نم VPN 5000 زكرم - IPsec قفن نيوكت لوصولا ةطقنل 4.1 ةيامح رادج ىلإ

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات المكونات المستخدمة الاصطلاحات التكوين الرسم التخطيطي للشبكة التكوينات <u>جدار حماية نقطة التفتيش 4.1</u> التحقق من الصحة استكشاف الأخطاء وإصلاحها أوامر أستكشاف أخطاء مركز VPN 5000 وإصلاحها تلخبص الشبكة <u>تصحيح أخطاء جدار الحماية Checkpoint 4.1</u> إخراج تصحيح الأخطاء للعينة معلومات ذات صلة

<u>المقدمة</u>

يوضح هذا المستند كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للانضمام إلى شبكتين خاصتين. وهو ينضم إلى شبكة خاصة داخل مركز 192.168.1.x) (Cisco VPN 5000) إلى شبكة خاصة داخل جدار حماية نقطة التفتيش 4.1 (x.10.32.50). يفترض أن حركة المرور من داخل مركز الشبكة الخاصة الظاهرية (VPN) وداخل نقطة التفتيش إلى الإنترنت (ممثلة في هذا المستند بشبكات x.172.18.124) تتدفق قبل أن تبدأ هذا التكوين.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

لا توجد متطلبات خاصة لهذا المستند.

<u>المكونات المستخدمة</u>

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

- مرکز Cisco VPN 5000
- برنامج مركز Cisco VPN 5000 نسخة 5.2.19.0001

• جدار حماية نقطة التفتيش 4.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

<u>الاصطلاحات</u>

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

<u>التكوين</u>

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

<u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:



<u>التكوينات</u>

يستخدم هذا المستند هذا التكوين.

	مرکز Cisco VPN 5000
	[IP Ethernet 0:0]
Mode	= Routed
SubnetMask	= 255.255.255.0

```
IPAddress
                                         = 192.168.1.1
                                           [ General ]
         EthernetAddress
                                   = 00:00:a5:e9:c8:00
   DeviceType
                            = VPN 5002/8 Concentrator
 ConfiguredOn
                          = Timeserver not configured
ConfiguredFrom
                         = Command Line, from Console
                                     = "cisco_endpoint
          "DeviceName
             IPSecGateway
                                       = 172.18.124.34
                                        [ IKE Policy ]
                Protection
                                          = SHA_DES_G2
                              [ Tunnel Partner VPN 1 ]
                                               = 28800
                     KeyLifeSecs
          "LocalAccess
                                     = "192.168.1.0/24
           "Peer
                                      = "10.32.50.0/24
            "BindTo
                                       = "ethernet 1:0
              "SharedKey
                                         = "ciscorules
                                                 = Auto
                      KeyManage
              (Transform
                                         = esp(sha,des
                                      = 172.18.124.157
            Partner
                      Mode
                                                 = Main
                                          [ IP VPN 1 ]
                       Numbered
                                                  = Off
                    Mode
                                              = Routed
                                   [ IP Ethernet 1:0 ]
             IPAddress
                                       = 172.18.124.35
                                     = 255.255.255.240
           SubnetMask
                    Mode
                                              = Routed
                                         [ IP Static ]
                     VPN 1 1 255.255.255.0 10.32.50.0
       .Configuration size is 1131 out of 65500 bytes
```

جدار حماية نقطة التفتيش 4.1

أكمل الخطوات التالية لتكوين جدار حماية نقطة الوصول 4.1.

1. حدد **خصائص > تشفير** لتعيين فترات حياة IPsec لنقطة التحقق للاتفاق مع **KeyLifeSeconds = 28800** أمر مركز VPN.**ملاحظة:** أترك نقاط التفتيش فترات حياة تبادل مفاتيح الإنترنت (IKE) في الوضع الافتراضي.

Properties Setup	×
High Availability IP Pool NAT Acces Security Policy Traffic Control Services L Authentication SYNDefender LDAP	ss Lists Desktop Security .og and Alert Security Servers Encryption ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key :	Manual IPSEC SPI allocation range (hex):
Every120Seconds (0 for infinity)orEvery10485760Bytes (0 for infinity)	Erom 100 Lo ffff
IKE Renegotiate I <u>K</u> E Security Associations every	1440 minutes
Renegotiate I <u>P</u> SEC Security Associations every	28800 seconds
OK Cancel	Help

2. حدد **إدارة > كائنات الشبكة > جديد (أو تحرير) > الشبكة** لتكوين الكائن للشبكة الداخلية ("CPINSIDE") خلف نقطة التفتيش. يجب أن يتوافق هذا مع **النظير =** أمر **مركز** الشبكة الخاصة الظاهرية ((VPN

General NAT Name: Cpinside IP Address: 10.32.50.0 Get address Net Mask: 255.255.255.0 Color: Image: Color: Corrent: Color: Image: Color: Image: Color: Location: Broadcast: Image: DK Disallowed	Network Properties	×
Name: Cpinside IP Address: 10.32.50.0 Get address Net Mask: 255.255.255.0 Comment: Color: Location: Broadcast: Image: Internal Image: External Image: Allowed Image: Ima	General NAT	
IP Address: 10.32.50.0 Get address Net Mask: 255.255.255.0 Color: ▼ Location: Color: ▼ Location: Broadcast: ● Allowed ● Disallowed OK Cancel Help Help External Help	Name: cpinside	
Net Mask: 255.255.255.0 Comment: Color: Location: Broadcast: Internal External Image: Allowed Disallowed	IP Address: 10.32.50.0 Get address	
Color: Image: Color: Location: Broadcast: ● Internal ● External ● Allowed ● Disallowed OK Cancel Help	Net <u>M</u> ask: 255.255.255.0	
Location: Broadcast: Internal External Allowed Disallowed OK Cancel Help	Color: Color:	
OK Cancel Help	Location: ● Internal ● External ● Allowed ● Disallowed	
	OK Cancel Help	

3. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير الكائن لنقطة نهاية العبارة ("نقطة تفتيش RTPCPVPN") التي يشير إليها مركز VPN في الأمر partner = <ip>.حدد **داخلي** أسفل الموقع.حدد **عبارة** للنوع.تحقق من VPN-1 ومحطة الإدارة ضمن الوحدات

Workstation Properties	×
General Interfaces SNMP 1	NAT Certificates VPN Authe
	· [
Name: RTPCPVPN	
172 10 124 157	Cot address
IP Address: [172.10.124.137	
Comment: Firewalled gatev	way to internet
Location:	Type:
	<u>○ H</u> ost ⊙ Gate <u>w</u> ay
Modules Installed	
VPN-1 & EireWall-1	Version: 4.1 💌 Get
FloodGate-1	Version: 4.1
Compression	Version: 4.1
Management Station	Color:
ОК	Cancel Help
	يبة.

عبيبية. 4. حدد **إدارة > كائنات الشبكة > جديد (أو تحرير) > الشبكة** لتكوين الكائن للشبكة الخارجية ("inside_cisco") خلف مركز VPN.يجب أن يتوافق هذا مع LocalAccess = <192.168.1.0/24>أمر مركز

Network Properties	×
General NAT	
<u>N</u> ame: <mark>inside_cisco</mark>	
IP Address: 192.168.1.0	<u>G</u> et address
Net <u>M</u> ask: 255.255.255.0	
<u>C</u> omment:	Color:
Location: ○ Internal	adcast: <u>Allowed O D</u> isallowed
OK Cance	

5. حدد **إدارة > كائنات الشبكة > جديد > محطة عمل** لإضافة كائن لبوابة مركز VPN الخارجية ("Cisco_Endpoint").هذا هو الواجهة "الخارجية" من مركز VPN مع الاتصال بنقطة التفتيش (في هذا المستند، يمثل 172.18.124.35 عنوان IP في **الأمر** iP = IPAddress=).حدد **خارجي** أسفل الموقع. حدد **عبارة** للنوع.**ملاحظة:** عدم التحقق من -VPN-1/FireWall

Workstation Properties			
General Interfaces SNMP NAT VPN			
Nama: loisco endocint			
IP Address: 172.18.124.35			
Comment:			
Location:Type:			
<u>○ I</u> nternal <u>○ E</u> xternal <u>○ H</u> ost <u>○</u> Gate <u>w</u> ay			
Modules Installed			
□ VPN-1 & <u>F</u> ireWall-1 Version: 4.1 <u>Get</u>			
FloodGate-1 Version: 4.1			
Compression Version: 4.1			
Management Station Color: ▼			
OK Cancel Help			

6. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير نقطة نهاية عبارة نقطة النهاية (تسمى "RTPCPVPN") لعلامة التبويب VPN. تحت المجال، حدد **آخر** ثم حدد داخل شبكة نقطة التفتيش (والتي تسمى "cpinside") من القائمة المنسدلة. تحت تشفير نظام يعين، حدد IK**E**، ثم انقر

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
Domain: Disabled Valid Addresses(of Interfaces) Image: Differior
OK Cancel Help

7. قم بتغيير خصائص IKE إلى تشفير DES وتجزئة SHA1 للاتفاق مع أمر مركز SHA_DES_G2 VPN.**ملاحظة:** تشير "G2" إلى مجموعة Diffie-Hellman رقم 1 أو 2. وفي الاختبار، اكتشف أن نقطة التفتيش تقبل إما "G2" أو "G1".تغيير هذه الإعدادات:عدم تحديد **الوضع المتداخل**.تحقق من **دعم الشبكات الفرعية**.تحقق من **سر مشترك مسبقا** تحت أسلوب

General Interfaces SNMP NAT Certifi	cates VPN Authe
KE Properties	×
General	
Key <u>N</u> egotiation Encryption Method(s): <u>H</u> ash Method:
DES DES	□ MD <u>5</u>
CAST	SHA1
Authentication Method:	
Pre-Shared Secret	Edit <u>S</u> ecrets
Public Key Signatures	Configure
Supports Aggresive Mode 🔽 S	upports Su <u>b</u> nets
OK Cancel	Help
	مصادقة

8. انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا للاتفاق مع SharedKey = <key>أمر مركز

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret
Shared Secrets List:
Peer Name Shared Secret
<u>Edit</u>
Remove
OK Cancel
OK Cancel Help
OK Cancel Help

9. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير علامة التبويب VPN "cisco_endpoint". تحت المجال، حدد **آخر**، ثم حدد داخل شبكة مركز VPN (تسمى "inside_cisco"). تحت تشفير نظام يعين، حدد IK**E**، ثم انقر

Workstation Properties	×
General Interfaces SNMP NAT	VPN
Domain:	Encryption schemes defined:
O <u>D</u> isabled	Manual IPSEC
 Valid Addresses(of Interfaces) Other: 	
🖳 inside_cisco 🔽	
Egportable for SecuRemote	<u>E</u> dit
Traffic Control Logging	
Ium on Traffic Control Loggin	g
·	
OK Can	icel Help
	حرير.

10. قَم^{َّ} بَتغيير خصائص IKE إلى تشفير **DES** وتجزئة **SHA1** للاتفاق مع أمر مركز SHA_DES_G2 VPN.**ملاحظة:** تشير "G2" إلى مجموعة Diffie-Hellman رقم 1 أو 2. وعند الاختبار، تبين أن نقطة التفتيش. تقبل إما "G2" أو "G1".تغيير هذه الإعدادات:عدم تحديد **الوضع المتداخل**.تحقق من **دعم الشبكات الفرعية**.تحقق من **سر مشترك مسبقا** تحت أسلوب

General Interfaces SNMP NAT Certificates VPN Authe
KE Properties 🔀
General
Key Negotiation Encryption Method(s): Hash Method: DES MD5 CAST SHA1
Authentication Method:
☐ Supports Aggresive <u>M</u> ode
OK Cancel Help
المصادقة. 4 ابت فريت برج الأربابات بالرناية الشراب بتايالاتناية برماي جريمكالمعماكماً مكر
ا . الفر فوق تحرير الاسرار للغيين المفتاح المسترك مسبقا للاتفاق مع Key – Key امر مردر IKE Properties
General
Shared Secret
Shared Secrets List: Peer Name Shared Secret BTPCPVPN **** Edit <u>R</u> emove
OK Cancel
OK Cancel Help

12. في نافذة "محرر النهج"، قم بإدراج قاعدة بكل من "المصدر والوجهة" و"inside_cisco" و"cpinside" (ثنائي الإتجاه). set **service=any، action=encrypt**، وtrack=long.

٣	RTPC	PVPN - Check Po	oint Policy Editor				- 🗆 🗵
Ei	e <u>E</u> dil	t ⊻iew <u>M</u> anage	<u>Policy W</u> indow <u>H</u>	elp			
6] 🖨	🖪 🖉 🕹 🖻	🖻 🚇 😽 🧖	B. 🕫 🌇	🖆 🖳 🖀 🐣	" 🖦 🖳 🔫 🕪	🖶 🗟 🖫 🚯
ä	3 Secu	urity Policy - Standard	📩 Address Trans	slation - Standard	l 🛛 🕡 Bandwidth Po	licy - Standard	
	No.	Source	Destination	Servic	e Actio	n Tracl	k In
Ì	1	🚆 inside_cisco	nside_cisco	Any	Encry	pt Long	G
l							
Fo	r Help, j	press F1			RTPCPVPN	Read/Write	

13. تحت عنوان الإجراء، انقر على أيقونة **التشفير** الأخضر وحدد **تحرير الخصائص** لتكوين سياسات



15. في نافذة خصائص IKE، قم بتغيير هذه الخصائص لتوافق مع أمر مركز **التحويل = (esp(sha،des**

VPN.تحت التحويل، حدد **التشفير + تكامل البيانات (ESP)**. يجب أن تكون خوارزمية التشفير **DES**، ويجب أن تكون تكامل البيانات SHA1، ويجب أن تكون بوابة النظير المسموح بها عبارة مركز VPN الخارجية (تسمى "Cisco_Endpoint"). وانقر فوق

IKE Properties	
General	
Tanatan	
Encryption + Data Integrity (ESP)	
C Data Integrity Only (AH)	
Encryption Algorithm: DES	
Data Integrity SHA1	
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
OK Cancel Help	ЭК

16. بعد تكوين نقطة التحقق، حدد **نهج > تثبيت** في قائمة نقطة التفتيش لتفعيل التغييرات.

<u>التحقق من الصحة</u>

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

<u>استكشاف الأخطاء وإصلاحها</u>

أوامر أستكشاف أخطاء مركز VPN 5000 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.

- VPN Trace Dump all —يعرض معلومات حول جميع إتصالات VPN المطابقة، بما في ذلك معلومات حول الوقت، ورقم VPN، وعنوان IP الحقيقي للنظير، والذي تم تشغيل البرامج النصية، وفي حالة حدوث خطأ، الروتين ورقم سطر رمز البرنامج حيث حدث الخطأ.
 - show system log buffer— يعرض محتويات المخزن المؤقت للسجل الداخلي.
- show vpn statistics يعرض هذه المعلومات للمستخدمين والشركاء والإجمالي لكل من. (للطرز النمطية، يتضمن العرض قسما لكل فتحة وحدة نمطية. ارجع إلى قسم <u>إخراج تصحيح الأخطاء للعينة.</u>) الاتصالات
 النشطة الحالية. الاتصالات التفاوضية الحالية. —أعلى عدد من الاتصالات النشطة المتزامنة منذ آخر إعادة
 تشغيل. —إجمالي عدد الاتصالات الناجحة منذ آخر إعادة تشغيل."xo عدد الانفاق التي لم تكن هنالك أخطاء وحدة المعلومات.
 - show vpn statistics verbose— يعرض إحصائيات تفاوض ISAKMP، وإحصاءات اتصال أكثر نشاطا.

<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 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 10.0.10 /24 لتضمينها في النفق، فقد يتم تلخيصها إلى 10.0.00 /23.

<u>تصحيح أخطاء جدار الحماية Checkpoint 4.1</u>

كان هذا تثبيت Microsoft Windows NT. نظرا لتعيين التعقب في نافذة محرر النهج (كما هو موضح في <u>الخطوة</u> <u>12</u>)، يجب أن تظهر حركة المرور المرفوضة باللون الأحمر في عارض السجل. يمكن الحصول على المزيد من تصحيح الأخطاء المطبعية من خلال:

> C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d eفي نافذة تانية:

C:\WINNT\FW1\4.1\fwstart قم بإصدار هذه الأوامر لمسح اقترانات الأمان (SAs) على نقطة التفتيش:

> fw tab -t IKE_SA_table -x fw tab -t ISAKMP_ESP_table -x fw tab -t inbound_SPI -x fw tab -t ISAKMP_AH_table -x أجب بنعم في ؟

إخراج تصحيح الأخطاء للعينة

```
cisco_endpoint#vpn trac dump all
                                       -- seconds -- stepmngr trace enabled 4
                          (new script: lan-lan primary initiator for <no id> (start
                        (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                                          (seconds doing l2lp_init, (0 @ 0 38
                                (seconds doing l2lp_do_negotiation, (0 @ 0 38
      (new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start
                                    (seconds doing isa_i_main_init, (0 @ 0 38
                         (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done
                        (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                           (seconds doing isa_i_main_process_pkt_2, (0 @ 0 38
                         (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done
                        (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                           (seconds doing isa_i_main_process_pkt_4, (0 @ 0 38
                         (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done
                        (manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                           (seconds doing isa_i_main_process_pkt_6, (0 @ 0 39
                                 (seconds doing isa_i_main_last_op, (0 @ 0 39
    (end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0
(next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0
                                  (seconds doing l2lp_phase_1_done, (0 @ 0 39
                                 (seconds doing l2lp_start_phase_2, (0 @ 0 39
          (new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start
                                          (seconds doing iph2_init, (0 @ 0 39
                                   (seconds doing iph2_build_pkt_1, (0 @ 0 39
```

(seconds doing iph2_send_pkt_1, (0 @ 0 39 (manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done (manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start (seconds doing iph2_pkt_2_wait, (0 @ 0 39 (seconds doing ihp2_process_pkt_2, (0 @ 0 39 (seconds doing iph2_build_pkt_3, (0 @ 0 39 (seconds doing iph2_config_SAs, (0 @ 0 39 (seconds doing iph2_send_pkt_3, (0 @ 0 39 (seconds doing iph2_last_op, (0 @ 0 39 (end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0 (next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0 (seconds doing l2lp_open_tunnel, (0 @ 0 39 (seconds doing l2lp_start_i_maint, (0 @ 0 39 (new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start (seconds doing imnt_init, (0 @ 0 39 (manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done

cisco_endpoint#show vpn stat

Current Active	In Negot	t	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error	
Use	ers	0	0	0	0	0	0	0
Par	tners	1	0	1	1	1	0	0
Tot	al	1	0	1	1	1	0	0

:IOP slot 1

Curr	ent :	In		High	Running	Tunnel	Tunnel	Tunnel	
Act	ive	Negot	t	Water	Total	Starts	OK	Error	
	User	5	0	0	0	0	0	0	0
	Parti	ners	0	0	0	0	0	0	0
	Tota	1	0	0	0	0	0	0	0

cisco_endpoint#show vpn stat verb

Cur	rent	In		High	Running	Tunnel	Tunnel	Tunnel	
Ac	tive	Nego	t	Water	Total	Starts	OK	Error	
			·						
	User	s	0	0	0	0	0	0	0
	Part	ners	1	0	1	1	1	0	0
	Tota	ıl	1	0	1	1	1	0	0

Stats	VPN0:1
Wrapped	13
Unwrapped	9
BadEncap	0
BadAuth	0
BadEncrypt	0
rx IP	9
rx IPX	0
rx Other	0
tx IP	13
tx IPX	0
tx Other	0
IKE rekey	0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

Admin packets in 4 Fastswitch packets in 0 No cookie found 0 Can't insert cookie 0 Inserted cookie(L) 1 Inserted cookie(R) 0 Cookie not inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted cookie(L) 0 Deleted cookie(R) 0 Cookie not deleted(L) 0 Cookie not deleted(R) 0 Forwarded to RP 0 Forwarded to IOP 0 Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 Bad Responder cookie 0 Has Responder cookie 0 No Responder cookie 0 No SA 0 Bad find conn 0 Admin queue full 0 Priority queue full 0 Bad IKE packet 0 No memory 0 Bad Admin Put 0 IKE pkt dropped 0 No UDP PBuf 0 No Manager 0 Mgr w/ no cookie 0 Cookie Scavenge Add 1 Cookie Scavenge Rem 0 Cookie Scavenged 0 Cookie has mgr err 0 New conn limited 0

:IOP slot 1

Current	In		High	Running	Tunnel	Tunnel	Tunnel	
Active	Nego	t.	Water	Total	Starts	ОК	Error	
Use	rs	0	0	0	0	0	0	0
Par	tners	0	0	0	0	0	0	0
Tot	al	0	0	0	0	0	0	0
								Stats
								Wrapped
							τ	Jnwrapped
								BadEncap
								BadAuth
							Ba	adEncrypt
								rx IP
								rx IPX
								rx Other
								tx IP
								tx IPX
								tx Other
							:	IKE rekey

ISAKMP Negotiation stats Admin packets in 0 Fastswitch packets in 3 No cookie found 0 Can't insert cookie 0 Inserted cookie(L) 0 Inserted cookie(R) 1 Cookie not inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted cookie(L) 0 Deleted cookie(R) 0 Cookie not deleted(L) 0 Cookie not deleted(R) 0 Forwarded to RP 0 Forwarded to IOP 3 Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 Bad Responder cookie 0 Has Responder cookie 0 No Responder cookie 0 No SA 0 Bad find conn 0 Admin queue full 0 Priority queue full 0 Bad IKE packet 0 No memory 0 Bad Admin Put 0 IKE pkt dropped 0 No UDP PBuf 0 No Manager 0 Mgr w/ no cookie 0 Cookie Scavenge Add 1 Cookie Scavenge Rem 0 Cookie Scavenged Ο Cookie has mgr err 0 New conn limited 0

<u>معلومات ذات صلة</u>

- إعلان نهاية المبيعات لسلسلة <u>Cisco VPN 5000</u>
 - مفاوضة IPSec/بروتوكولات IKE
 - <u>الدعم التقني والمستندات 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