشبكة الداخلية لنقطة التحكم NG) و CONC\_INSIDE (الشبكة الداخلية لمركز

N	etwork Proper	ties - CP_inside		×
	General NAT	1		
	<u>N</u> ame:	CP_inside		
	IP <u>A</u> ddress:	10.32.0.0		
	Net <u>M</u> ask:	255.255.128.0		
	<u>C</u> omment:	CPINSIDE		
	Color:	<b></b>		
	Broadcast	address: ed <u>O No</u> t included		
		OK Cancel	Help	(Vi

Network Pro	perties - CONC_INSIDE	×
General	AT	
<u>N</u> ame:		
IP <u>A</u> ddre	ess: 192.168.10.0	
Net <u>M</u> a:	:k: 255.255.255.0	
<u>C</u> ommer	nt: Concentrator network	
Color:		
⊡Broad	cast address: kluded <u>O No</u> t included	
	OK Cancel Help	

2. انتقل إلى **إدارة > كائنات الشبكة** وحدد **جديد > محطة عمل** لإنشاء كائنات محطة عمل لأجهزة الشبكة الخاصة الظاهرية (VPN)، نقطة الوصول NG ومركز الشبكة الخاصة الظاهرية (VPN).**ملاحظة:** يمكنك إستخدام كائن محطة العمل NG لنقطة الوصول الذي تم إنشاؤه أثناء إعداد NG لنقطة الوصول الأولية. حدد الخيارات لتعيين محطة العمل كبوابة وجهاز VPN قابل للتشغيل البيني، ثم انقر فوق **موافق**.تظهر هذه الأمثلة مجموعة الكائنات التي تسمى CiscoCcp (نقطة الوصول NG) و Cisco\_CONC (مركز VPN)

Workstation Properties - (	сізсоср
Workstation Properties - ( General - Topology - NAT - VPN - Authentication - Management - Advanced	Seneral         Name:       ciscoop         IP Address:       172.18.124.157         Get address:       comment:         Checkpoint External IP         Color:       Image: Color Co
	Communication DN: cn=cp_mgmt,o=ciscocppvzfoa
	OK Cancel Help

Workstation Properties - (	CISCO_CONC	×
General Topology	General	
NAT	Name: CISCO_CONC	
	IP Address: 172.18.124.131 Get address	
	Comment: VPN Concentrator	
	Color:	
	Type: C <u>H</u> ost C Gate <u>w</u> ay	
	Check Point Products	
	Check Point products installed: Version NG Cet Version	
	□VPN-1 & FireWall-1 □FloodGate-1 □Policy Server □Management Station	
	Object Management	
	C Managed by this Management Server (Internal)	
	C Managed by another Management Server (External)	
	Interoperable ⊻PN Device      OK Cancel Help	1

3. انتقل إلى **إدارة > كائنات الشبكة > تحرير** لفتح نافذة خصائص محطة العمل الخاصة بمحطة العمل NG نقطة التحقق (CiscoPlug في هذا المثال). حدد **المخطط** من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد الشبكة التي سيتم تشفيرها. طقطقة **يحرر** in order to ثبتت القارن خاصية.في هذا المثال، CP\_Inside هو الشبكة الداخلية ل NG لنقطة التحقق.

orkstation Properties - c	iscocp				×
General	Topology				
Topology NAT	<u>G</u> et Interfaces	J			
VPN	Name	IP Address	Network Mask	IP Addresses behind	
- Authentication	E100B0	10.32.50.50	255.255.128.0	CP inside	
─ Management	E100B1	172.18.124.157	255.255.255.0	External	
	•				
	Add Show all IPs beh VPN Domain — All IP Addresse information. Manually Defin	<u>E</u> dit hind Gateway es <u>b</u> ehind Gateway b hed	Ased on Topology	≥now Show Show	
			OK C	Cancel Help	

4. في نافذة خصائص الواجهة، حدد الخيار لتعيين محطة العمل كمحطة عمل داخلية، ثم حدد عنوان IP المناسب. وانقر فوق OK.تعين تحديدات المخطط المعروضة محطة العمل كمحطة عمل داخلية وتحدد عناوين IP خلف

Interface Properties	
General Topology QoS	
Topology	
C External (leads out to the internet)	
Internal (leads to the local network)	
IP Addresses behind this interface:	
C Not 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	·CP Inside as

5. من نافذة "خصائص محطة العمل"، حدد الواجهة الخارجية على نقطة التفتيش NG التي تؤدي إلى الإنترنت، ثم انقر فوق **تحرير** لتعيين خصائص الواجهة. حدد الخيار لتعيين المخطط كمخطط خارجي، ثم انقر فوق

Interface Properties
General Topology QoS
Topology
External leads out to the internet!
Internal (leads to the local network)
IP Addresses behind this interface:
C Not Defined
C Network defined by the interface IP and Net Mask
C Specific:
Anti-Spoofing
Perform Anti-Spoofing based on interface topology
Spoof Tracking: ON <u>o</u> ne
OK Cancel Help

6. منّ نافذة خصائص محطة العمل الموجودة على نقطة التفتيش NG، حدد VPN من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد معلمات IKE لخوارزميات التشفير والمصادقة. طقطقة **يحرر** in order to شكلت ال ike سكلت ال

خاصية.

Workstation Properties -	ciscocp	×
General Topology NAT NAT Authentication Management Advanced	VPN   Encryption genemes   Image:	
	Nickname DN Certificate Authority	
	Add Egit Hemove	
	OK Cancel Help	

7. اضبط خصائص IKE لتطابق الخصائص على مركز VPN.في هذا المثال، حدد خيار التشفير ل **3DES** وخيار

IKE Properties		×
General		
Support key exchange encryption	with: Support data int	egrity with: —
Support authentication methods:		
✓ Pre-Shared Secret	Edit <u>S</u> ecrets	
Public <u>K</u> ey Signatures	Specify	
□ VPN-1 & FireWall-1 authenti	cation for SecuRemote (Hy	brid Mode)
	<u>A</u> d	vanced
ОК	Cancel Help	1

8. حدد خيار المصادقة **للأسرار المشتركة مسبقا**، ثم انقر **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا ليكون متوافقا مع المفتاح المشترك مسبقا على مركز VPN. طقطقة **يحرر** in order to دخلت مفتاحك كما هو موضح، بعد ذلك طقطقت **محموعة**،

		بالمقطقات مجموعة،	بعدد
Shar	ed Secret	×	1
<u>ج</u>	Shared Secrets List:		
	Peer Name Shared Secret CISCO_CONC ****	<u>E</u> dit <u>R</u> emove	
	Enter secret: ciscortprules Set		
	OK Cancel	<u>H</u> elp	ok

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**.عندما تنتهي، انقر **موافق**،

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)	
		36 DILJ	
Rekeying Parameters			
Renegotiate IKE security associ	ations	1440 📫	Minutes
Renegotiate IPSEC Security ass	ociations every	3600 🗦	Seconds
Renegotiate IPSEC Security	associations ever	y 50000 🚊	KBytes
Misc			
Support IP <u>c</u> ompression for S	SecureClient		
Support <u>agg</u> resive mode			
Support key exchange for su	ibnets		
ОК	Cancel	Help	
			ى.ا

10. انتقل إلى **إدارة > كائنات الشبكة > تحرير** لفتح نافذة خصائص محطة العمل لتركيز الشبكة الخاصة الظاهرية (VPN). أخترت **طوبولوجيا** من الخيار على الجانب الأيسر من النافذة in order to عينت يدويا ال VPN مجال.في هذا المثال، يتم تعريف CONC\_INSIDE (الشبكة الداخلية من مركز VPN) على أنها مجال شبكة VPN.

Workstation Properties - C	ISCO_CONC				×
- General	Topology				
Topology NAT	<u>G</u> et Interfaces	]			
- VPN Advanced	Name	IP Address	Network Mask		
	Add	Edt	<u>B</u> emove <u>S</u> h	OW	
	S <u>h</u> ow all IPs be	hind Gateway			
	VPN Domain				
	information.	es <u>p</u> enind Gateway b	ased on 1 opology	Show	
	Manually Defi	ned + CONC_INS	IDE 💌	Sho <u>w</u>	
	Exportable for	SecuRemote			
		_			
			OK Ca	ncel Help	

11. حدد **VPN** من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد **IKE** كمخطط تشفير. طقطقة **يحرر** in order to شكلت ال ike خاصية.

Workstation Properties - (	ISCO_CONC			×
General Topology NAT Advanced	VPN         Encryption schemes         Image: market transmission schemes         Image: market transmission schemes         Image: market transmission schemes			
		OK	Cancel	Help

12. قم بتعيين خصائص IKE لتعكس التكوين الحالي على مركز VPN.في هذا المثال، قم بتعيين خيار التشفير ل 3DES وخيار التجزئة ل

KE Properties	×
General	
Support key exchange encryption v	with:
	✓ MD <u>5</u>
I I I I I I I I I I I I I I I I I I I	SHA1
Support authentication methods:	
Pre-Shared Secret	Edit <u>S</u> ecrets
Public <u>K</u> ey Signatures	<u>Matching Criteria</u>
PN-1 & FireWall-1 authentica	ation for SecuRemote (Hybrid Mode)
	Advanced
OK Ca	ancel Help

13. حدد خيار المصادقة **للأسرار المشتركة مسبقا**، ثم انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا. طقطقة **يحرر** in order to دخلت مفتاحك كما هو موضح، بعد ذلك طقطقت **مجموعة**،

1	×		Shared Secret
			Shared Secrets List:
		Shared Secret	Peer Name
	<u>E</u> dit	****	ciscocp
	<u>R</u> emove		
		rtprules <u>Set</u>	
	Help	Cancel	ок
	<u>E</u> dit <u>R</u> emove	rtprules Set	Enter secret: cisc

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**.عندما تنتهي، انقر **موافق**،

✓ Use UDP encapsulation	-
UDP_VPN1_IPSEC_encapsu 🔽	
Support Diffie-Hellman groups	- 1
Group 1 (768 bit)	
Group 2 (1024 bit)	
Rekeying Parameters	—
Renegotiate IKE security associations 🛛 🗧 🕺 Minu	tes
Renegotiate IPSEC Security associations every 🛛 3600 🛛 🚍 Seco	nds
🔲 Renegotiate IPSEC Security associations every 50000 🛛 📇 KByte	es
Mise	_
Support aggressive mode	
Support key exchange for subnets	
OK Cancel Help	

15. حدد **قواعد > إضافة قواعد > أعلى** لتكوين قواعد التشفير للنهج. في نافذة "محرر النهج"، قم بإدراج قاعدة بمصدر على هيئة CP\_Inside (داخل شبكة من NG لنقطة التفتيش) والوجهة على هيئة CONC\_INSIDE (داخل الشبكة من مركز VPN). 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** 

			الحصائص.
CISCOCP - Check Point Policy Editor	Standard		
File Edit View Manage Rules Policy	Fopology Search Window Help		
] ■ ●   苯吗 晰  ] 4 極 復	▲│□│見⋶⋍ぇぇ∝│♥╽お	54 L	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	QQ 🖾 💊 🖾 🖻		
\$ € 4 0 8 8 8 0 %	🗱 Security - Standard 🗮 Address Translation - Standard	💭 QoS - Standard 🔟 Desktop Se	ecurity - Standard
Vetwork Objects     Workstation	NO. SOURCE DESTINATION S	ERVICE ACTION	TRACK INSTALL
CISCO_CONC	1 <sup>V</sup> CP_inside <sup>V</sup> CONC_NSDE * An V CONC_NSDE <sup>V</sup> CP_inside <sup>*</sup>	W CE Edit propert	ies Galeway
	2 4 CP_inside * Any * An	W Add Encrypt	Cateway
Image: Construction       Image: Const	Name IP	Comment	ath
	CISCO_CONC 172.18.124.131	VPN Concentrator Checkpoint Externe Query Colu Clear Query	и инг

Encryption	n Properties			×
General				
Encr C	yption <u>s</u> chemes defi ME M2 FWZ	ined: —		
	<u>E</u> dit			
	ОК	Cancel	Help	

- 16. حدد **IKE** وانقر **تحرير.ا**
- 17. في نافذة خصائص IKE، قم بتغيير الخصائص لتوافق مع تحويل مركز VPN.اضبط خيار التحويل على **التشفير** + تكامل البيانات (ESP).تعيين خوارزمية التشفير على 3DES.تعيين تكامل البيانات على MD5.قم بتعيين بوابة النظير المسموح بها لتطابق مركز VPN (Cisco CONC) عندما تنتهي انقر فوق.

۱۱ ):عندت شهي، الغر دوق		مستقل بها تتعابق
IKE Properties		×
General		
Transform		
Encryption + Data Integril	y (ESP)	
O Data Integrity Only (AH)		
Encryption Algorithm:	3DES	<b>_</b>
<u>D</u> ata Integrity	MD5	
<u>Compression method:</u>	, None	
Allowed Peer Gateway:		•
Use Perfect Forward Secrecy		
Use DH <u>G</u> roup:	Group 1 (768 bit)	<b>_</b>
── Perform IP <u>P</u> ool NAT		
OK Ca	ancel Help	

18. بعد تكوين NG لنقطة التحقق، احفظ النهج وحدد **نهج > تثبيت** لتمكينه.

CISCOCP - Check Point Policy	Editor - Standard				2	
File Edit View Manage Rules	Policy Topology Search Window	Help				
Image: Second system         Image: S		ddress Translation - Sta	andard 🔐 QoS - St	andard 🛙 🛄 Desktop S	ecurity - Standard	
Network Objects	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL OF
CISCO_CONC	Management High Availability	쑤 CONC_INSIDE 쑤 CP_Inside	<b>*</b> Αειγ	C Encrypt	🔲 Log	Gateways
-++ CONC_INSIDE	2 ++ CP_inside	* Any	* Any	G accept	Log	C Gateways
Domain     OSE Device     Embedded Device     Group     Uogical Server     Address Range						
Gateway Cluster						•
Dynamic Object	Name	IP	Comment			
		172.18.1 172.18.1	24.131 VPN Conce 24.157 Checkpoint	ntrator t External IP		

		أثناء تحويل النهج	ت ملاحظات التقدم	تعرض نافذة التثبيا
Install Policy				×
Standard.W: Security Policy S Standard: Compiled OK.	cript generated i	nto Standard.pf		
<u>र</u>				<b>&gt;</b>
	( <u>A</u> bo	rt		ر محیا.
	ل <b>إغلاق</b> لإنهاء	بيت النهج، انقر فوق	لتثبيت إلى اكتمال تثر	عندما تشير نافذة ا

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	
<u>Close</u>	

### <u>التحقق من الصحة</u>

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

<u>التحقق من اتصال الشبكة</u>

لاختبار الاتصال بين الشبكتين الخاصتين، يمكنك بدء إختبار اتصال من إحدى الشبكات الخاصة إلى الشبكة الخاصة الأخرى. في هذا التكوين، تم إرسال إختبار اتصال من جانب NG في نقطة التفتيش (10.32.50.51) إلى شبكة مركز VPN (192.168.10.2).

```
C:\WINNT\System32\cmd.exe
```

C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\>ping 192.168.10.2 Pinging 192.168.10.2 with 32 bytes of data: Reply from 192.168.10.2: bytes=32 time=10ms TTL=253 Reply from 192.168.10.2: bytes=32 time=10ms TTL=253 Reply from 192.168.10.2: bytes=32 time<10ms TTL=253 Reply from 192.168.10.2: bytes=32 time<10ms TTL=253 Ping statistics for 192.168.10.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = 10ms, Average = 5ms C:\> C:\> C:\> C:\>

<u>عرض حالة النفق على نقطة التفتيش NG</u>

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

CISCOCP - Check Point System Stat	us			
Eile View Modules Products Iools W	jindow <u>H</u> elp			
🕽 🗉 🖻 🛝 🛄 🔦 📟 🇞	💂 🚅 🎯 😤	54		
Modules	IP Address	VPN-1 Details		
E-12 CISCOCP		Status:	ок	
E- Ciscocp	172.18.124.157	Packets		
FireWal-1		Encrypted:	19	
FloodGate-1		Decrypted:	18	
- 👷 Management	1	Errors		
SVN Foundation		Encryption errors:	0	
		Decryption errors:	0	
		IKE events errors:	3	
		Hardware		
	- 1	HW Vendor Name:	none	
	- 1	HW Status:	none	
	1			
	1			
For Help, press F1				Last updated:09:34:14 PM

### <u>عرض حالة النفق على مركز VPN</u>

#### للتحقق من حالة النفق على مركز VPN، انتقل إلى **الإدارة > جلسات الإدارة**.

dministration   Adm	nister Sessions				1	Vednes	day, 11 Sept	ember 2002 20:37:0 Reset @ Refresh	
his screen shows st formation on a sess onnection to a session	atistics for sessions. ion, click on that sess on, click <b>Ping</b> .	To refresh the statist sion's name. To log o	ics, click <b>Refre</b> out a session, cl	sh. Sel ick Log	ect a Group gout in the tal	to filter ble belo	the sessions w. To test th	. For more e network	
roup [All ogout All: <u>PPTP U</u> Session Summa	er   L2TP User   IPS	ec User   L2TP/IPSe	c User   IPSec/U	DP Us	er   IPSec/TC	<u>P User</u>	PSec LAN	-to-LAN	
Active LAN-to- LAN Sessions	to- as Active Remote Access Sessions Active Access Sessions Sessions Sessions Sessions Active Access Sessions Sessions Sessions Sessions Active Sessions Sessions Sessions Sessions Sessions Active Sessions Sessions Sessions Sessions Sessions Sessions Sessions Sessions Sessions Sessions Session								
1	0	3	4		4	1	1500	17	
	die eerden wije die eerden were die eerden die die die die								
LAN-to-LAN S	essions	Protoso	Encor	mtlen	[ Remote Ac	cess Se	ssions   Mana	agement Sessions ]	
LAN-to-LAN S Connection Nan	essions le IP Address	Protocol IPSec/LAN-to-L	I Ener	yption	[ Remote Ac	cess Sei Ime	ssions   Mana	Actions	

تحت جلسات عمل الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN)، حدد اسم الاتصال لنقطة التفتيش لعرض التفاصيل حول شبكات SA التي تم إنشاؤها وعدد الحزم التي تم إرسالها/استقبالها.

C1							<b>n</b>					
Connection Name	IP Add	ress	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Ry				
Checkpoint	172.18.124	4.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	25				
1	Session ID	1		- Stonen	Encryption Algorit	hm 3DES-1	68					
			IK	E Session								
	Session ID	1 MD4			Encryption Algorithm 3DES-168							
Hashing Algorithm MI				Diffie-Heilman Group Group 2 (1024-bit)								
Authentica	tion Mode	Pre-Sha	red Keys	I	KE Negotiation Me	ode Main						
Rekey Tin	e Interval	86400 s	econds									
			IPS	ec Session								
1	Session ID	2			Remote Address 10.32.0.0/0.0.127.255							
Local Address 192.168.10.0/0.0.0.255				Encryption Algorithm 3DES-168								
Hashing	Algorithm	MD5			S	EP 1	P 1					
Encapsula	tion Mode	Tunnel			Rekey Time Interval 28800 seconds							
		484										

## <u>استكشاف الأخطاء وإصلاحها</u>

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

**ملاحظة:** يجب ألا يتم تحديد حركة المرور عبر نفق IPSec باستخدام عنوان IP العام لمركز بيانات الشبكة الخاصة الظاهرية (الواجهة الخارجية). وإلا فسيفشل النفق. لذلك، العنوان يستعمل ل PATing ينبغي كنت عنوان غير العنوان يشكل على القارن خارجي.

### <u>تلخيص الشبكة</u>

عندما يتم تكوين شبكات متعددة متجاورة، داخل الشبكات في مجال التشفير على نقطة التحقق، يمكن للجهاز تلخيص الشبكات تلقائيا فيما يتعلق بحركة المرور المفيدة. إذا لم يتم تكوين مركز الشبكة الخاصة الظاهرية (VPN) ليتطابق، فمن المحتمل أن يفشل النفق. على سبيل المثال، إذا تم تكوين الشبكات الداخلية من 10.0.00 /24 و 10.0.1.0 /24 لتضمينها في النفق، فيمكن تلخيص هذه الشبكات إلى 10.0.0.0 /23.

### <u>تصحيح أخطاء NG لنقطة التفتيش</u>

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

ā	TiscocP - Check Point Log Viewer - [fw.log]												×			
Ele	Ele Mode Edit Selection View Iools Window Help												1.1			
6	🕼 🖆 🖬 Log 🔄 🛥 🗛 🖣 🛓 🖆 🖩 🖬 😸 🗐 🎬 🛱 🌭 🖓 📲 🐁 🕙 👘															
	Date	Time	Product	1.1.1	Inter.	Orig	Туре	Action	Source	Destinati	Pr.,	Rule	S_Port	SrcKeyID	DstKeyID	×
1	13Aug2002	21:32:	VPN-1	& FireIV	📻 dae	ciscocp	📕 log	0- key instali	ciscoop	CISCO_CONC						
2	13Aug2002	21:32:	VPN-1	& FireVV	🕒 dae	ciscocp	🔲 log	Ove key instal	ciscocp	CISCO_CONC				0x5879f30d	0xt1351129	

### <u>تصحيح أخطاء مركز VPN</u>

لتمكين تصحيح الأخطاء على مركز VPN، انتقل إلى **التكوين > النظام > الأحداث > الفئات**. قم بتمكين المصادقة و

#### authdbg و ike و ikedbg و iPSec و IPSECDBG من حيث الخطورة للتسجيل من 1 إلى 13. لعرض تصحيح الأخطاء، حدد **مراقبة > سجل أحداث قابل للتصفية**.

SEV=8 IKEDBG/0 RPT=506 172.18.124.157 20:36:03.610 09/11/2002 1 : RECEIVED Message (msgid=0) with payloads HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128 SEV=9 IKEDBG/0 RPT=507 172.18.124.157 20:36:03.610 09/11/2002 3 processing SA payload SEV=8 IKEDBG/0 RPT=508 20:36:03.610 09/11/2002 4 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE :Parsing received transform :Phase 1 failure against global IKE proposal # 1 :Mismatched attr types for class Auth Method Rcv'd: Preshared Key (Cfg'd: XAUTH with Preshared Key (Initiator authenticated SEV=8 IKEDBG/0 RPT=509 20:36:03.610 09/11/2002 10 :Phase 1 failure against global IKE proposal # 2 :Mismatched attr types for class DH Group Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 SEV=7 IKEDBG/0 RPT=510 172.18.124.157 20:36:03.610 09/11/2002 13 Oakley proposal is acceptable SEV=9 IKEDBG/47 RPT=9 172.18.124.157 20:36:03.610 09/11/2002 14 processing VID payload SEV=9 IKEDBG/0 RPT=511 172.18.124.157 20:36:03.610 09/11/2002 15 processing IKE SA SEV=8 IKEDBG/0 RPT=512 20:36:03.610 09/11/2002 16 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE :Parsing received transform :Phase 1 failure against global IKE proposal # 1 :Mismatched attr types for class Auth Method Rcv'd: Preshared Kev (Cfg'd: XAUTH with Preshared Key (Initiator authenticated SEV=8 IKEDBG/0 RPT=513 20:36:03.610 09/11/2002 22 :Phase 1 failure against global IKE proposal # 2 :Mismatched attr types for class DH Group Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 20:36:03.610 09/11/2002 25 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3 SEV=9 IKEDBG/0 RPT=514 172.18.124.157 20:36:03.610 09/11/2002 26 constructing ISA\_SA for isakmp SEV=8 IKEDBG/0 RPT=515 172.18.124.157 20:36:03.610 09/11/2002 27 : SENDING Message (msgid=0) with payloads HDR + SA (1) + NONE (0) ... total length : 84 SEV=8 IKEDBG/0 RPT=516 172.18.124.157 20:36:03.630 09/11/2002 29 : RECEIVED Message (msgid=0) with payloads HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

SEV=8 IKEDBG/0 RPT=517 172.18.124.157 20:36:03.630 09/11/2002 31 : RECEIVED Message (msgid=0) with payloads HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 20:36:03.630 09/11/2002 33 processing ke pavload SEV=9 IKEDBG/0 RPT=519 172.18.124.157 20:36:03.630 09/11/2002 34 processing ISA\_KE SEV=9 IKEDBG/1 RPT=91 172.18.124.157 20:36:03.630 09/11/2002 35 processing nonce payload SEV=9 IKEDBG/0 RPT=520 172.18.124.157 20:36:03.660 09/11/2002 36 constructing ke pavload SEV=9 IKEDBG/1 RPT=92 172.18.124.157 20:36:03.660 09/11/2002 37 constructing nonce payload SEV=9 IKEDBG/46 RPT=37 172.18.124.157 20:36:03.660 09/11/2002 38 constructing Cisco Unity VID payload SEV=9 IKEDBG/46 RPT=38 172.18.124.157 20:36:03.660 09/11/2002 39 constructing xauth V6 VID payload SEV=9 IKEDBG/48 RPT=19 172.18.124.157 20:36:03.660 09/11/2002 40 Send IOS VID SEV=9 IKEDBG/38 RPT=10 172.18.124.157 20:36:03.660 09/11/2002 41 , Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0 (capabilities: 20000001 SEV=9 IKEDBG/46 RPT=39 172.18.124.157 20:36:03.660 09/11/2002 43 constructing VID payload SEV=9 IKEDBG/48 RPT=20 172.18.124.157 20:36:03.660 09/11/2002 44 Send Altiga GW VID SEV=9 IKEDBG/0 RPT=521 172.18.124.157 20:36:03.660 09/11/2002 45 ... Generating keys for Responder SEV=8 IKEDBG/0 RPT=522 172.18.124.157 20:36:03.670 09/11/2002 46 : SENDING Message (msgid=0) with payloads HDR + KE (4) + NONCE (10) ... total length : 256 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 20:36:03.690 09/11/2002 48 : RECEIVED Message (msgid=0) with payloads HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 20:36:03.690 09/11/2002 50 [Group [172.18.124.157 Processing ID SEV=9 IKEDBG/0 RPT=524 172.18.124.157 20:36:03.690 09/11/2002 51 [Group [172.18.124.157 processing hash SEV=9 IKEDBG/0 RPT=525 172.18.124.157 20:36:03.690 09/11/2002 52 [Group [172.18.124.157 computing hash SEV=9 IKEDBG/23 RPT=10 172.18.124.157 20:36:03.690 09/11/2002 53 [Group [172.18.124.157 Starting group lookup for peer 172.18.124.157

SEV=8 AUTHDBG/1 RPT=10 20:36:03.690 09/11/2002 54 AUTH\_Open() returns 9 SEV=7 AUTH/12 RPT=10 20:36:03.690 09/11/2002 55 Authentication session opened: handle = 9 SEV=8 AUTHDBG/3 RPT=10 20:36:03.690 09/11/2002 56 (AUTH\_PutAttrTable(9, 748174 SEV=8 AUTHDBG/6 RPT=10 20:36:03.690 09/11/2002 57 (AUTH\_GroupAuthenticate(9, 2f1b19c, 49c648 SEV=8 AUTHDBG/59 RPT=10 20:36:03.690 09/11/2002 58 (AUTH\_BindServer(51a6b48, 0, 0 SEV=9 AUTHDBG/69 RPT=10 20:36:03.690 09/11/2002 59 Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1 SEV=8 AUTHDBG/65 RPT=10 20:36:03.690 09/11/2002 60 (AUTH\_CreateTimer(51a6b48, 0, 0 SEV=9 AUTHDBG/72 RPT=10 20:36:03.690 09/11/2002 61 Reply timer created: handle = 4B0018 SEV=8 AUTHDBG/61 RPT=10 20:36:03.690 09/11/2002 62 (AUTH\_BuildMsg(51a6b48, 0, 0 SEV=8 AUTHDBG/64 RPT=10 20:36:03.690 09/11/2002 63 (AUTH\_StartTimer(51a6b48, 0, 0 SEV=9 AUTHDBG/73 RPT=10 20:36:03.690 09/11/2002 64 ,Reply timer started: handle = 4B0018, timestamp = 1163319 timeout = 30000SEV=8 AUTHDBG/62 RPT=10 20:36:03.690 09/11/2002 65 (AUTH\_SndRequest(51a6b48, 0, 0 SEV=8 AUTHDBG/50 RPT=19 20:36:03.690 09/11/2002 66 (IntDB\_Decode(3825300, 156 SEV=8 AUTHDBG/47 RPT=19 20:36:03.690 09/11/2002 67 (IntDB\_Xmt(51a6b48 SEV=9 AUTHDBG/71 RPT=10 20:36:03.690 09/11/2002 68  $xmit_cnt = 1$ SEV=8 AUTHDBG/47 RPT=20 20:36:03.690 09/11/2002 69 (IntDB\_Xmt(51a6b48 SEV=8 AUTHDBG/49 RPT=10 20:36:03.790 09/11/2002 70 (IntDB\_Match(51a6b48, 3eb7ab0 SEV=8 AUTHDBG/63 RPT=10 20:36:03.790 09/11/2002 71 (AUTH\_RcvReply(51a6b48, 0, 0 SEV=8 AUTHDBG/50 RPT=20 20:36:03.790 09/11/2002 72 (IntDB Decode(3eb7ab0, 298 SEV=8 AUTHDBG/48 RPT=10 20:36:03.790 09/11/2002 73 (IntDB\_Rcv(51a6b48 SEV=8 AUTHDBG/66 RPT=10 20:36:03.790 09/11/2002 74 (AUTH\_DeleteTimer(51a6b48, 0, 0

SEV=9 AUTHDBG/74 RPT=10 20:36:03.790 09/11/2002 75 Reply timer stopped: handle = 4B0018, timestamp = 1163329 SEV=8 AUTHDBG/58 RPT=10 20:36:03.790 09/11/2002 76 (AUTH\_Callback(51a6b48, 0, 0 SEV=6 AUTH/41 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 77 ,Authentication successful: handle = 9, server = Internal group = 172.18.124.157SEV=7 IKEDBG/0 RPT=526 172.18.124.157 20:36:03.790 09/11/2002 78 [Group [172.18.124.157 (Found Phase 1 Group (172.18.124.157 SEV=8 AUTHDBG/4 RPT=10 20:36:03.790 09/11/2002 79 (AUTH\_GetAttrTable(9, 748420 SEV=7 IKEDBG/14 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 80 [Group [172.18.124.157 Authentication configured for Internal SEV=9 IKEDBG/19 RPT=19 172.18.124.157 20:36:03.790 09/11/2002 81 [Group [172.18.124.157 IKEGetUserAttributes: IP Compression = disabled SEV=9 IKEDBG/19 RPT=20 172.18.124.157 20:36:03.790 09/11/2002 82 [Group [172.18.124.157 IKEGetUserAttributes: Split Tunneling Policy = Disabled SEV=8 AUTHDBG/2 RPT=10 20:36:03.790 09/11/2002 83 (AUTH\_Close(9 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 20:36:03.790 09/11/2002 84 [Group [172.18.124.157 constructing ID SEV=9 IKEDBG/0 RPT=527 20:36:03.790 09/11/2002 85 [Group [172.18.124.157 construct hash payload SEV=9 IKEDBG/0 RPT=528 172.18.124.157 20:36:03.790 09/11/2002 86 [Group [172.18.124.157 computing hash SEV=9 IKEDBG/46 RPT=40 172.18.124.157 20:36:03.790 09/11/2002 87 [Group [172.18.124.157 constructing dpd vid payload SEV=8 IKEDBG/0 RPT=529 172.18.124.157 20:36:03.790 09/11/2002 88 : SENDING Message (msgid=0) with payloads HDR + ID (5) + HASH (8) ... total length : 80 SEV=4 IKE/119 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 90 [Group [172.18.124.157 PHASE 1 COMPLETED SEV=6 IKE/121 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 91 Keep-alive type for this connection: None SEV=6 IKE/122 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 92

Keep-alives configured on but peer does not

(support keep-alives (type = None

SEV=7 IKEDBG/0 RPT=530 172.18.124.157 20:36:03.790 09/11/2002 93 [Group [172.18.124.157 (Starting phase 1 rekey timer: 64800000 (ms SEV=4 AUTH/22 RPT=16 20:36:03.790 09/11/2002 94 User 172.18.124.157 connected SEV=8 AUTHDBG/60 RPT=10 20:36:03.790 09/11/2002 95 (AUTH\_UnbindServer(51a6b48, 0, 0 SEV=9 AUTHDBG/70 RPT=10 20:36:03.790 09/11/2002 96 Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0 SEV=8 AUTHDBG/10 RPT=10 20:36:03.790 09/11/2002 97 (AUTH\_Int\_FreeAuthCB(51a6b48 SEV=7 AUTH/13 RPT=10 20:36:03.790 09/11/2002 98 Authentication session closed: handle = 9 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 20:36:03.790 09/11/2002 99 : RECEIVED Message (msgid=54796f76) with payloads (HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0 total length : 156 ... SEV=9 IKEDBG/0 RPT=532 172.18.124.157 20:36:03.790 09/11/2002 102 [Group [172.18.124.157 processing hash SEV=9 IKEDBG/0 RPT=533 172.18.124.157 20:36:03.790 09/11/2002 103 [Group [172.18.124.157 processing SA payload SEV=9 IKEDBG/1 RPT=95 172.18.124.157 20:36:03.790 09/11/2002 104 [Group [172.18.124.157 processing nonce payload SEV=9 IKEDBG/1 RPT=96 172.18.124.157 20:36:03.790 09/11/2002 105 [Group [172.18.124.157 Processing ID SEV=5 IKE/35 RPT=6 172.18.124.157 20:36:03.790 09/11/2002 106 [Group [172.18.124.157 :Received remote IP Proxy Subnet data in ID Payload Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 20:36:03.790 09/11/2002 109 [Group [172.18.124.157 Processing ID SEV=5 IKE/34 RPT=6 172.18.124.157 20:36:03.790 09/11/2002 110 [Group [172.18.124.157 :Received local IP Proxy Subnet data in ID Payload Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0 SEV=8 IKEDBG/0 RPT=534 20:36:03.790 09/11/2002 113 QM IsRekeyed old sa not found by addr SEV=5 IKE/66 RPT=8 172.18.124.157 20:36:03.790 09/11/2002 114 [Group [172.18.124.157 IKE Remote Peer configured for SA: L2L: Checkpoint

SEV=9 IKEDBG/0 RPT=535 172.18.124.157 20:36:03.790 09/11/2002 115 [Group [172.18.124.157 processing IPSEC SA

SEV=7 IKEDBG/27 RPT=8 172.18.124.157 20:36:03.790 09/11/2002 116 [Group [172.18.124.157 IPSec SA Proposal # 1, Transform # 1 acceptable SEV=7 IKEDBG/0 RPT=536 172.18.124.157 20:36:03.790 09/11/2002 117 [Group [172.18.124.157 !IKE: requesting SPI SEV=9 IPSECDBG/6 RPT=39 20:36:03.790 09/11/2002 118 ,IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000 ,seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0 ,spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0 lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300 SEV=9 IPSECDBG/1 RPT=139 20:36:03.790 09/11/2002 122 !Processing KEY\_GETSPI msg SEV=7 IPSECDBG/13 RPT=10 20:36:03.790 09/11/2002 123 Reserved SPI 305440147 SEV=8 IKEDBG/6 RPT=10 20:36:03.790 09/11/2002 124 IKE got SPI from key engine: SPI = 0x1234a593 SEV=9 IKEDBG/0 RPT=537 172.18.124.157 20:36:03.790 09/11/2002 125 [Group [172.18.124.157 oakley constucting quick mode SEV=9 IKEDBG/0 RPT=538 172.18.124.157 20:36:03.800 09/11/2002 126 [Group [172.18.124.157 constructing blank hash SEV=9 IKEDBG/0 RPT=539 172.18.124.157 20:36:03.800 09/11/2002 127 [Group [172.18.124.157 constructing ISA\_SA for ipsec SEV=9 IKEDBG/1 RPT=98 172.18.124.157 20:36:03.800 09/11/2002 128 [Group [172.18.124.157 constructing ipsec nonce payload SEV=9 IKEDBG/1 RPT=99 172.18.124.157 20:36:03.800 09/11/2002 129 [Group [172.18.124.157 constructing proxy ID SEV=7 IKEDBG/0 RPT=540 172.18.124.157 20:36:03.800 09/11/2002 130

[Group [172.18.124.157 :Transmitting Proxy Id Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0 Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

SEV=9 IKEDBG/0 RPT=541 172.18.124.157 20:36:03.800 09/11/2002 134 [Group [172.18.124.157 constructing qm hash

SEV=8 IKEDBG/0 RPT=542 172.18.124.157 20:36:03.800 09/11/2002 135 : SENDING Message (msgid=54796f76) with payloads HDR + HASH (8) + SA (1) ... total length : 152

SEV=8 IKEDBG/0 RPT=543 172.18.124.157 20:36:03.800 09/11/2002 137 : RECEIVED Message (msgid=54796f76) with payloads HDR + HASH (8) + NONE (0) ... total length : 48

SEV=9 IKEDBG/0 RPT=544 172.18.124.157 20:36:03.800 09/11/2002 139 [Group [172.18.124.157]

processing hash

SEV=9 IKEDBG/0 RPT=545 172.18.124.157 20:36:03.800 09/11/2002 140 [Group [172.18.124.157 loading all IPSEC SAs SEV=9 IKEDBG/1 RPT=100 172.18.124.157 20:36:03.800 09/11/2002 141 [Group [172.18.124.157 !Generating Quick Mode Key SEV=9 IKEDBG/1 RPT=101 172.18.124.157 20:36:03.800 09/11/2002 142 [Group [172.18.124.157 !Generating Quick Mode Key SEV=7 IKEDBG/0 RPT=546 172.18.124.157 20:36:03.800 09/11/2002 143 [Group [172.18.124.157 :Loading subnet Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0 SEV=4 IKE/49 RPT=7 172.18.124.157 20:36:03.800 09/11/2002 146 [Group [172.18.124.157 (Security negotiation complete for LAN-to-LAN Group (172.18.124.157 Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959 SEV=9 IPSECDBG/6 RPT=40 20:36:03.800 09/11/2002 149 , IPSEC key message parse - msgtype 1, len 606, vers 1, pid 0000000 ,seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0 ,spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3 lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 SEV=9 IPSECDBG/1 RPT=140 20:36:03.800 09/11/2002 153 !Processing KEY\_ADD msg SEV=9 IPSECDBG/1 RPT=141 20:36:03.800 09/11/2002 154 key\_msghdr2secassoc(): Enter SEV=7 IPSECDBG/1 RPT=142 20:36:03.800 09/11/2002 155 No USER filter configured SEV=9 IPSECDBG/1 RPT=143 20:36:03.800 09/11/2002 156 KeyProcessAdd: Enter SEV=8 IPSECDBG/1 RPT=144 20:36:03.800 09/11/2002 157 KeyProcessAdd: Adding outbound SA SEV=8 IPSECDBG/1 RPT=145 20:36:03.800 09/11/2002 158 ,KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255 dst 10.32.0.0 mask 0.0.127.255 SEV=8 IPSECDBG/1 RPT=146 20:36:03.810 09/11/2002 159 KeyProcessAdd: FilterIpsecAddIkeSa success SEV=9 IPSECDBG/6 RPT=41 20:36:03.810 09/11/2002 160 ,IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000 ,seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0 ,spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3 lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

> SEV=9 IPSECDBG/1 RPT=147 20:36:03.810 09/11/2002 164 !Processing KEY\_UPDATE msg

> SEV=9 IPSECDBG/1 RPT=148 20:36:03.810 09/11/2002 165 Update inbound SA addresses

SEV=7 IPSECDBG/1 RPT=150 20:36:03.810 09/11/2002 167 No USER filter configured

SEV=9 IPSECDBG/1 RPT=151 20:36:03.810 09/11/2002 168 KeyProcessUpdate: Enter

SEV=8 IPSECDBG/1 RPT=152 20:36:03.810 09/11/2002 169 KeyProcessUpdate: success

SEV=8 IKEDBG/7 RPT=7 20:36:03.810 09/11/2002 170
IKE got a KEY\_ADD msg for SA: SPI = 0x0df37959

SEV=8 IKEDBG/0 RPT=547 20:36:03.810 09/11/2002 171 pitcher: rcv KEY\_UPDATE, spi 0x1234a593

SEV=4 IKE/120 RPT=7 172.18.124.157 20:36:03.810 09/11/2002 172 [Group [172.18.124.157 (PHASE 2 COMPLETED (msgid=54796f76

### <u>معلومات ذات صلة</u>

- <u>صفحة دعم مركز Cisco VPN 3000 Series</u>
- <u>صفحة دعم عميل Cisco VPN 3000 Series</u>
  - <u>صفحة دعم IPSec</u>
  - <u>الدعم الفني Cisco Systems</u>

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