

Konfigurieren eines IPSec-Tunnels zwischen einem Cisco Router und einem Checkpoint NG

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdigramm](#)

[Konventionen](#)

[Konfigurieren des Cisco 1751 VPN-Routers](#)

[Konfigurieren des Prüfpunkts NG](#)

[Überprüfung](#)

[Überprüfen des Cisco Routers](#)

[Prüfpunkt NG überprüfen](#)

[Fehlerbehebung](#)

[Cisco Router](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird veranschaulicht, wie ein IPSec-Tunnel mit vorinstallierten Schlüsseln aufgebaut wird, um zwei private Netzwerke miteinander zu verbinden:

- Das private 172.16.15.x-Netzwerk im Router.
- Das private 192.168.10.x-Netzwerk im ^{Checkpoint™} Next Generation (NG).

Voraussetzungen

Anforderungen

Die in diesem Dokument beschriebenen Verfahren basieren auf diesen Annahmen.

- Die ^{Checkpoint™} NG-Grundrichtlinie wird eingerichtet.
- Alle Zugriffs-, Network Address Translation (NAT)- und Routing-Konfigurationen werden konfiguriert.
- Datenverkehr von innerhalb des Routers und innerhalb des ^{Checkpoint™} NG zum Internet fließt.

Verwendete Komponenten

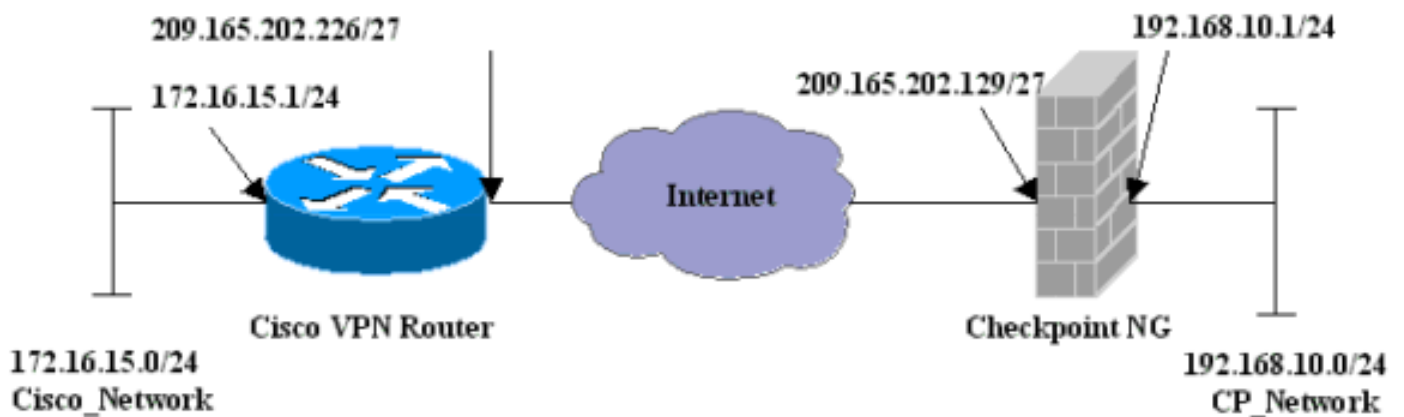
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Router 1751
- Cisco IOS® Software (C1700-K9O3SY7-M), Version 12.2(8)T4, RELEASE-SOFTWARE (fc1)
- Checkpoint™ NG Build 50027

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#).

Konfigurieren des Cisco 1751 VPN-Routers

```
Cisco VPN 1751-Router

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

```

Konfigurieren des Prüfpunkts NG

Das Checkpoint™ NG ist eine objektorientierte Konfiguration. Netzwerkobjekte und -regeln werden definiert, um die Richtlinie für die einzurichtende VPN-Konfiguration zu bilden. Diese Richtlinie wird dann mithilfe des Checkpoint™ NG Policy Editor installiert, um die Checkpoint™ NG-Seite der VPN-Konfiguration abzuschließen.

1. Erstellen Sie das Cisco Netzwerk-Subnetz und das Checkpoint™ NG-Netzwerk-Subnetz als Netzwerkobjekte. Das ist verschlüsselt. Wählen Sie zum Erstellen der Objekte **Verwalten > Netzwerkobjekte** und dann **Neu > Netzwerk aus**. Geben Sie die entsprechenden Netzwerkinformationen ein, und klicken Sie dann auf **OK**. Diese Beispiele zeigen eine Reihe von Objekten mit dem Namen CP_Network und

Network Properties - CP_Network

General NAT

Name: CP_Network

IP Address: 192.168.10.0

Net Mask: 255.255.255.0

Comment:

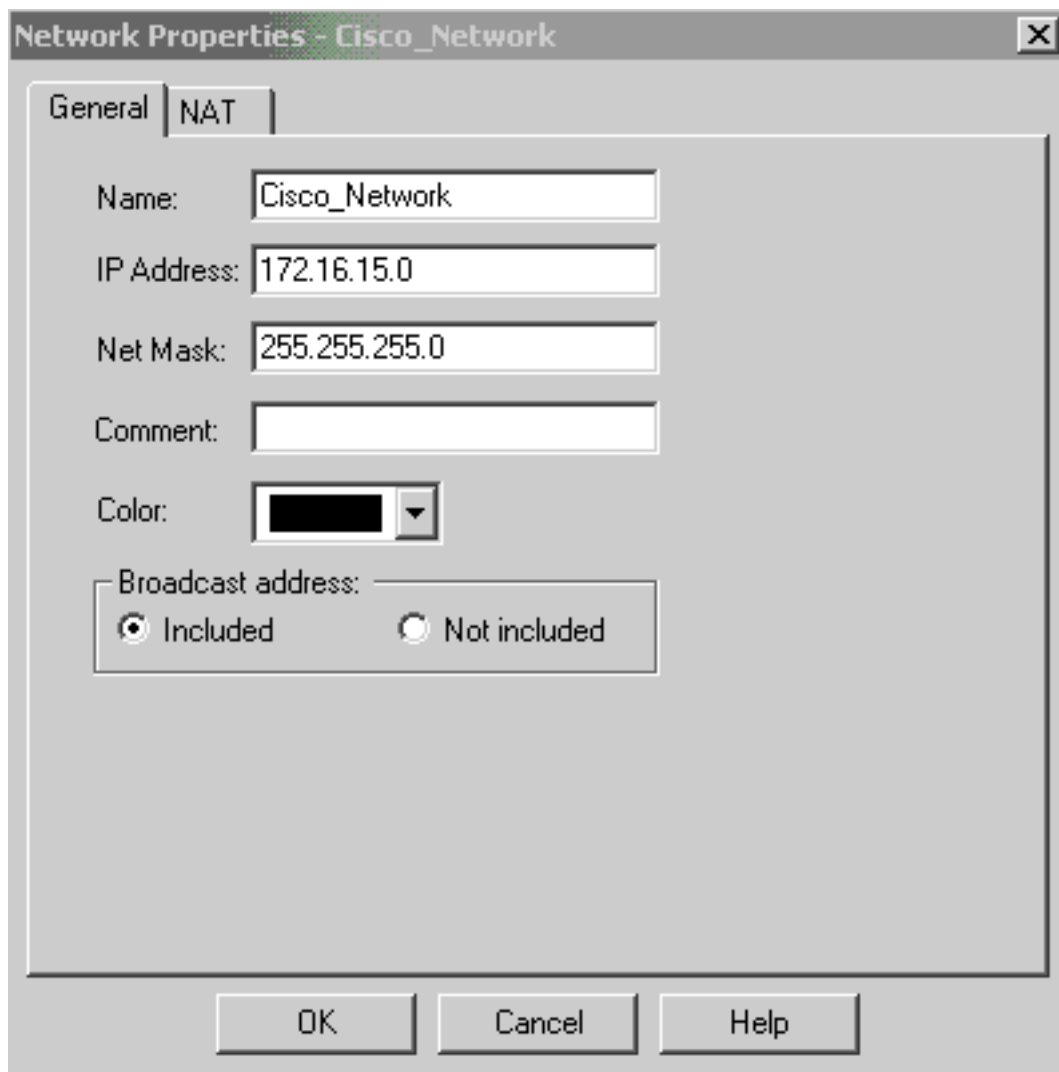
Color:

Broadcast address:

Included Not included

OK Cancel Help

Cisco_Network.



2. Erstellen Sie die Objekte Cisco_Router und Checkpoint_NG als Workstation-Objekte. Dies sind die VPN-Geräte. Wählen Sie zum Erstellen der Objekte **Verwalten > Netzwerkobjekte** und dann **Neu > Workstation aus**. Beachten Sie, dass Sie das ^{Checkpoint™} NG-Workstation-Objekt verwenden können, das während der ersten ^{Checkpoint™} NG-Einrichtung erstellt wurde. Wählen Sie die Optionen aus, um die Workstation als **Gateway** und **Interoperable VPN Device** festzulegen. Diese Beispiele zeigen eine Reihe von Objekten, die als Chef und Cisco_Router bezeichnet werden.

General

Topology

NAT

VPN

Authentication

Management

+ Advanced

General

Name: chef

IP Address: 209.165.202.129

Get address

Comment: CP_Server

Color: Type: Host Gateway

Check Point Products

 Check Point products installed: Version NG

- 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)

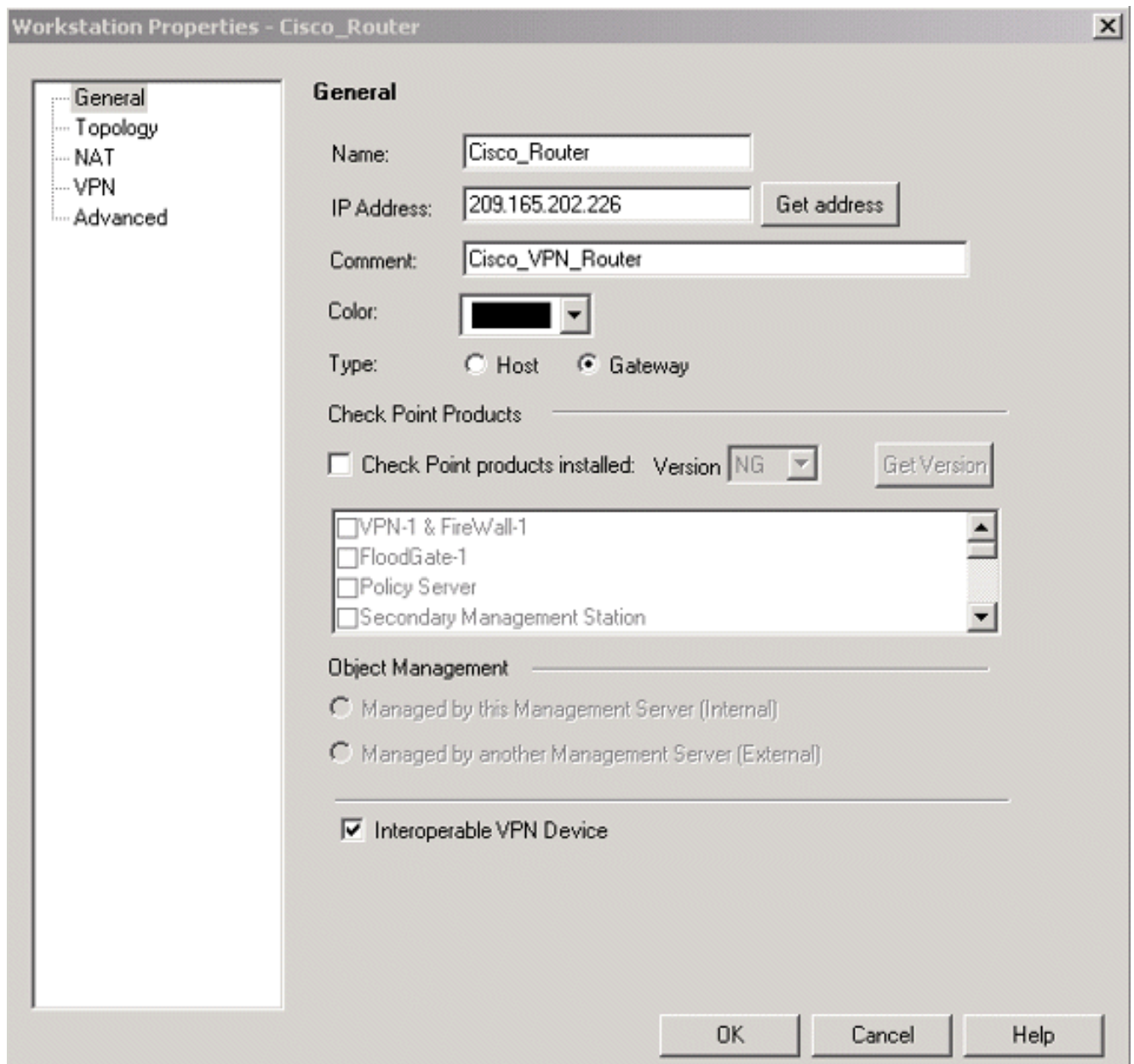
Secure Internal Communication

 DN: cn=cp_mgmt,o=chef.6h9tua Interoperable VPN Device

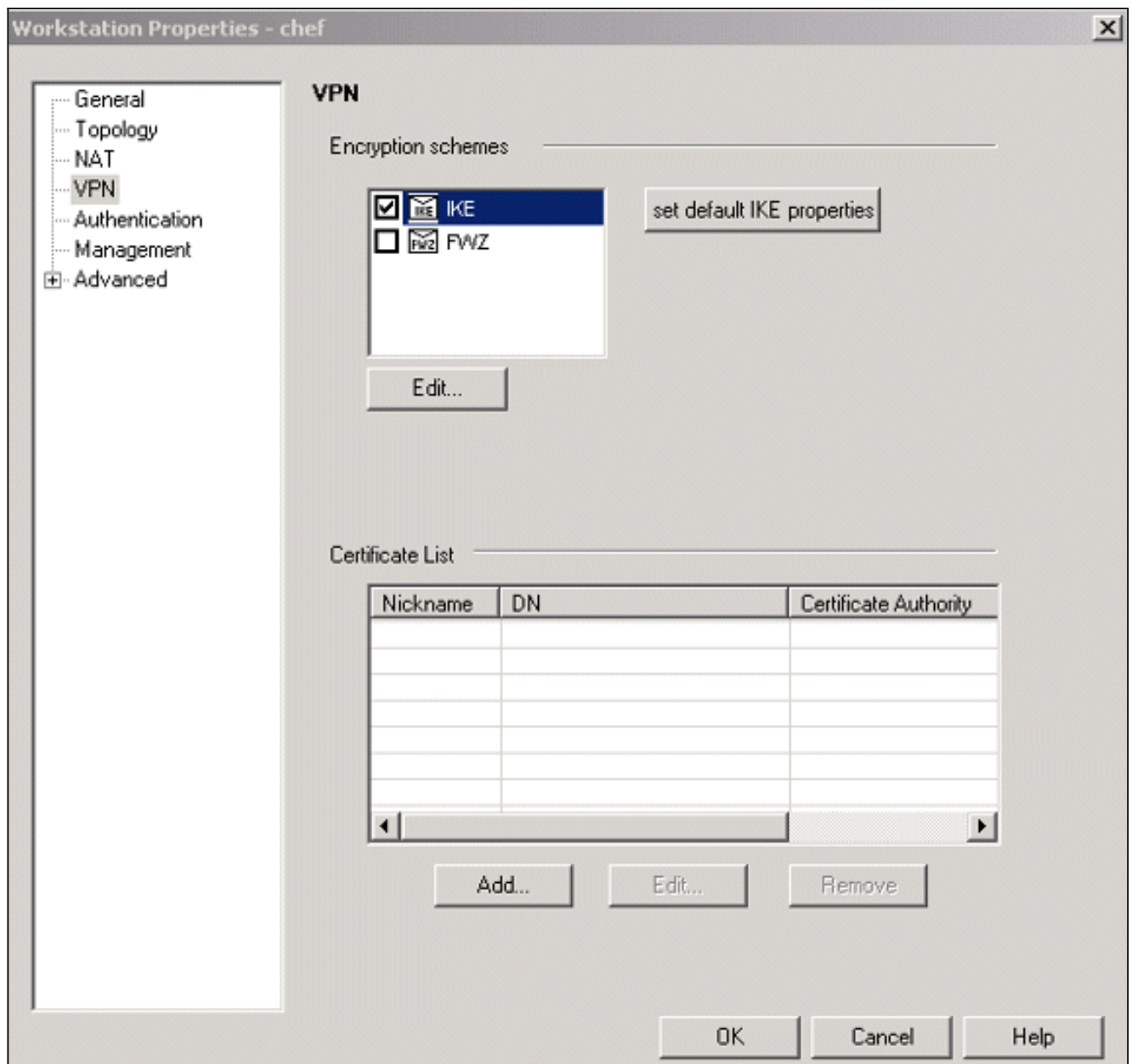
OK

Cancel

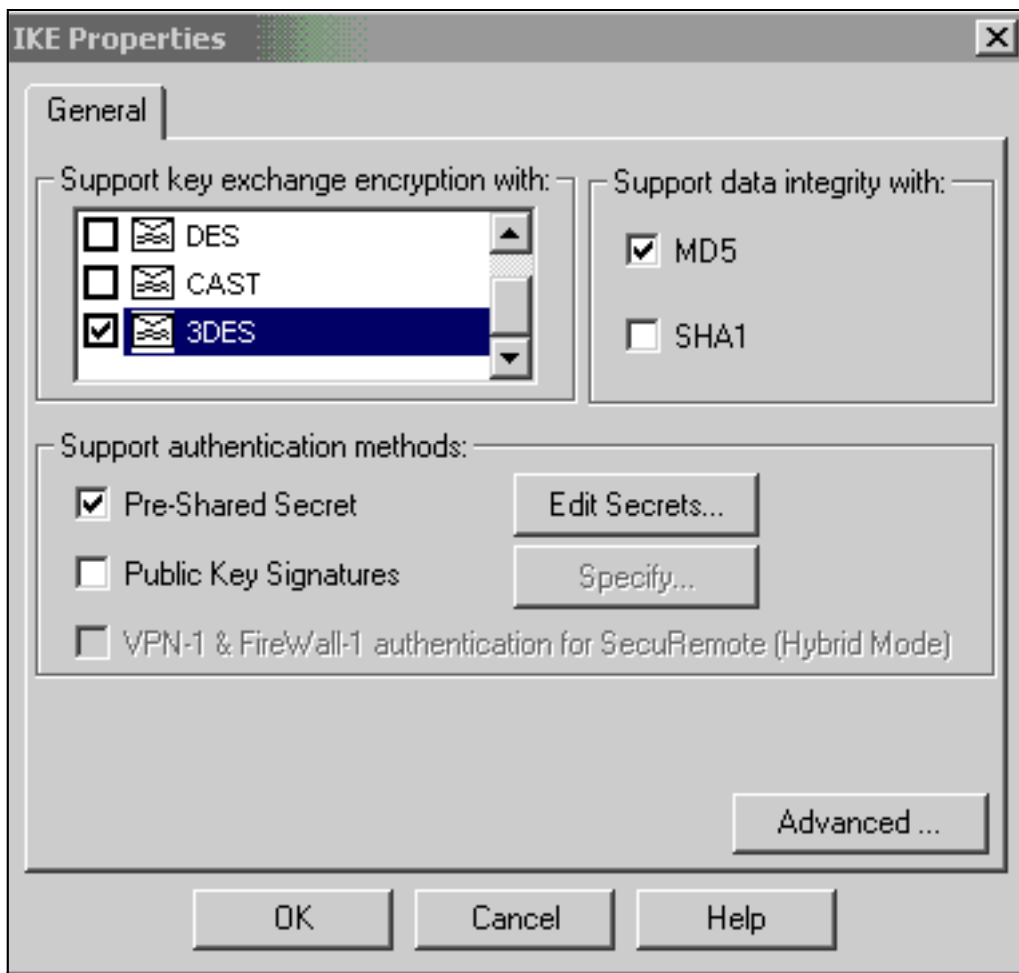
Help



3. Konfigurieren Sie IKE auf der Registerkarte VPN, und klicken Sie dann auf **Bearbeiten**.

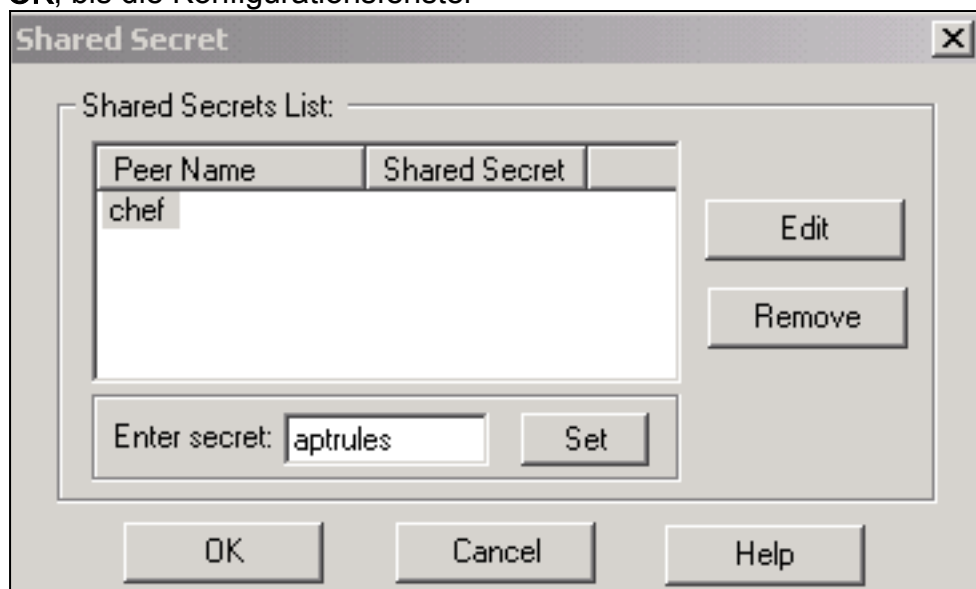


4. Konfigurieren Sie die Schlüsselaustauschrichtlinie, und klicken Sie auf **Edit**



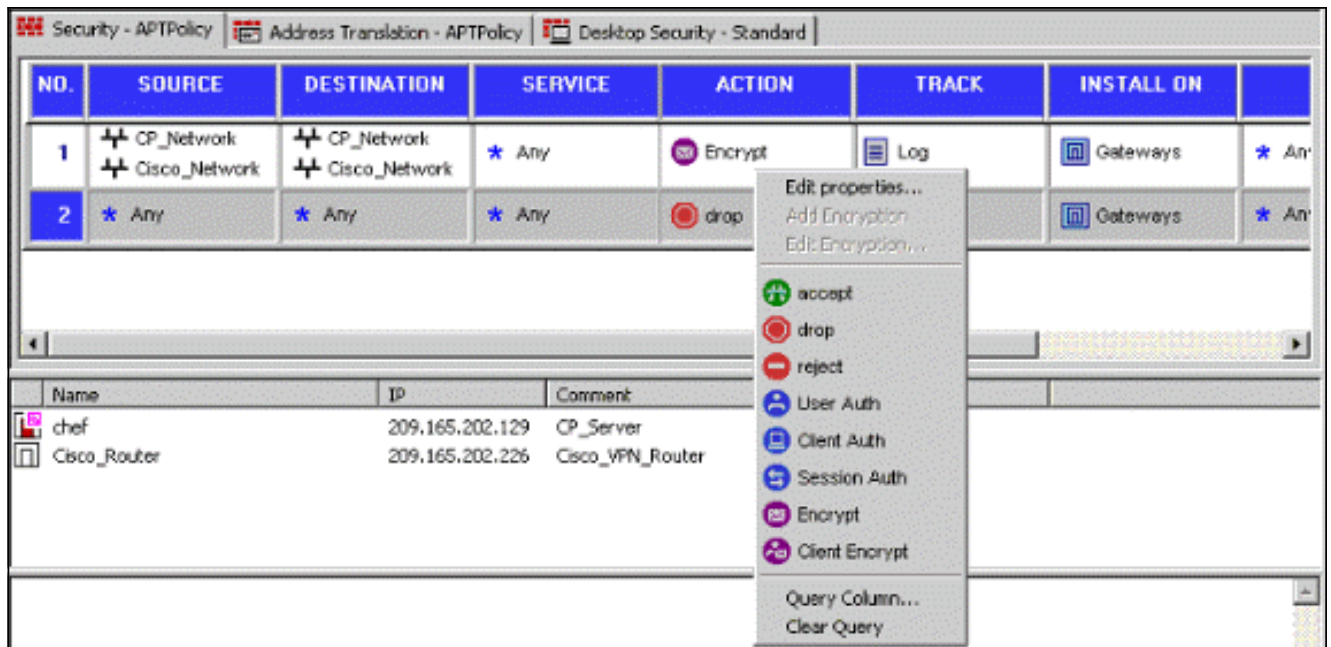
Secrets.

5. Legen Sie die zu verwendenden vorinstallierten Schlüssel fest, und klicken Sie dann mehrmals auf **OK**, bis die Konfigurationsfenster

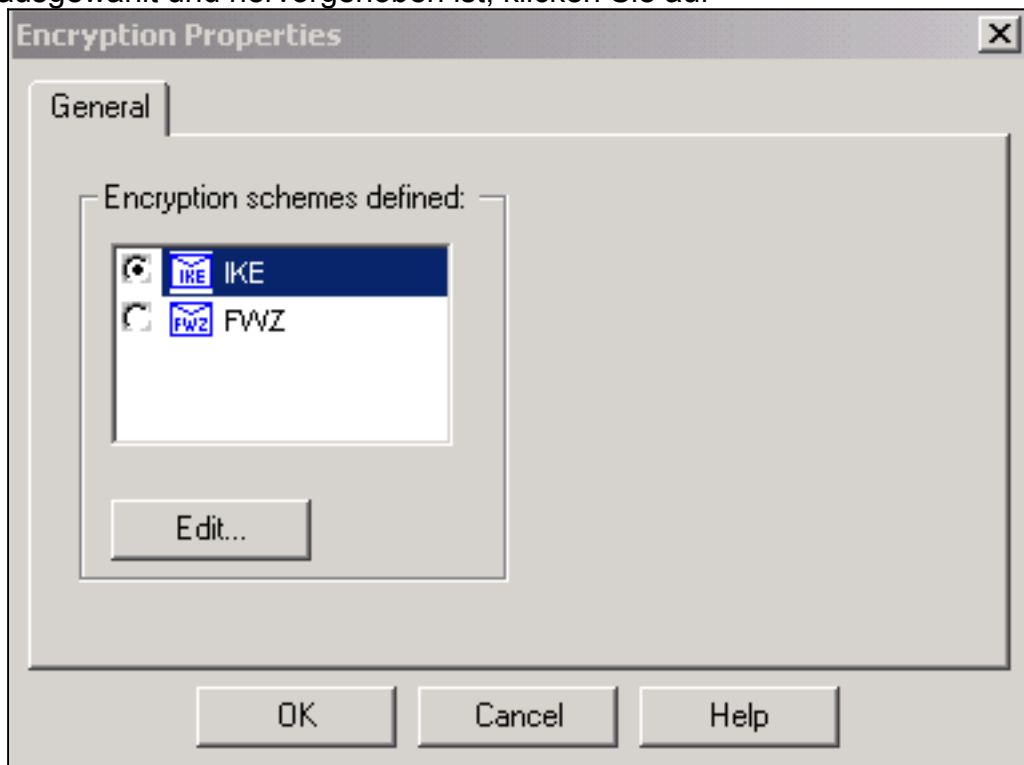


verschwinden.

6. Wählen Sie **Regeln > Regeln hinzufügen > Oben**, um die Verschlüsselungsregeln für die Richtlinie zu konfigurieren. Die Regel oben ist die erste Regel, die vor jeder anderen Regel ausgeführt wird, die die Verschlüsselung umgehen kann. Konfigurieren Sie die Quelle und das Ziel so, dass sie das CP_Network und das Cisco_Network enthalten, wie hier gezeigt. Nachdem Sie den Abschnitt "Encrypt Action" der Regel hinzugefügt haben, klicken Sie mit der rechten Maustaste auf **Aktion**, und wählen Sie **Eigenschaften bearbeiten** aus.

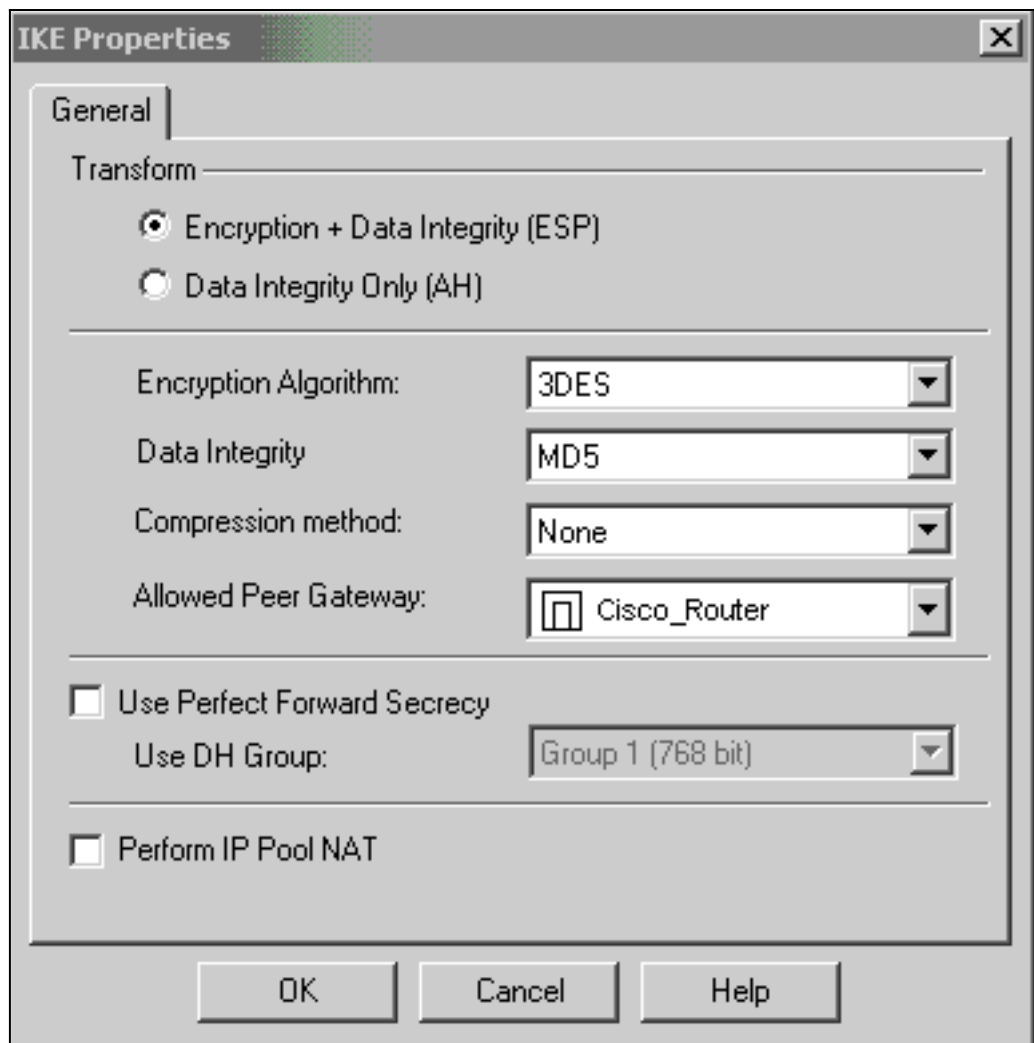


7. Wenn IKE ausgewählt und hervorgehoben ist, klicken Sie auf



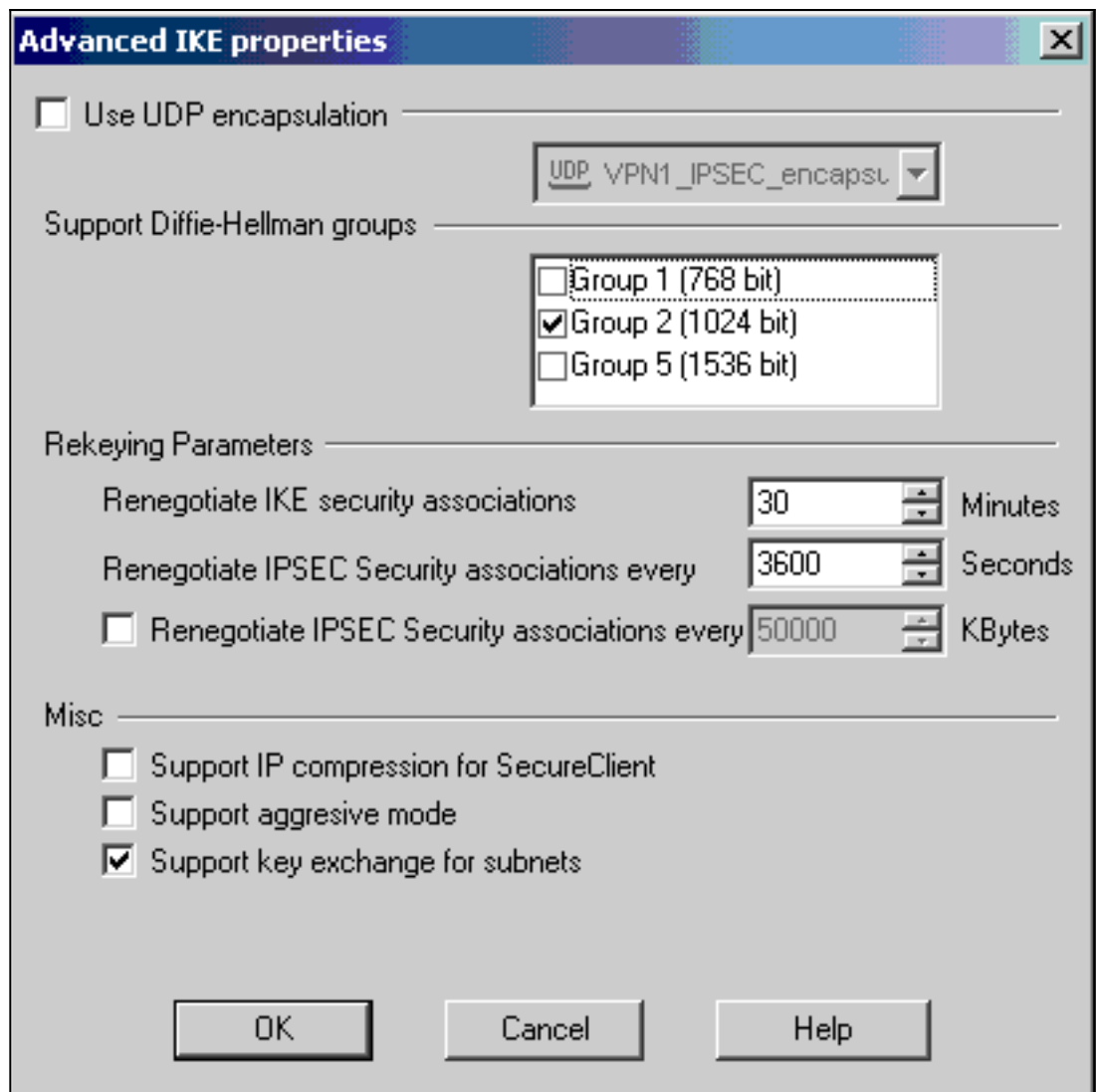
Bearbeiten.

8. Bestätigen Sie die IKE-



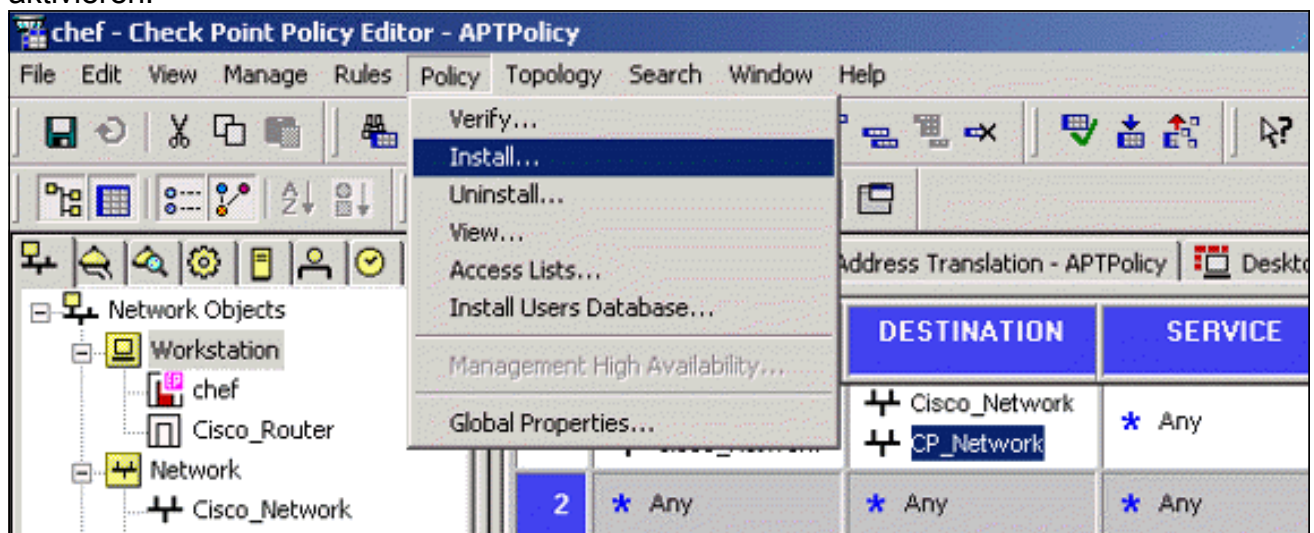
Konfiguration.

9. Eines der Hauptprobleme bei der Ausführung von VPN zwischen Cisco Geräten und anderen IPSec-Geräten ist die Neuaushandlung des Key Exchange. Stellen Sie sicher, dass die Einstellung für den IKE-Austausch auf dem Cisco Router exakt mit der Einstellung auf dem Checkpoint™ NG übereinstimmt. **Hinweis:** Der tatsächliche Wert dieses Parameters hängt von Ihrer jeweiligen Sicherheitsrichtlinie ab. In diesem Beispiel wurde die [IKE-Konfiguration auf dem Router](#) mit dem Befehl **lebenslange 1800** auf 30 Minuten festgelegt. Der gleiche Wert muss auf dem Checkpoint™ NG festgelegt werden. Um diesen Wert für Checkpoint™ NG festzulegen, wählen Sie **Netzwerkobjekt verwalten**, wählen Sie anschließend das Checkpoint™ NG-Objekt aus, und klicken Sie auf **Bearbeiten**. Wählen Sie anschließend **VPN** aus, und bearbeiten Sie IKE. Wählen Sie **Advance aus**, und konfigurieren Sie die Neueingabeparameter. Nachdem Sie den Schlüsselaustausch für das Checkpoint™ NG-Netzwerkobjekt konfiguriert haben, führen Sie die gleiche Konfiguration der Neuverhandlung von Key Exchange für das Cisco_Router-Netzwerkobjekt durch. **Hinweis:** Stellen Sie sicher, dass die richtige Diffie-Hellman-Gruppe ausgewählt ist, die mit der auf dem Router konfigurierten Gruppe

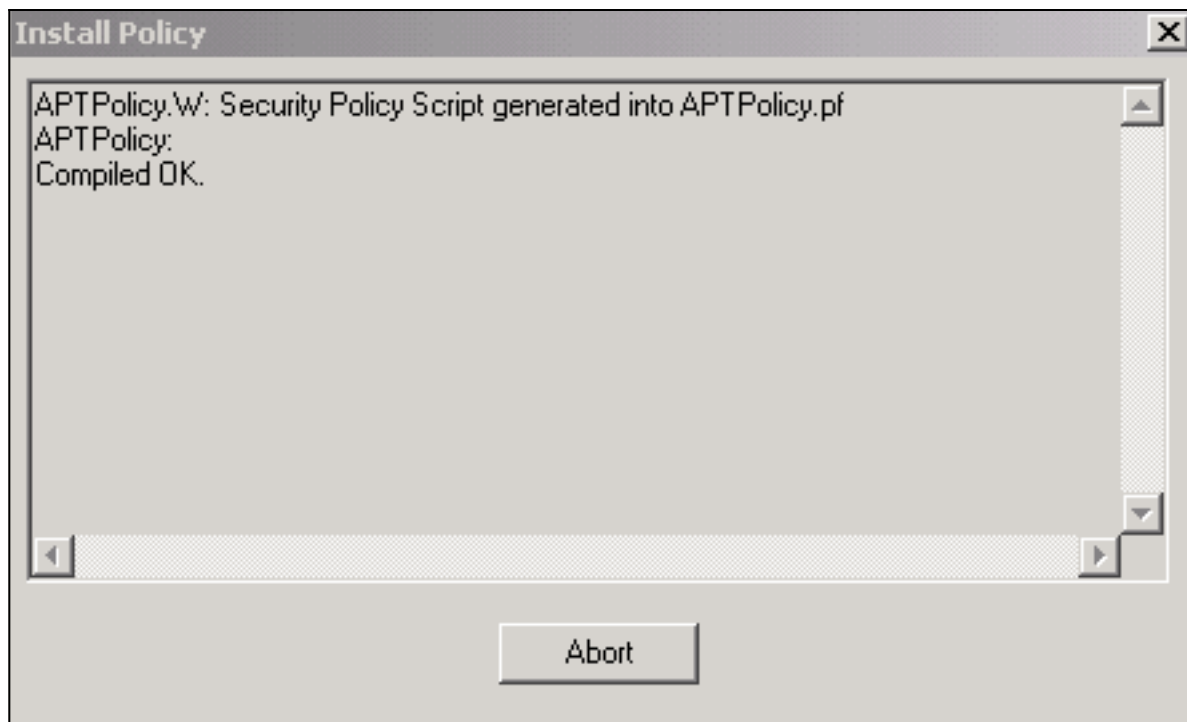


übereinstimmt.

- Die Richtlinienkonfiguration ist abgeschlossen. Speichern Sie die Richtlinie, und wählen Sie **Richtlinie > Installieren**, um sie zu aktivieren.

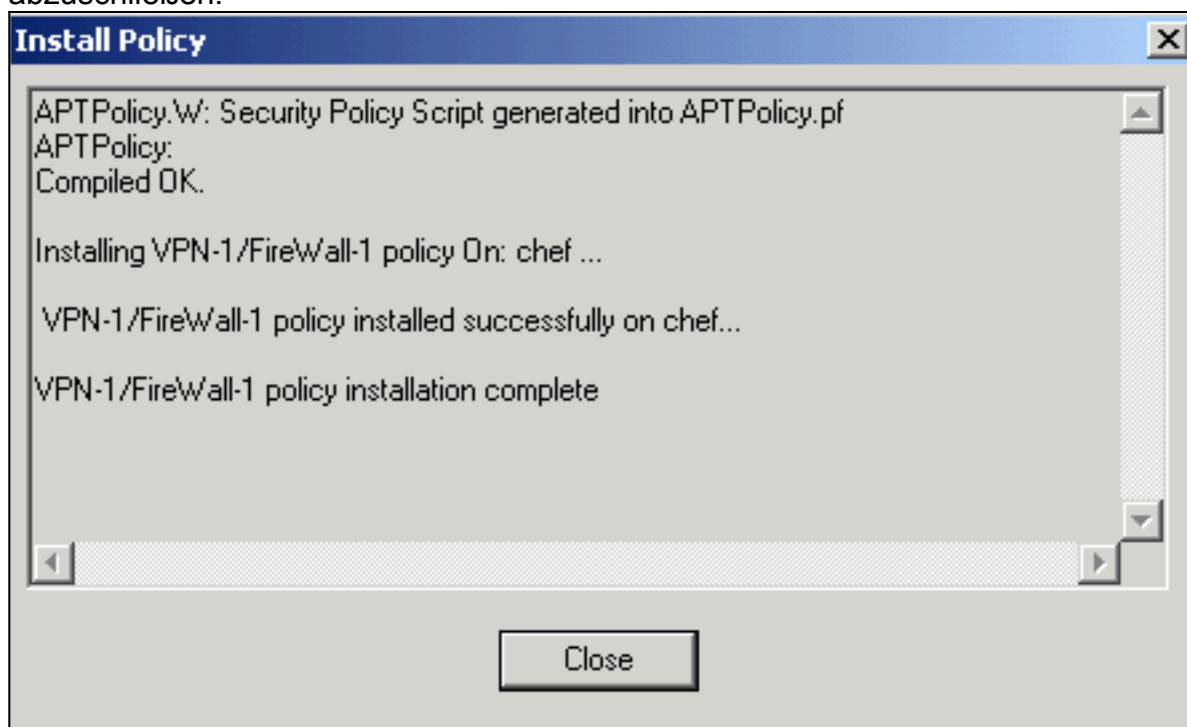


Im Installationsfenster werden beim Kompilieren der Richtlinie Fortschrittshinweise angezeigt.



Wenn

das Installationsfenster anzeigt, dass die Richtlinieninstallation abgeschlossen ist, klicken Sie auf **Schließen**, um das Verfahren abzuschließen.



Überprüfung

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

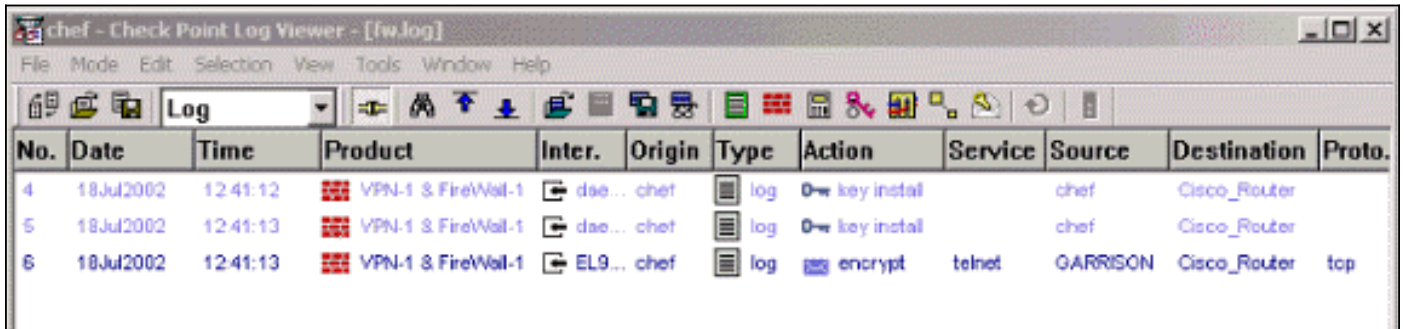
Überprüfen des Cisco Routers

Einige Befehle des Typs **show** werden vom Tool [Output Interpreter unterstützt \(nur für registrierte Kunden\)](#), mit dem sich [Analysen der Ausgabe von Befehlen des Typs show abrufen lassen](#).

- **show crypto isakmp sa:** Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an.
- **show crypto ipsec sa:** Zeigt die von aktuellen SAs verwendeten Einstellungen an.

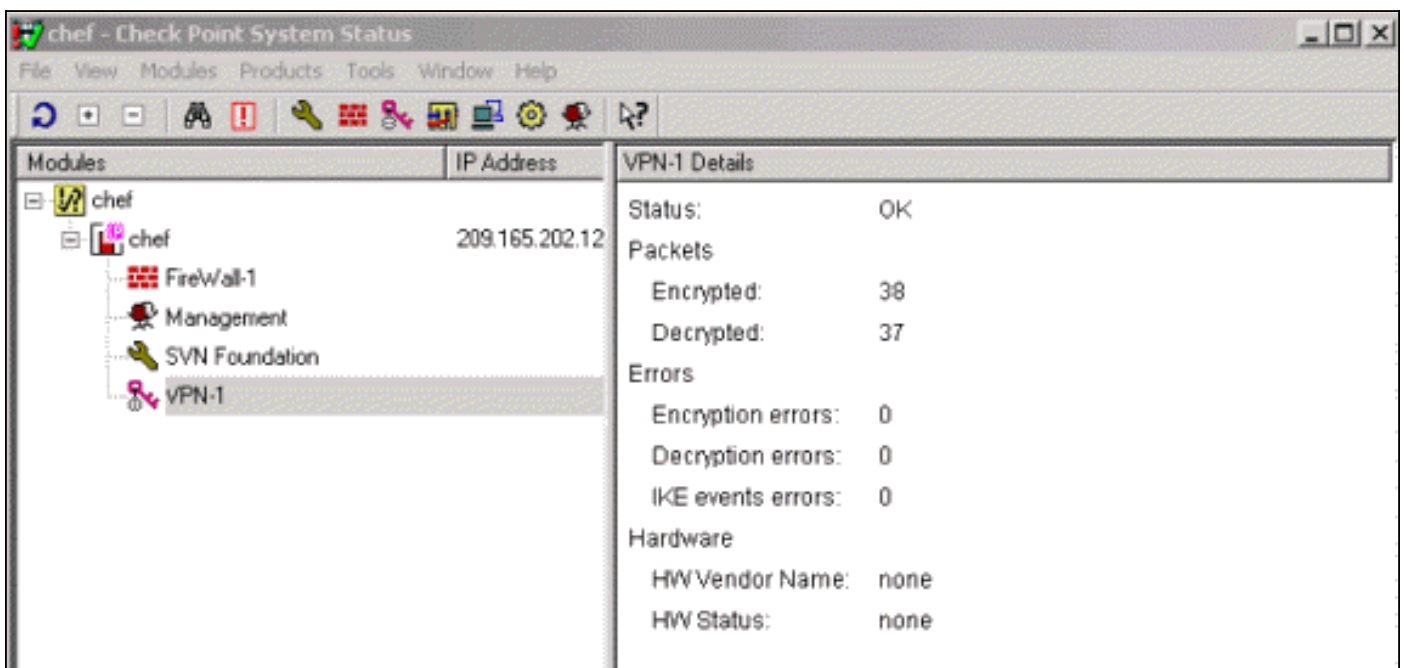
Prüfpunkt NG überprüfen

Um die Protokolle anzuzeigen, wählen Sie **Fenster > Protokollanzeige**.



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	tcp

Um den Systemstatus anzuzeigen, wählen Sie **Fenster > Systemstatus**.



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

Fehlerbehebung

Cisco Router

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Weitere Informationen zur Fehlerbehebung finden Sie unter [IP Security Troubleshooting - Understanding and Using debug Commands](#).

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie [Wichtige Informationen über Debug-Befehle](#).

- **debug crypto engine** - Zeigt Debugmeldungen über Krypto Engines an, die Verschlüsselung

und Entschlüsselung durchführen.

- **debug crypto isakmp**: Zeigt Meldungen über IKE-Ereignisse an.
- **debug crypto ipsec**: Zeigt IPSec-Ereignisse an.
- **clear crypto isakmp** - Löscht alle aktiven IKE-Verbindungen.
- **clear crypto sa**: Löscht alle IPSec SAs.

Erfolgreiche Debug Log-Ausgabe

```
18:05:32: ISAKMP (0:0): received packet from
209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: 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
but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
against priority 1 policy
18:05:32: 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
18:05:33: 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,
IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
MM_KEY_EXCH
```

18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
QM_IDLE
18:05:33: ISAKMP (0:1): processing HASH payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing SA payload.
message ID = -1335371103
18:05:33: 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,
(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
18:05:33: ISAKMP (0:1): processing NONCE payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec
18:05:33: ISAKMP (0:1): Node -1335371103,
Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA
from 209.165.202.226 to 209.165.202.129 for prot 3

18:05:33: ISAKMP: received ke message (2/1)
18:05:33: ISAKMP (0:1): sending packet to
209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Node -1335371103,
Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
18:05:33: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Creating IPsec SAs
18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226
(proxy 192.168.10.0 to 172.16.15.0)
18:05:33: 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
(proxy 172.16.15.0 to 192.168.10.0)
18:05:33: 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
FALSE reason "quick mode done (await())"
18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(initialize_sas): ,
(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
18:05:33: IPSEC(initialize_sas): ,
(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
18:05:33: IPSEC(create_sa): sa created,
(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
18:05:33: IPSEC(create_sa): sa created,
(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
18:05:34: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103
18:05:34: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2

18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103

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

```
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, #recv 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
1 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 0
200 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 24
201 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 21 0
```

[Zugehörige Informationen](#)

- [IPSec-Support-Seite](#)
- [Technischer Support – Cisco Systems](#)