

NG شيرتفت ة طقون نيب IPsec ق فن نيوكت هجوم ل او

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [الاصطلاحات](#)
- [تكوين الموجه VPN 1751 من Cisco](#)
- [تكوين NG لنقطة التحقق](#)
- [التحقق من الصحة](#)
- [التحقق من موجه Cisco](#)
- [التحقق من NG لنقطة التحقق](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [موجه Cisco](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للانضمام إلى شبكتين خاصتين:

- الشبكة الخاصة x.172.16.15 داخل الموجه.
- الشبكة الخاصة x.192.168.10 داخل CheckpointTM من الجيل التالي (NG).

المتطلبات الأساسية

المتطلبات

وتستند الإجراءات الميينة في هذه الوثيقة إلى هذه الافتراضات.

- تم إعداد نهج NG CheckpointTM الأساسي.
- شكلت كل منفذ، شبكة عنوان ترجمة (NAT)، وتحشد أداة.
- حركة المرور من داخل الموجه وداخل NG CheckpointTM إلى تدفقات الإنترنت.

المكونات المستخدمة

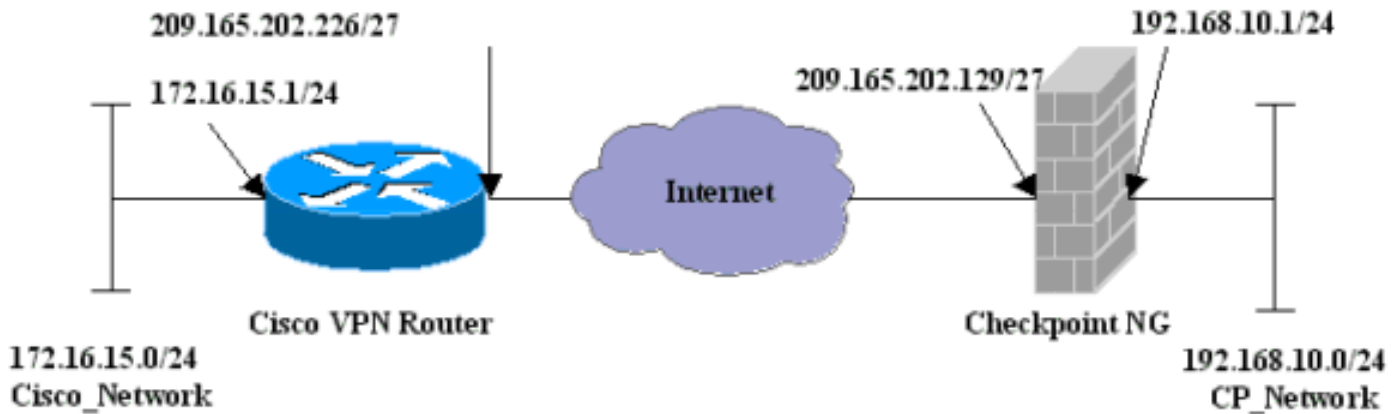
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- موجّه Cisco 1751
- برنامج (IOS® (C1700-K9O3SY7-M من Cisco، الإصدار T4(8)12.2، برنامج الإصدار (FC1)
- Checkpoint™ NG Build 50027

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميحات Cisco التقنية](#).

تكوين الموجه VPN 1751 من Cisco

```

Cisco 1751 VPN من
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname svl-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100
Internet Key Exchange (IKE) configuration. crypto ---!
isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
lifetime 1800
IPSec configuration. crypto isakmp key aptrules ---!
address 209.165.202.129

```

```

!
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
!
crypto map aptmap 1 ipsec-isakmp
set peer 209.165.202.129
set transform-set aptset
match address 110
!
interface Ethernet0/0
ip address 209.165.202.226 255.255.255.224
ip nat outside
half-duplex
crypto map aptmap
!
interface FastEthernet0/0
ip address 172.16.15.1 255.255.255.0
ip nat inside
speed auto
NAT configuration. ip nat inside source route-map ---!
nonat interface Ethernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.225
no ip http server
ip pim bidir-enable
Encryption match address access list. access-list ---!
110 permit ip 172.16.15.0 0.0.0.255 192.168.10.0
0.0.0.255
NAT access list. access-list 120 deny ip ---!
172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10
match ip address 120
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password cisco
login
end

```

تكوين NG لنقطة التحقق

يعد NG CheckpointTM تكويناً قائماً على الكائنات. يتم تحديد كائنات الشبكة وقواعدها لتكوين السياسة المتعلقة بتكوين VPN الذي سيتم إعداده. ويتم تثبيت هذا النهج بعد ذلك باستخدام محرر نهج CheckpointTM NG لإكمال جانب NG CheckpointTM من تكوين الشبكة الخاصة الظاهرية (VPN).

1. إنشاء شبكة Cisco الفرعية وشبكة NG CheckpointTM الفرعية ككائنات شبكة. هذا هو المشفر لإنشاء الكائنات، حدد إدارة < كائنات الشبكة، ثم حدد جديد < شبكة. أدخل معلومات الشبكة المناسبة، ثم انقر على موافق. تظهر هذه الأمثلة مجموعة من الكائنات تسمى CP_Network و

Network Properties - CP_Network

General NAT

Name: CP_Network

IP Address: 192.168.10.0

Net Mask: 255.255.255.0

Comment:

Color:

Broadcast address:

Included Not included

OK Cancel Help

.Cisco_Network

Network Properties - Cisco_Network

General NAT

Name: Cisco_Network

IP Address: 172.16.15.0

Net Mask: 255.255.255.0

Comment:

Color:

Broadcast address:

Included Not included

OK Cancel Help

2. قم بإنشاء كائنات Cisco_Router و Checkpoint_NG ككائنات محطة عمل. هذه هي أجهزة شبكة VPN. لإنشاء الكائنات، حدد إدارة < كائنات الشبكة، ثم حدد جديد < محطة عمل. لاحظ أنه يمكنك استخدام كائن محطة العمل NG CheckpointTM الذي تم إنشاؤه أثناء إعداد CheckpointTM الأولي. حدد الخيارات لتعيين محطة العمل كبوابة وجهاز VPN قابل للتشغيل البيئي. تظهر هذه الأمثلة مجموعة من الكائنات تسمى Chef و Cisco_Router.

General

- ... Topology
- ... NAT
- ... VPN
- ... Authentication
- ... Management
- + Advanced

General

Name:

IP Address:

Comment:

Color:

Type: Host Gateway

Check Point Products

Check Point products installed: Version

- VPN-1 & FireWall-1
- FloodGate-1
- Policy Server
- Primary Management Station

Object Management

- Managed by this Management Server (Internal)
- Managed by another Management Server (External)

Secure Internal Communication

DN:

Interoperable VPN Device

Workstation Properties - Cisco_Router

General

Name: Cisco_Router

IP Address: 209.165.202.226

Comment: Cisco_VPN_Router

Color:

Type: Host Gateway

Check Point Products

Check Point products installed: Version NG

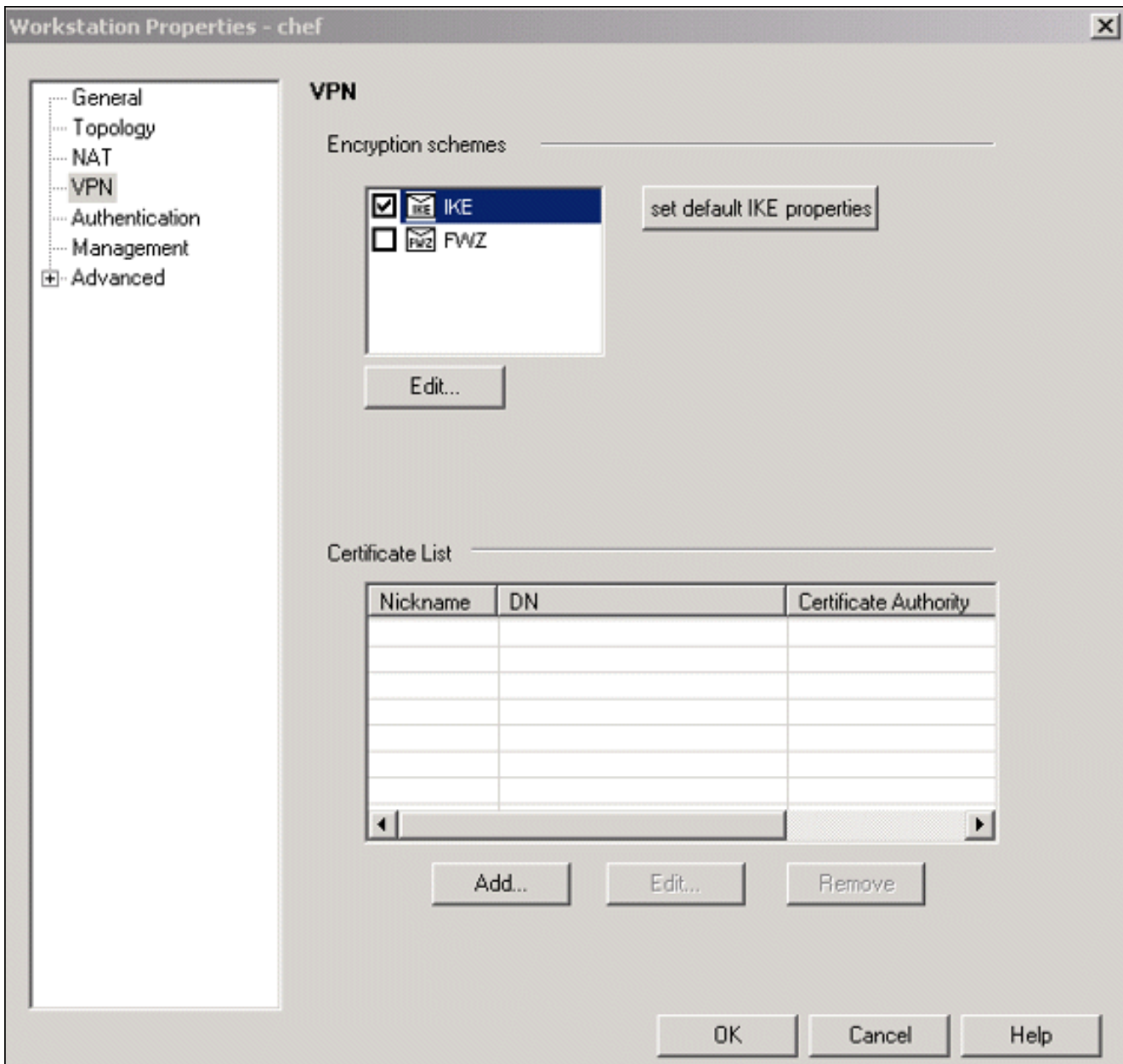
VPN-1 & FireWall-1
 FloodGate-1
 Policy Server
 Secondary Management Station

Object Management

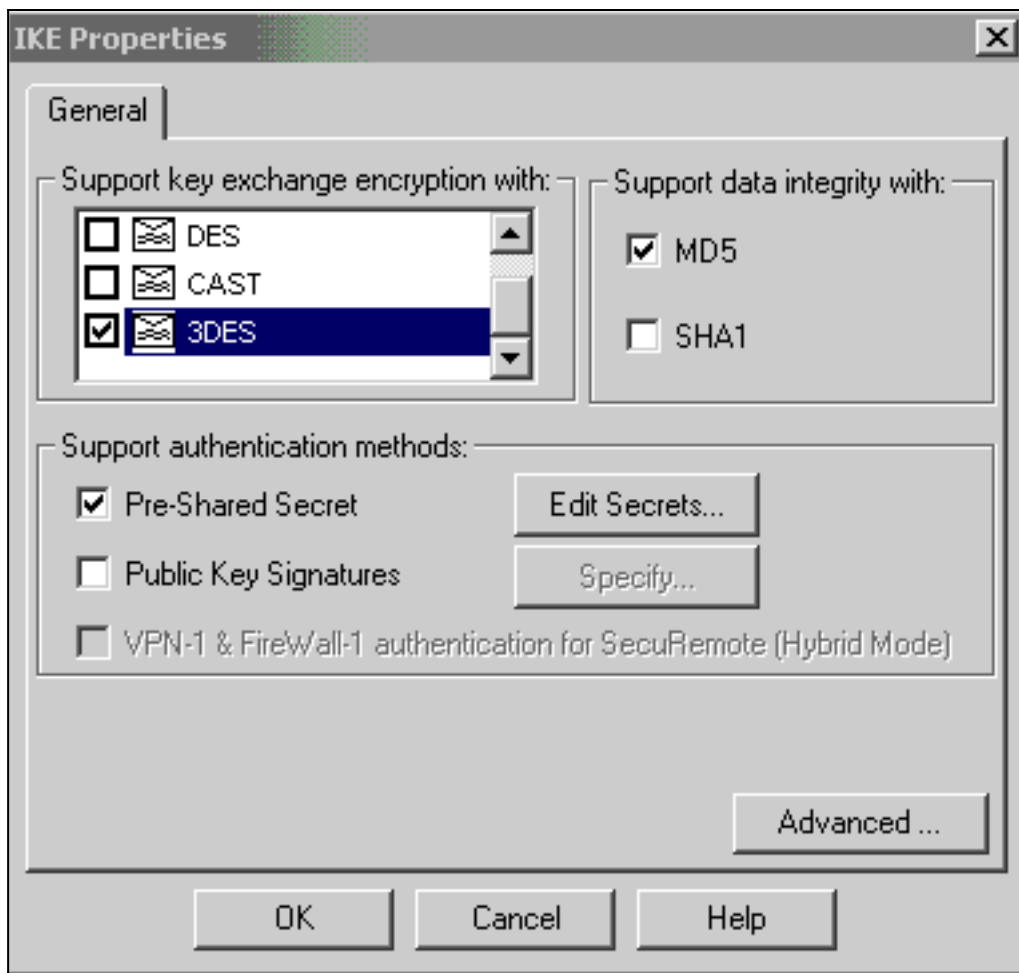
Managed by this Management Server (Internal)
 Managed by another Management Server (External)

Interoperable VPN Device

3. قم بتكوين IKE على علامة التويب VPN، ثم انقر فوق تحرير.

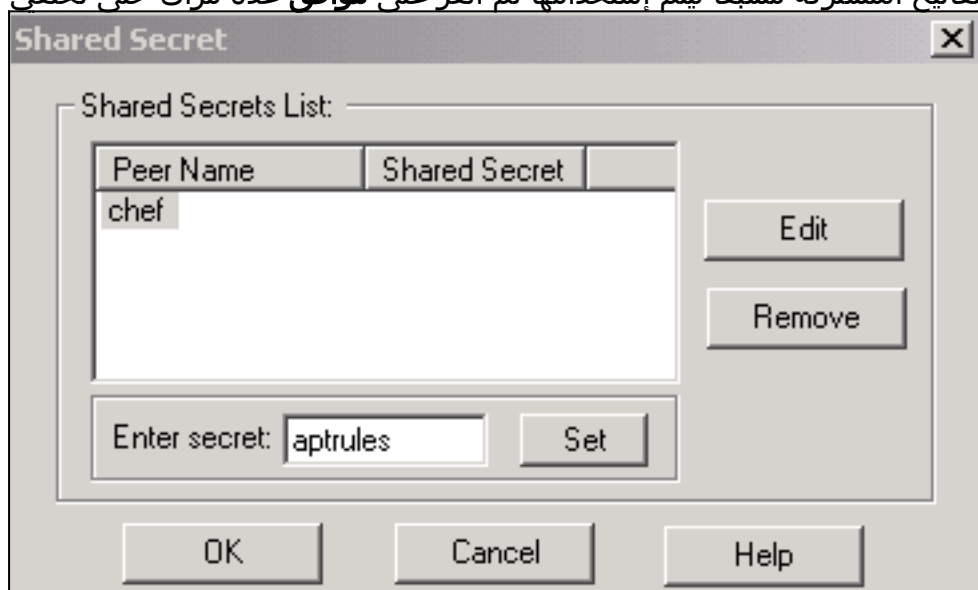


4. قم بتكوين نهج تبادل المفاتيح، وانقر فوق تحرير



الأسرار

5. اضبط المفاتيح المشتركة مسبقاً ليتم استخدامها ثم انقر على موافق عدة مرات حتى تختفي إطارات



التكوين.

6. حدد قواعد < إضافة قواعد > أعلى لتكوين قواعد التشفير للنهج. القاعدة في الأعلى هي القاعدة الأولى التي يتم تنفيذها قبل أي قاعدة أخرى قد تتجاوز التشفير. قم بتكوين المصدر والوجهة لتضمين CP_Network و Cisco_Network، كما هو موضح هنا. بمجرد أن تقوم بإضافة قسم إجراء التشفير من القاعدة، انقر بزر الماوس الأيمن فوق الإجراء وحدد تحرير الخصائص.

Security - APTPolicy | Address Translation - APTPolicy | Desktop Security - Standard

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON
1	CP_Network Cisco_Network	CP_Network Cisco_Network	* Any	Encrypt	Log	Gateways
2	* Any	* Any	* Any	drop		Gateways

- accept
- drop
- reject
- User Auth
- Client Auth
- Session Auth
- Encrypt
- Client Encrypt

Name	IP	Comment
chef	209.165.202.129	CP_Server
Cisco_Router	209.165.202.226	Cisco_VPN_Router

7. مع تحديد IKE وإبرازه، انقر

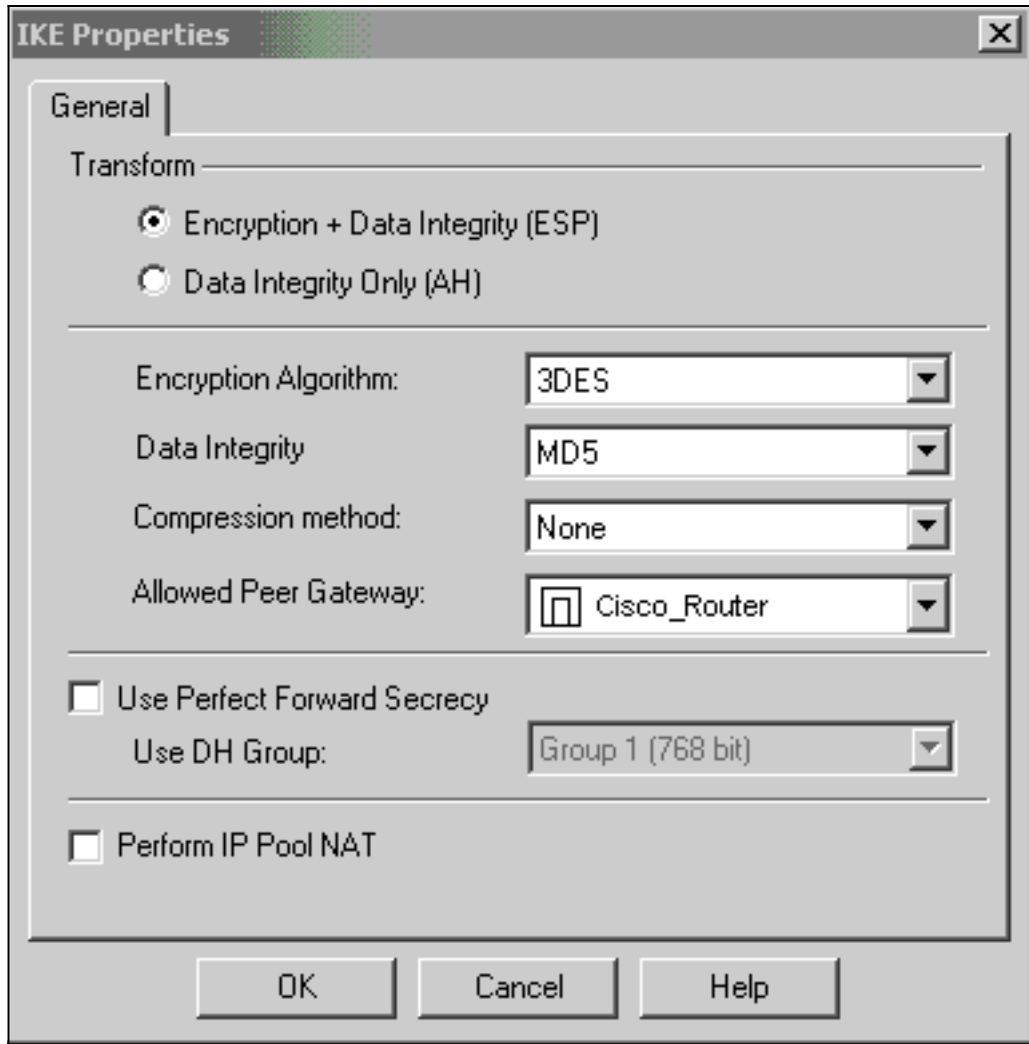
Encryption Properties

General

Encryption schemes defined:

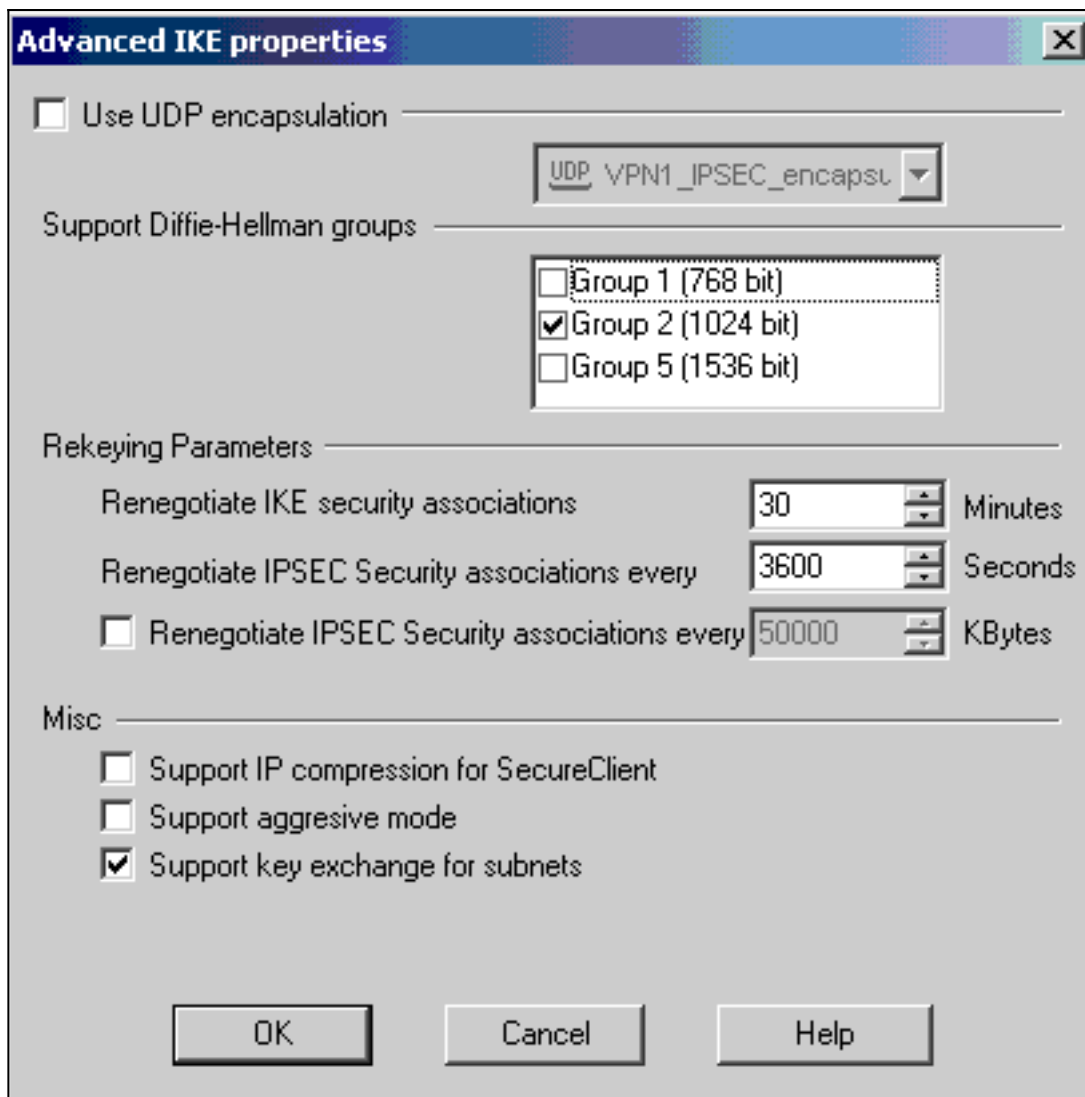
- IKE
- FWZ

تحرير.



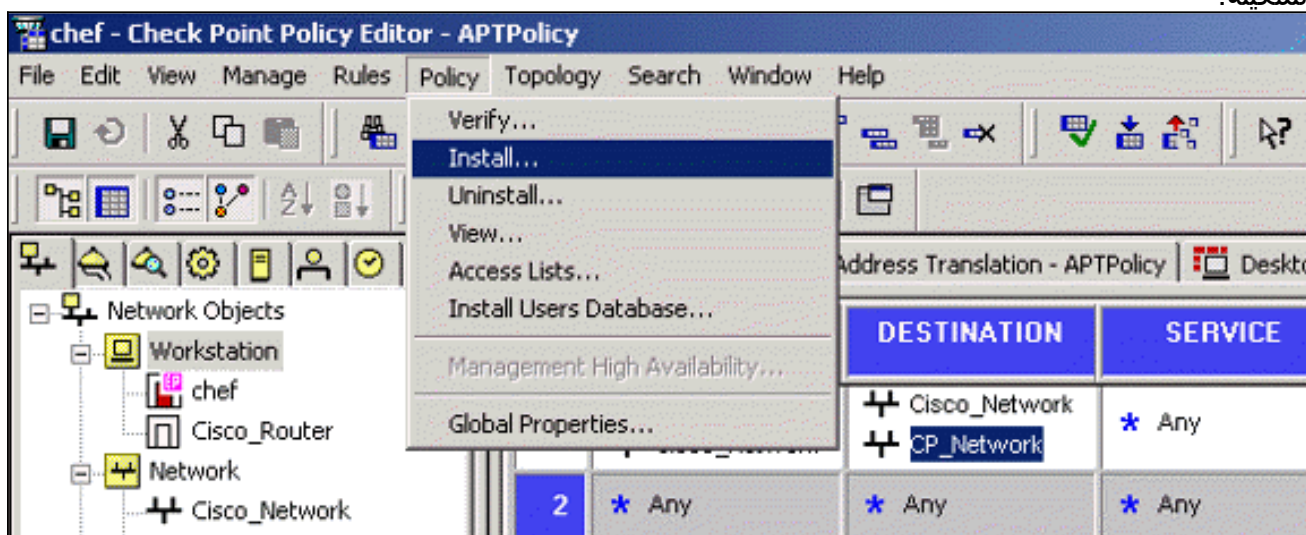
8. تأكيد تكوين IKE.

9. أحد المشاكل الأساسية مع تشغيل VPN بين أجهزة Cisco وأجهزة IPsec الأخرى هو إعادة التفاوض لتبادل المفاتيح. تأكد من أن إعداد تبادل IKE على موجه Cisco هو نفسه تماما الذي تم تكوينه على CheckpointTM NG. ملاحظة: تعتمد القيمة الفعلية لهذا المعامل على سياسة أمان الشركة الخاصة بك. في هذا المثال، تم تعيين تكوين IKE على الموجه إلى 30 دقيقة باستخدام الأمر life 1800. يجب تعيين نفس القيمة على CheckpointTM NG. لتعيين هذه القيمة على NG CheckpointTM، حدد إدارة كائن الشبكة، ثم حدد كائن NG CheckpointTM وانقر فوق Edit. ثم حدد VPN، وقم بتحرير IKE. حدد مقدمة وقم بتكوين معلمات إعادة التشكيل. بعد تكوين تبادل المفاتيح لكائن الشبكة NG CheckpointTM، قم بإجراء نفس تكوين إعادة التفاوض لتبادل المفاتيح لكائن شبكة Cisco_Router. ملاحظة: تأكد من تحديد مجموعة Diffie-Hellman الصحيحة لمطابقة المجموعة التي تم تكوينها على

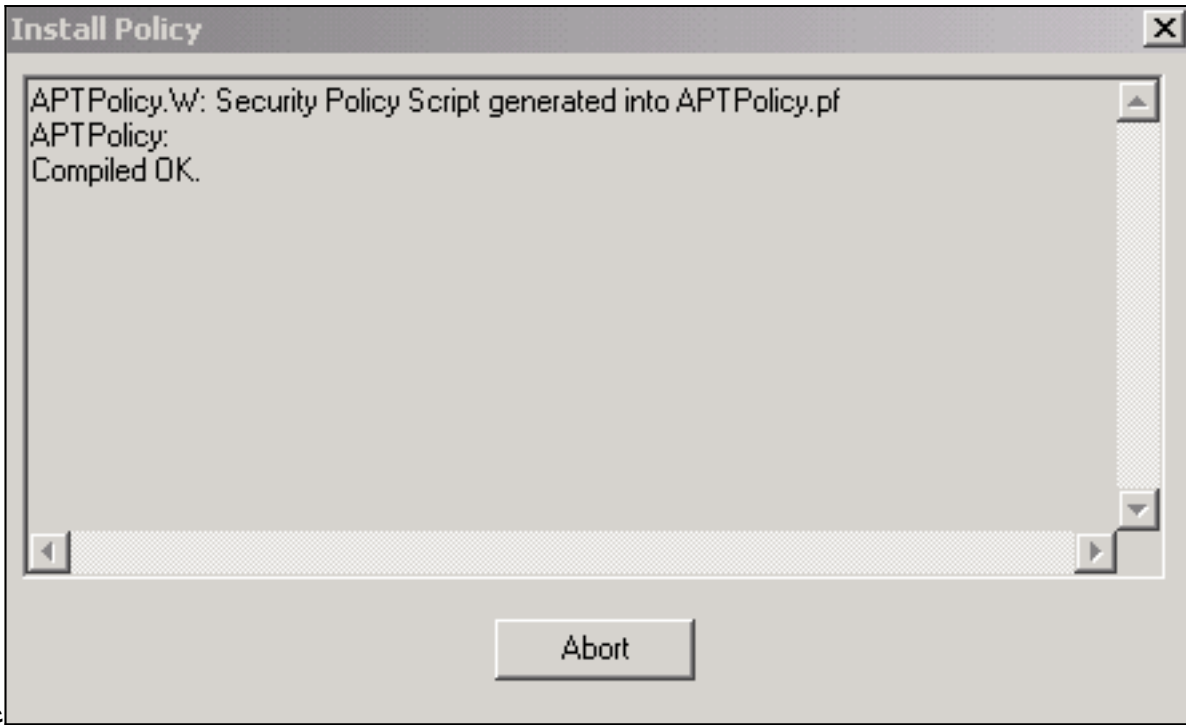


الموجه.

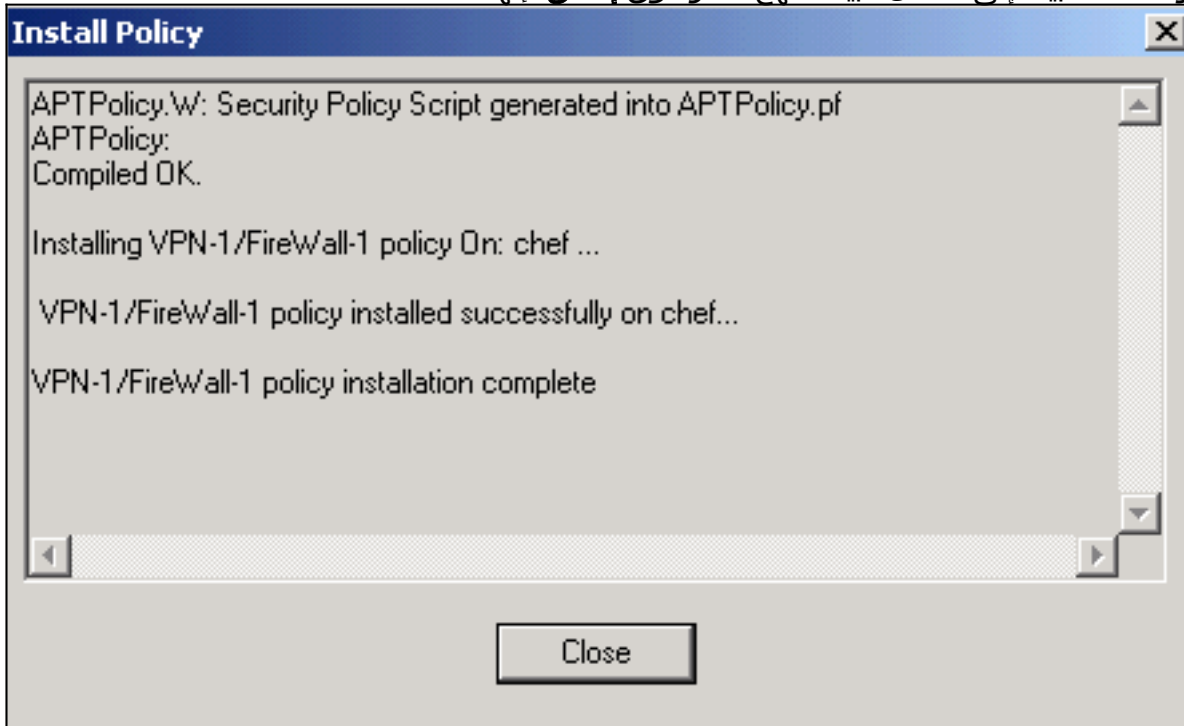
10. تم إكمال تكوين النهج. قم بحفظ النهج وحدد نهج < تثبيت
 لتمكينه.



تعرض نافذة التثبيت ملاحظات التقدم أثناء تحويل النهج



برمجيا. عندما تظهر نافذة التثبيت إلى اكمال تثبيت النهج، انقر فوق إغلاق لإنهاء



الإجراء.

[التحقق من الصحة](#)

يوفر هذا القسم معلومات يمكنك استخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

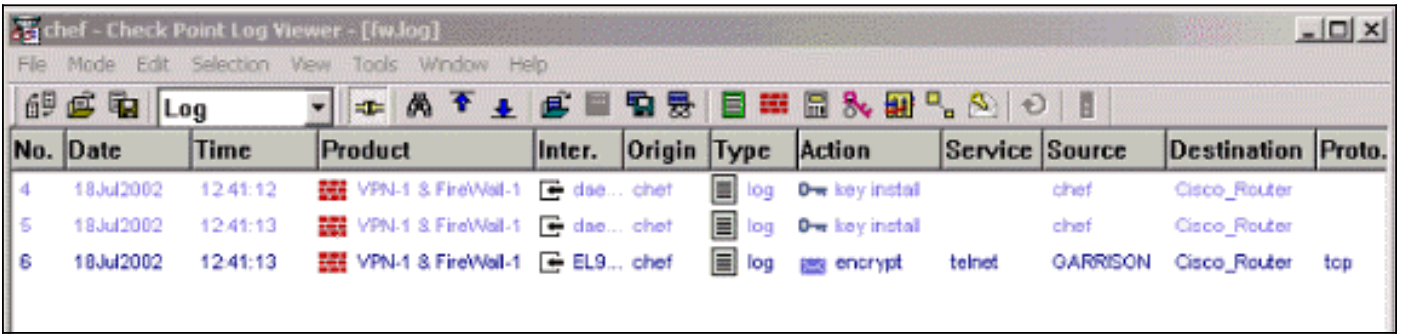
[التحقق من موجه Cisco](#)

يتم دعم بعض أوامر العرض بواسطة أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر العرض.

- `show crypto isakmp sa` — يعرض جميع اقترانات أمان (SAs) (IKE) الحالية في نظير.
- `show crypto ipSec` — يعرض الإعدادات المستخدمة من قبل SAs الحالية.

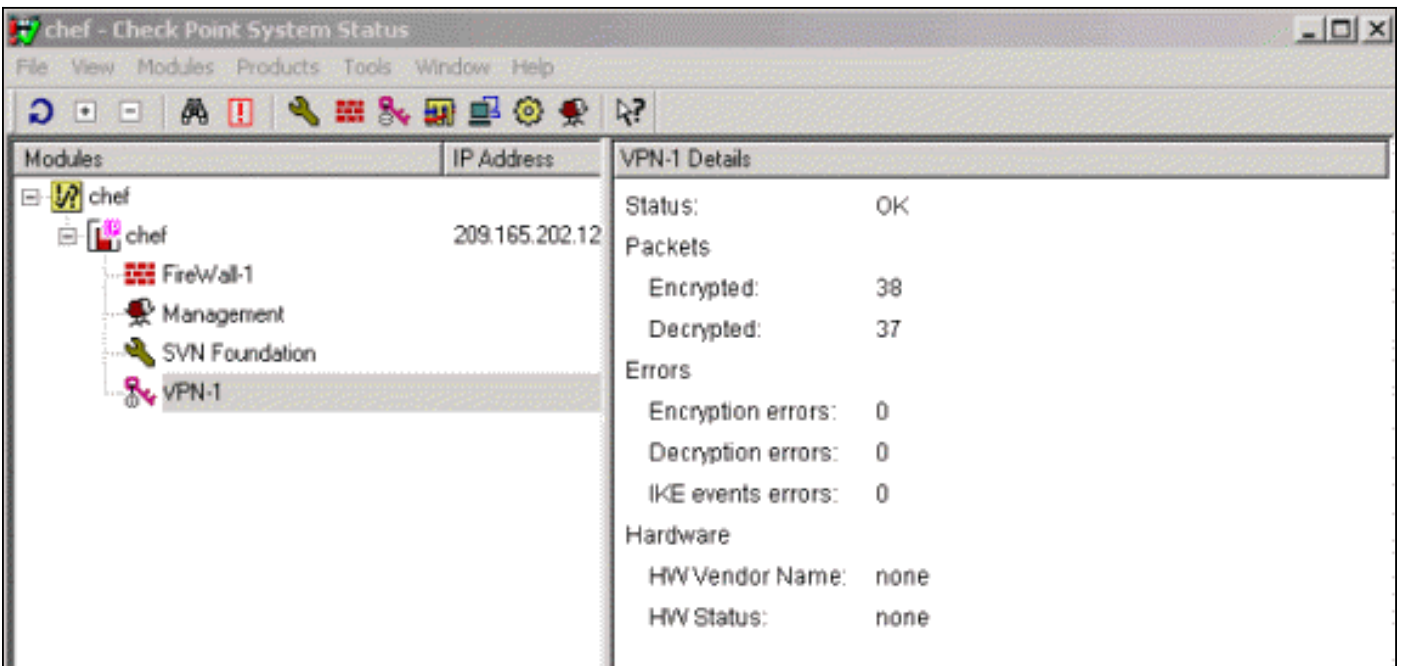
التحقق من NG لنقطة التحقق

لعرض السجلات، حدد نافذة < عارض السجل.



No.	Date	Time	Product	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.
4	18Jul2002	12:41:12	VPN-1 & FireWall-1	dae...	chef	log	key instal		chef	Cisco_Router	
5	18Jul2002	12:41:13	VPN-1 & FireWall-1	dae...	chef	log	key instal		chef	Cisco_Router	
6	18Jul2002	12:41:13	VPN-1 & FireWall-1	EL9...	chef	log	encrypt	telnet	GARRISON	Cisco_Router	top

لعرض حالة النظام، حدد نافذة < حالة النظام.



Modules	IP Address	VPN-1 Details
chef		Status: OK
chef	209.165.202.12	Packets
FireWall-1		Encrypted: 38
Management		Decrypted: 37
SVN Foundation		Errors
VPN-1		Encryption errors: 0
		Decryption errors: 0
		IKE events errors: 0
		Hardware
		HW Vendor Name: none
		HW Status: none

استكشاف الأخطاء وإصلاحها

Cisco

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

للحصول على معلومات إضافية حول استكشاف الأخطاء وإصلاحها، يرجى الرجوع إلى [استكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها](#).

ملاحظة: قبل إصدار أوامر تصحيح الأخطاء، راجع [المعلومات المهمة في أوامر تصحيح الأخطاء](#).

- debug crypto engine—يعرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تقوم بالتشفير وفك التشفير.
- debug crypto isakmp—يعرض الرسائل المتعلقة بأحداث IKE.
- debug crypto ipSec—يعرض أحداث IPsec.
- مسح التشفير isakmp—مسح جميع اتصالات IKE النشطة.
- مسح التشفير sa—يمحو جميع شبكات IPsec SAs.

إخراج سجل تصحيح الأخطاء الناجح

```
ISAKMP (0:0): received packet from :18:05:32
                N) NEW SA) 209.165.202.129
ISAKMP: local port 500, remote port 500 :18:05:32
,ISAKMP (0:1): Input = IKE_MSG_FROM_PEER :18:05:32
                IKE_MM_EXCH
                Old State = IKE_READY New State = IKE_R_MM1
ISAKMP (0:1): processing SA payload. message ID = 0 :18:05:32
ISAKMP (0:1): processing vendor id payload :18:05:32
                ISAKMP (0:1): vendor ID seems Unity/DPD :18:05:32
                        but bad major
ISAKMP (0:1): found peer pre-shared key :18:05:32
                matching 209.165.202.129
ISAKMP (0:1): Checking ISAKMP transform 1 :18:05:32
                against priority 1 policy
                ISAKMP: encryption 3DES-CBC :18:05:32
                        ISAKMP: hash MD5 :18:05:32
                                ISAKMP: auth pre-share :18:05:32
                                        ISAKMP: default group 2 :18:05:32
                                                ISAKMP: life type in seconds :18:05:32
                ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8 :18:05:32
ISAKMP (0:1): atts are acceptable. Next payload is 0 :18:05:32
                ISAKMP (0:1): processing vendor id payload :18:05:33
ISAKMP (0:1): vendor ID seems Unity/DPD but bad major :18:05:33
                ,ISAKMP (0:1): Input = IKE_MSG_INTERNAL :18:05:33
                        IKE_PROCESS_MAIN_MODE
                        Old State = IKE_R_MM1 New State = IKE_R_MM1
                (ISAKMP (0:1): sending packet to 209.165.202.129 (R :18:05:33
                        MM_SA_SETUP
                ,ISAKMP (0:1): Input = IKE_MSG_INTERNAL :18:05:33
                        IKE_PROCESS_COMPLETE
                        Old State = IKE_R_MM1 New State = IKE_R_MM2
                (ISAKMP (0:1): received packet from 209.165.202.129 (R :18:05:33
                        MM_SA_SETUP
                ,ISAKMP (0:1): Input = IKE_MSG_FROM_PEER :18:05:33
                        IKE_MM_EXCH
                        Old State = IKE_R_MM2 New State = IKE_R_MM3
                .ISAKMP (0:1): processing KE payload :18:05:33
                        message ID = 0
                .ISAKMP (0:1): processing NONCE payload :18:05:33
                        message ID = 0
                ISAKMP (0:1): found peer pre-shared key :18:05:33
                        matching 209.165.202.129
                ISAKMP (0:1): SKEYID state generated :18:05:33
                ,ISAKMP (0:1): Input = IKE_MSG_INTERNAL :18:05:33
                        IKE_PROCESS_MAIN_MODE
                        Old State = IKE_R_MM3 New State = IKE_R_MM3
                (ISAKMP (0:1): sending packet to 209.165.202.129 (R :18:05:33
                        MM_KEY_EXCH
                ,ISAKMP (0:1): Input = IKE_MSG_INTERNAL :18:05:33
                        IKE_PROCESS_COMPLETE
                        Old State = IKE_R_MM3 New State = IKE_R_MM4
                (ISAKMP (0:1): received packet from 209.165.202.129 (R :18:05:33
                        MM_KEY_EXCH
                ,ISAKMP (0:1): Input = IKE_MSG_FROM_PEER :18:05:33
                        IKE_MM_EXCH
                        Old State = IKE_R_MM4 New State = IKE_R_MM5
                .ISAKMP (0:1): processing ID payload :18:05:33
                        message ID = 0
                .ISAKMP (0:1): processing HASH payload :18:05:33
                        message ID = 0
```

```
ISAKMP (0:1): SA has been authenticated :18:05:33
                with 209.165.202.129
,ISAKMP (0:1): Input = IKE_MSG_INTERNAL :18:05:33
                IKE_PROCESS_MAIN_MODE
                Old State = IKE_R_MM5 New State = IKE_R_MM5
ISAKMP (0:1): SA is doing pre-shared key authentication :18:05:33
                using id type ID_IPV4_ADDR
                ISAKMP (1): ID payload :18:05:33
                        next-payload : 8
                        type : 1
                        protocol : 17
                        port : 500
                        length : 8
                ISAKMP (1): Total payload length: 12 :18:05:33
ISAKMP (0:1): sending packet to 209.165.202.129 :18:05:33
                R) QM_IDLE)
,ISAKMP (0:1): Input = IKE_MSG_INTERNAL :18:05:33
                IKE_PROCESS_COMPLETE
                Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
,ISAKMP (0:1): Input = IKE_MSG_INTERNAL :18:05:33
                IKE_PHASE1_COMPLETE
                Old State = IKE_P1_COMPLETE
                New State = IKE_P1_COMPLETE
(ISAKMP (0:1): received packet from 209.165.202.129 (R :18:05:33
                QM_IDLE
                .ISAKMP (0:1): processing HASH payload :18:05:33
                        message ID = -1335371103
                .ISAKMP (0:1): processing SA payload :18:05:33
                        message ID = -1335371103
                ISAKMP (0:1): Checking IPsec proposal 1 :18:05:33
                        ISAKMP: transform 1, ESP_3DES :18:05:33
                        :ISAKMP: attributes in transform :18:05:33
                        ISAKMP: SA life type in seconds :18:05:33
                ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10 :18:05:33
                        ISAKMP: authenticator is HMAC-MD5 :18:05:33
                        ISAKMP: encaps is 1 :18:05:33
                .ISAKMP (0:1): atts are acceptable :18:05:33
                ,IPSEC(validate_proposal_request): proposal part #1 :18:05:33
                ,key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129)
                ,(local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4
                ,(remote_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 (0:1): processing NONCE payload :18:05:33
                        message ID = -1335371103
                .ISAKMP (0:1): processing ID payload :18:05:33
                        message ID = -1335371103
                .ISAKMP (0:1): processing ID payload :18:05:33
                        message ID = -1335371103
                ISAKMP (0:1): asking for 1 spis from ipsec :18:05:33
                ,ISAKMP (0:1): Node -1335371103 :18:05:33
                Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
                Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
                ...IPSEC(key_engine): got a queue event :18:05:33
                IPSEC(spi_response): getting spi 2147492563 for SA :18:05:33
                from 209.165.202.226 to 209.165.202.129 for prot 3
                (ISAKMP: received ke message (2/1 :18:05:33
                ISAKMP (0:1): sending packet to :18:05:33
                        R) QM_IDLE) 209.165.202.129
                ,ISAKMP (0:1): Node -1335371103 :18:05:33
                Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
                Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
                ISAKMP (0:1): received packet :18:05:33
```



```

from 209.165.202.129 (R) QM_IDLE
ISAKMP (0:1): Creating IPsec SAs :18:05:33
inbound SA from 209.165.202.129 to 209.165.202.226 :18:05:33
(proxy 192.168.10.0 to 172.16.15.0)
has spi 0x800022D3 and conn_id 200 and flags 4 :18:05:33
lifetime of 3600 seconds :18:05:33
outbound SA from 209.165.202.226 to 209.165.202.129 :18:05:33
(proxy 172.16.15.0 to 192.168.10.0)
has spi -2006413528 and conn_id 201 and flags C :18:05:33
lifetime of 3600 seconds :18:05:33
ISAKMP (0:1): deleting node -1335371103 error :18:05:33
"()FALSE reason "quick mode done (await
,ISAKMP (0:1): Node -1335371103, Input = IKE_MSG_FROM_PEER :18:05:33
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
...IPSEC(key_engine): got a queue event :18:05:33
, : (IPSEC(initialize_sas :18:05:33
,key eng. msg.) INBOUND local= 209.165.202.226)
,remote=209.165.202.129
,(local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-3des esp-md5-hmac
,lifedur= 3600s and 0kb
,spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0
flags= 0x4
, : (IPSEC(initialize_sas :18:05:33
,key eng. msg.) OUTBOUND local= 209.165.202.226)
,remote=209.165.202.129
,(local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-3des esp-md5-hmac
,lifedur= 3600s and 0kb

,spi= 0x88688F28(2288553768), conn_id= 201, keysize= 0
flags= 0xC
,IPSEC(create_sa): sa created :18:05:33
,(sa) sa_dest= 209.165.202.226, sa_prot= 50)
,(sa_spi= 0x800022D3(2147492563
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200
,IPSEC(create_sa): sa created :18:05:33
,(sa) sa_dest= 209.165.202.129, sa_prot= 50)
,(sa_spi= 0x88688F28(2288553768
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201
ISAKMP (0:1): received packet :18:05:34
from 209.165.202.129 (R) QM_IDLE
ISAKMP (0:1): phase 2 packet is a duplicate :18:05:34
.of a previous packet
ISAKMP (0:1): retransmitting due to retransmit phase 2 :18:05:34
ISAKMP (0:1): ignoring retransmission, because phase2 :18:05:34
node marked dead -1335371103
ISAKMP (0:1): received packet :18:05:34
from 209.165.202.129 (R) QM_IDLE
ISAKMP (0:1): phase 2 packet is a duplicate :18:05:34
.of a previous packet
ISAKMP (0:1): retransmitting due to retransmit phase 2 :18:05:34
ISAKMP (0:1): ignoring retransmission, because phase2 :18:05:34
node marked dead -1335371103

svl-6#show crypto isakmp sa
dst src state conn-id slot
QM_IDLE 1 0 209.165.202.129 209.165.202.226

```

```

svl-6#show crypto ipsec sa
interface: Ethernet0/0
Crypto map tag: aptmap, local addr. 209.165.202.226
(local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0
current_peer: 209.165.202.129
{,PERMIT, flags={origin_is_acl
pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21#
pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
send errors 0, #rcv errors 0#
local crypto endpt.: 209.165.202.226, remote crypto endpt.: 209.165.202.129
path mtu 1500, media mtu 1500
current outbound spi: 88688F28
:inbound esp sas
(spi: 0x800022D3(2147492563
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap
(sa timing: remaining key lifetime (k/sec): (4607997/3559
IV size: 8 bytes
replay detection support: Y
:inbound ah sas
:inbound pcp sas
:outbound esp sas
(spi: 0x88688F28(2288553768
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap
(sa timing: remaining key lifetime (k/sec): (4607997/3550
IV size: 8 bytes
replay detection support: Y
:outbound ah sas
:outbound pcp sas

```

```

svl-6#show crypto engine conn act
ID Interface IP- Address State Algorithm Encrypt Decrypt
Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 0 1
Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 24 200
Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 21 0 201

```

[معلومات ذات صلة](#)

- [صفحة دعم IPsec](#)
- [الدعم الفني - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا اء ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا