Konfigurieren eines IPsec-Tunnels - Cisco Router zu Checkpoint Firewall 4.1

Inhalt

Einführung

In diesem Dokument wird veranschaulicht, wie ein IPsec-Tunnel mit vorinstallierten Schlüsseln aufgebaut wird, um zwei private Netzwerke miteinander zu verbinden: das private Netzwerk 192.168.1.x innerhalb des Cisco Routers und das private Netzwerk 10.32.50.x innerhalb der Checkpoint-Firewall.

Voraussetzungen

Anforderungen

Bei dieser Beispielkonfiguration wird davon ausgegangen, dass der Datenverkehr vom Router und innerhalb des Prüfpunkts zum Internet (dargestellt durch die Netzwerke 172.18.124.x) fließt, bevor Sie mit der Konfiguration beginnen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Router der Serie 3600

- Cisco IOS® Software (C3640-JO3S56I-M), Version 12.1(5)T, Release-SOFTWARE (fc1)
- Checkpoint-Firewall 4.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

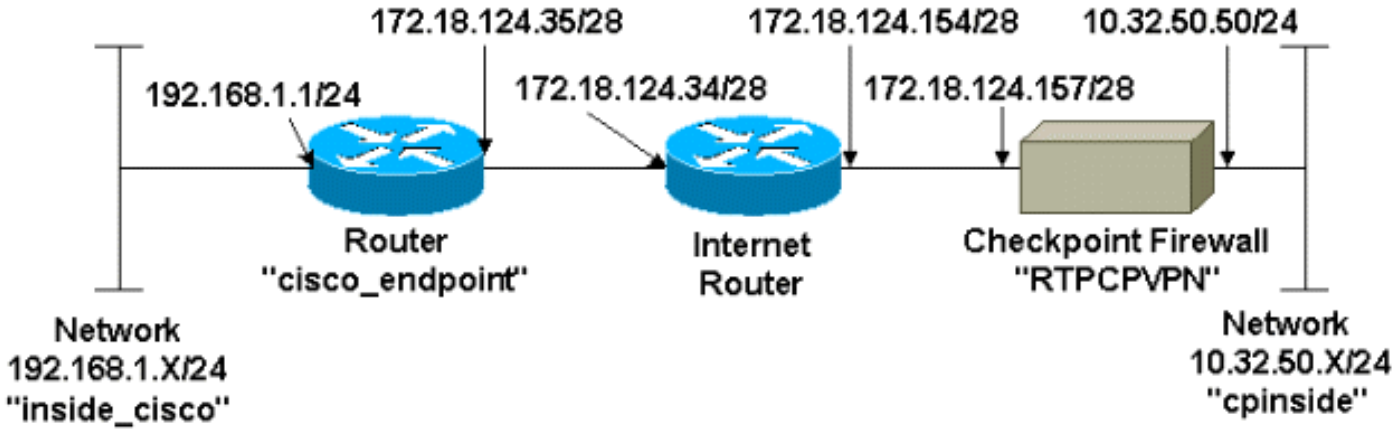
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- Routerkonfiguration
- Checkpoint-Firewall-Konfiguration

Routerkonfiguration

Konfiguration des Cisco 3600 Routers
`Current configuration : 1608 bytes` `!`

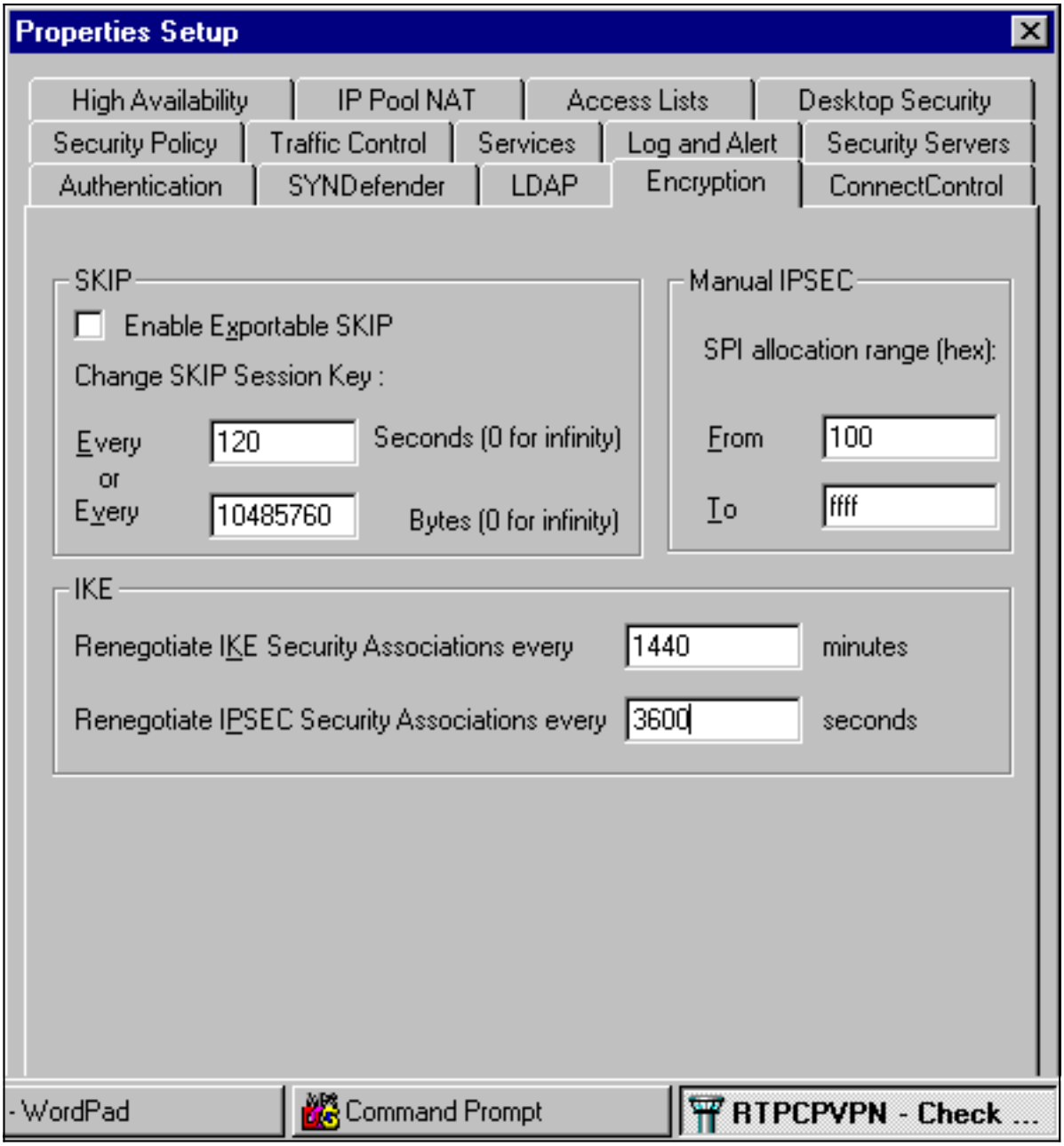
```
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des esp-sha-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
!
controller T1 1/0
!
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.255.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
```

```
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 115 permit ip 192.168.1.0 0.0.0.255
10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

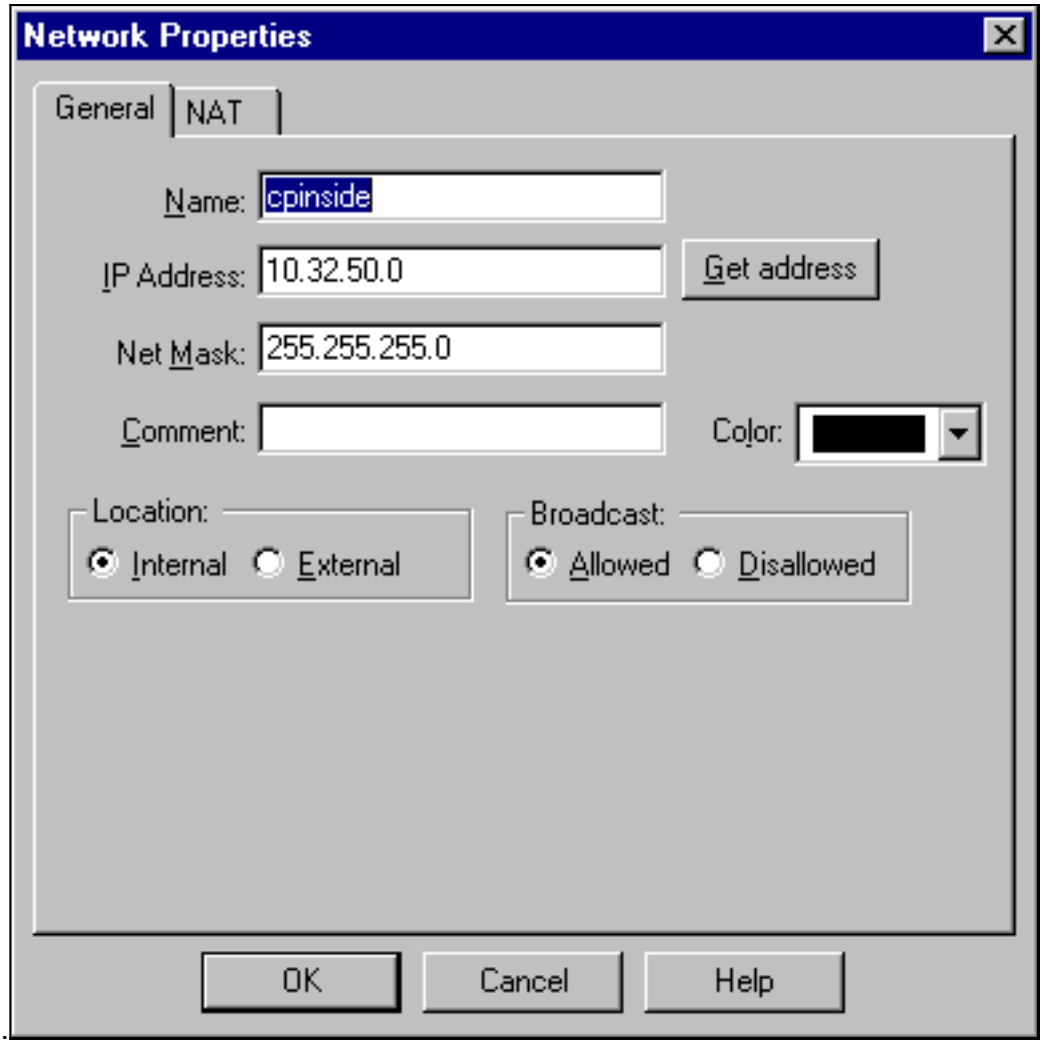
Checkpoint-Firewall-Konfiguration

Führen Sie diese Schritte aus, um die Checkpoint-Firewall zu konfigurieren.

1. Da sich die Standard-Lebensdauer von IKE und IPsec von Anbieter zu Anbieter unterscheidet, wählen Sie **Eigenschaften > Verschlüsselung aus,** um die Lebensdauer des Prüfpunkts so einzustellen, dass sie den Cisco Standardeinstellungen entspricht.Die IKE-Standardlebensdauer von Cisco beträgt 86400 Sekunden (= 1440 Minuten) und kann mithilfe der folgenden Befehle geändert werden:**crypto isakmp policy #Lebenszeitnr.**Die konfigurierbare Cisco IKE-Lebensdauer beträgt 60-86400 Sekunden. Die standardmäßige IPsec-Lebensdauer von Cisco beträgt 3.600 Sekunden und kann mit dem **Befehl crypto ipsec security-associated life seconds #**(Lebensdauer der **Crypto ipsec-Sicherheitszuordnung)** geändert werden.Die konfigurierbare Cisco IPsec-Lebensdauer beträgt 120-86400 Sekunden.

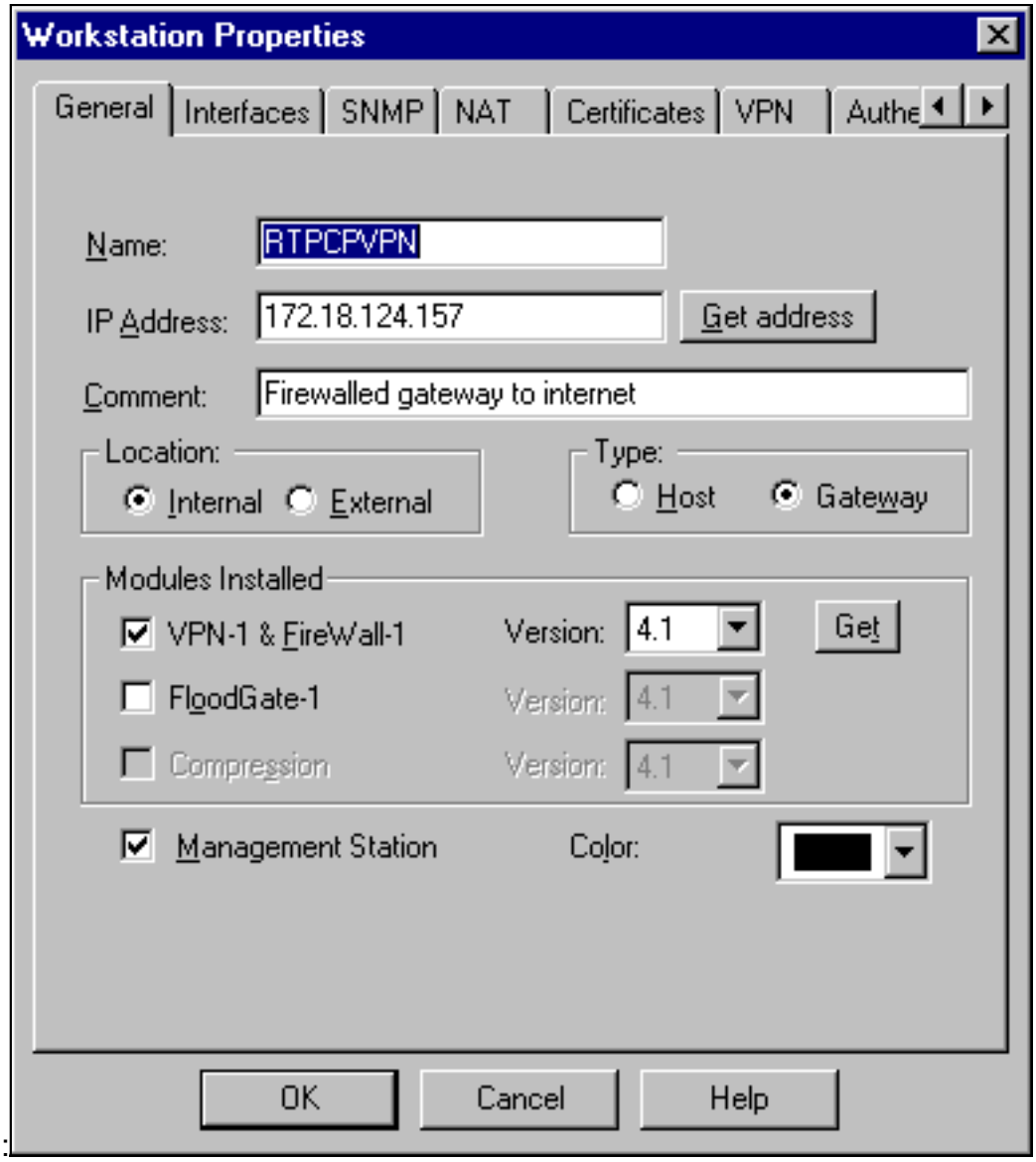


2. Wählen Sie **Verwalten > Netzwerkobjekte > Neu (oder Bearbeiten) > Netzwerk** aus, um das Objekt für das interne Netzwerk (als "cpinside" bezeichnet) hinter dem Prüfpunkt zu konfigurieren.Dies sollte mit dem Ziel-Netzwerk (zweites) im Befehl **access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255** übereinstimmen.Wählen Sie **Interne** unter



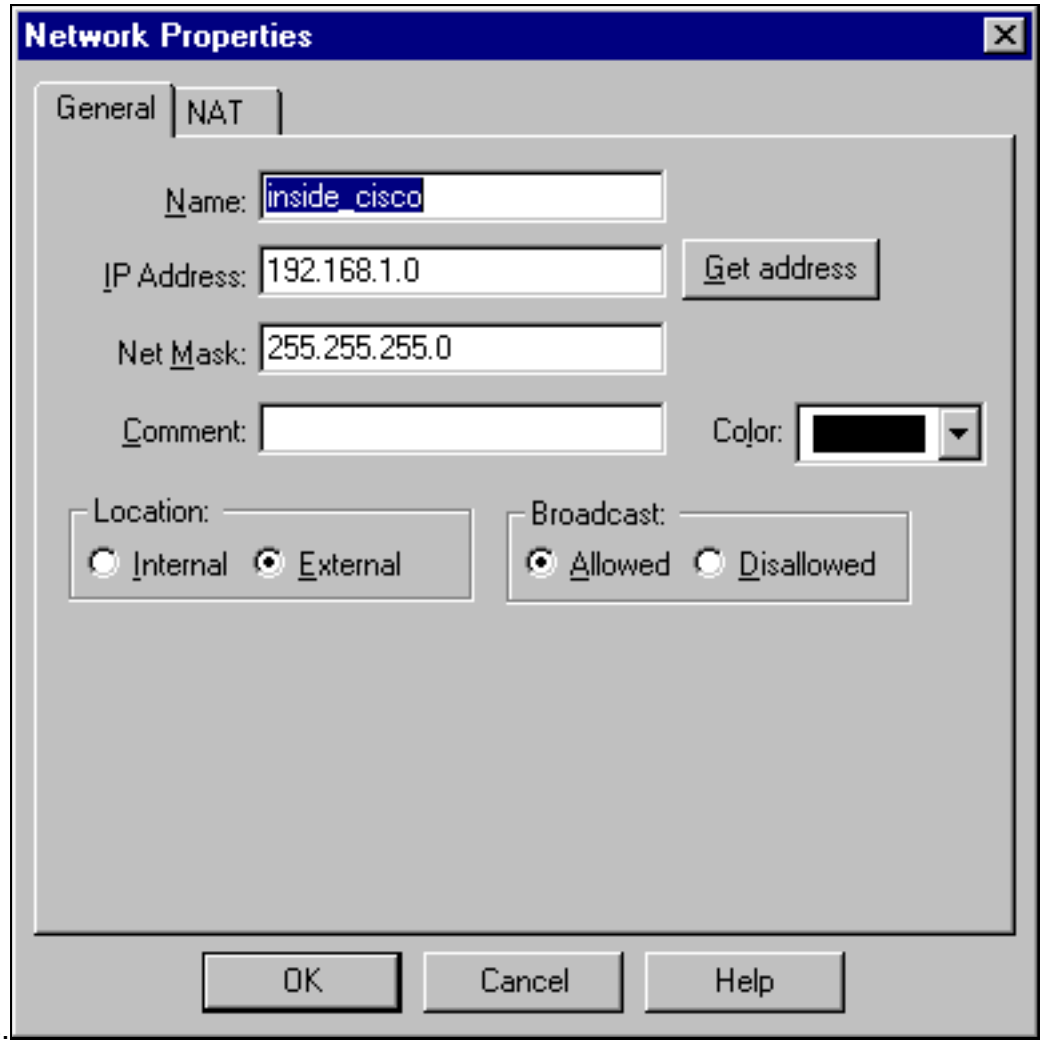
Speicherort aus.

3. Wählen Sie **Verwalten > Netzwerkobjekte > Bearbeiten**, um das Objekt für den RTPCPVPN Checkpoint (Gateway)-Endpunkt zu bearbeiten, auf den der Cisco Router im Befehl **set peer 172.18.124.157** verweist.Wählen Sie **Interne** unter Speicherort aus. Wählen Sie als Typ **Gateway** aus. Aktivieren Sie unter Installierte Module das Kontrollkästchen **VPN-1 & FireWall-1**, und aktivieren Sie außerdem das Kontrollkästchen **Management**



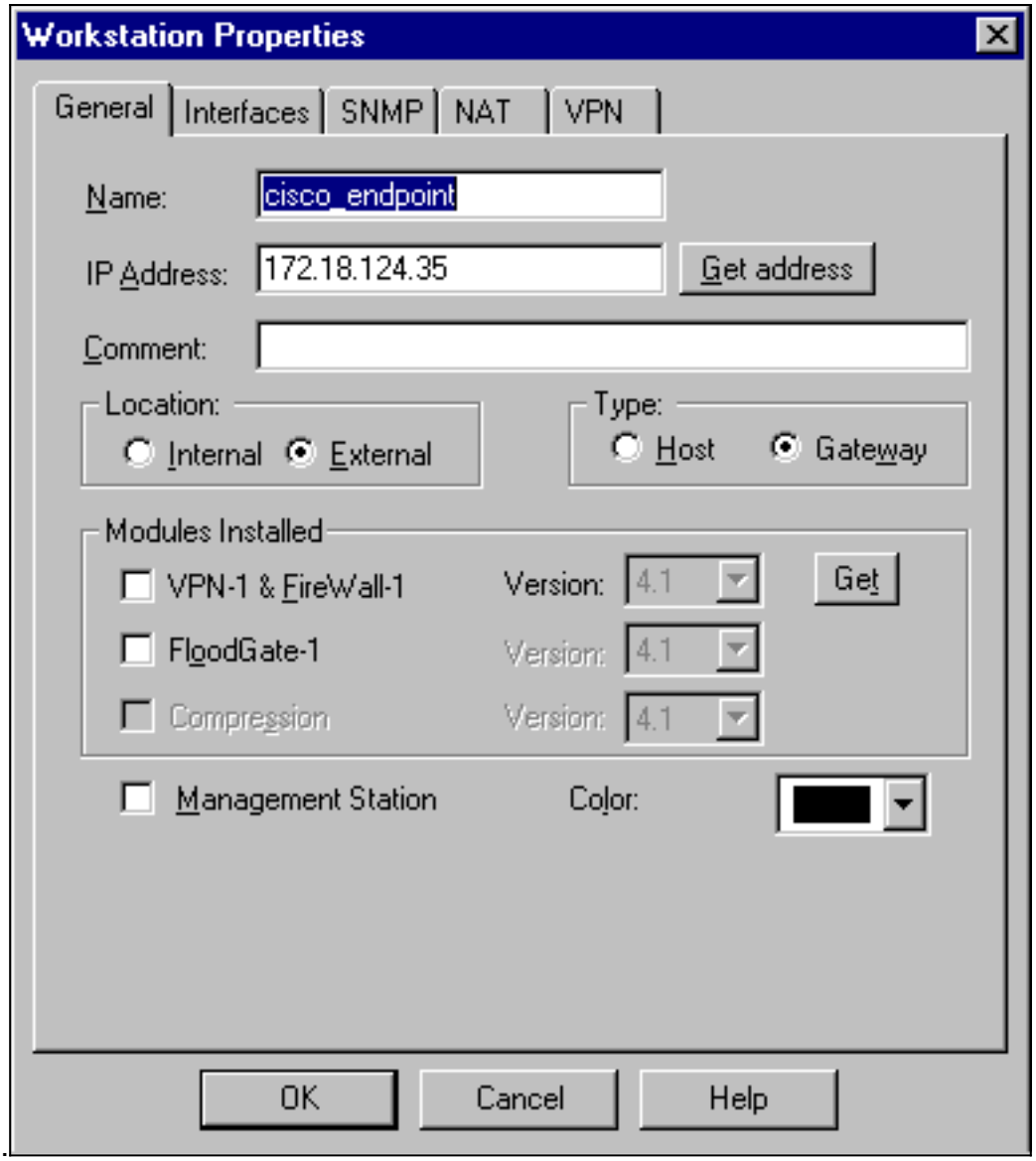
Station:

4. Wählen Sie **Verwalten > Netzwerkobjekte > Neu > Netzwerk**, um das Objekt für das externe Netzwerk (namens "inside_cisco") hinter dem Cisco Router zu konfigurieren.Dies sollte mit dem Quell-(Erstes) Netzwerk im Cisco **Zugriffsliste-**Befehl **115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.255** übereinstimmen.Wählen Sie **Extern** unter Speicherort

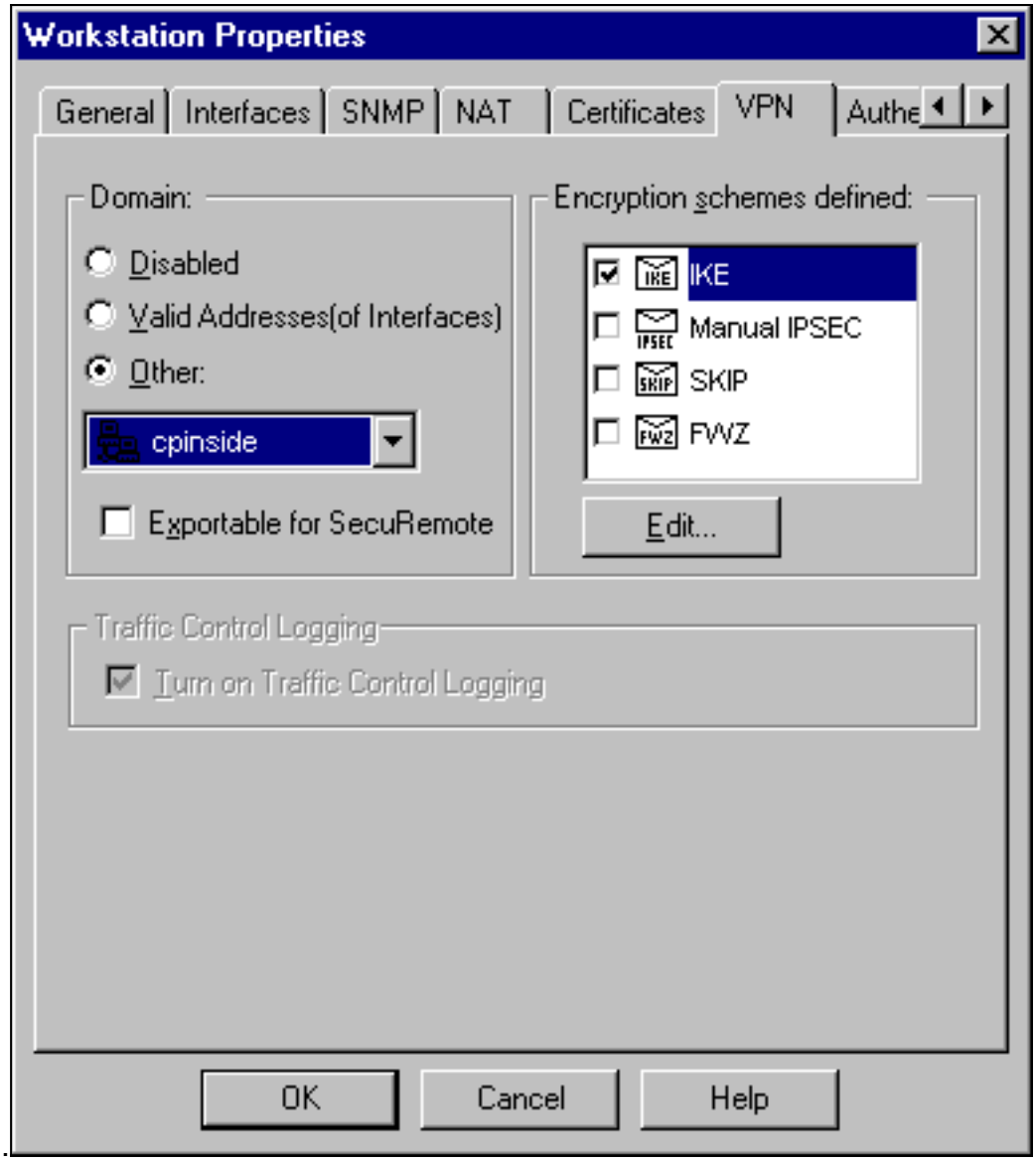


aus.

5. Wählen Sie **Verwalten > Netzwerkobjekte > Neu > Workstation**, um ein Objekt für das externe Cisco Router-Gateway (auch "cisco_endpoint" genannt) hinzuzufügen. Dies ist die Cisco-Schnittstelle, auf die der **Befehl crypto map *name* angewendet** wird.Wählen Sie **Extern** unter Speicherort aus. Wählen Sie als Typ **Gateway** aus.**Hinweis:** Aktivieren Sie nicht das Kontrollkästchen VPN-1/FireWall-

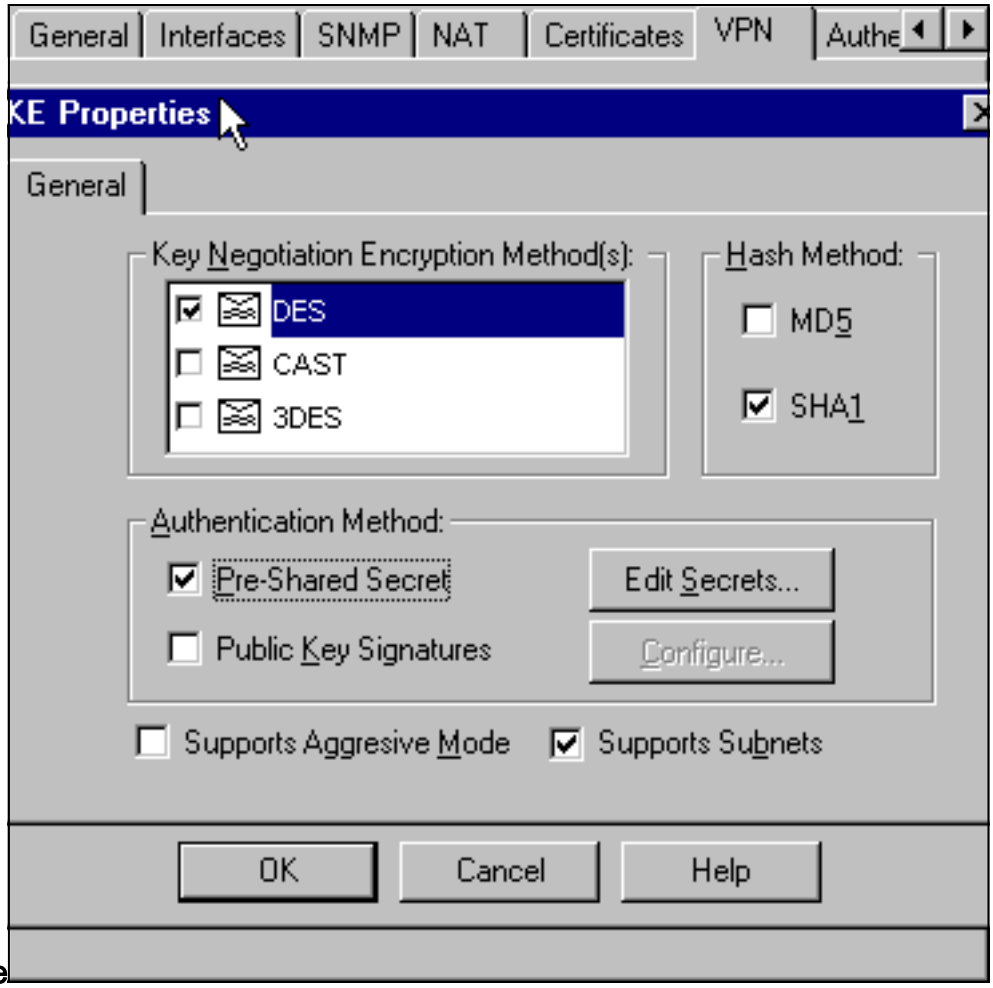
1. 

6. Wählen Sie **Verwalten > Netzwerkobjekte > Bearbeiten**, um die Registerkarte für das Checkpoint Gateway-Endgerät (RTPCPVPN genannt) zu bearbeiten. Wählen Sie unter Domain (Domäne) die Option **Other (Andere**) aus, und wählen Sie dann die Innenseite des Checkpoint-Netzwerks (als "cpinside" bezeichnet) aus der Dropdown-Liste aus. Wählen Sie unter Definierte Verschlüsselungsschemata die Option **IKE aus**, und klicken Sie dann auf



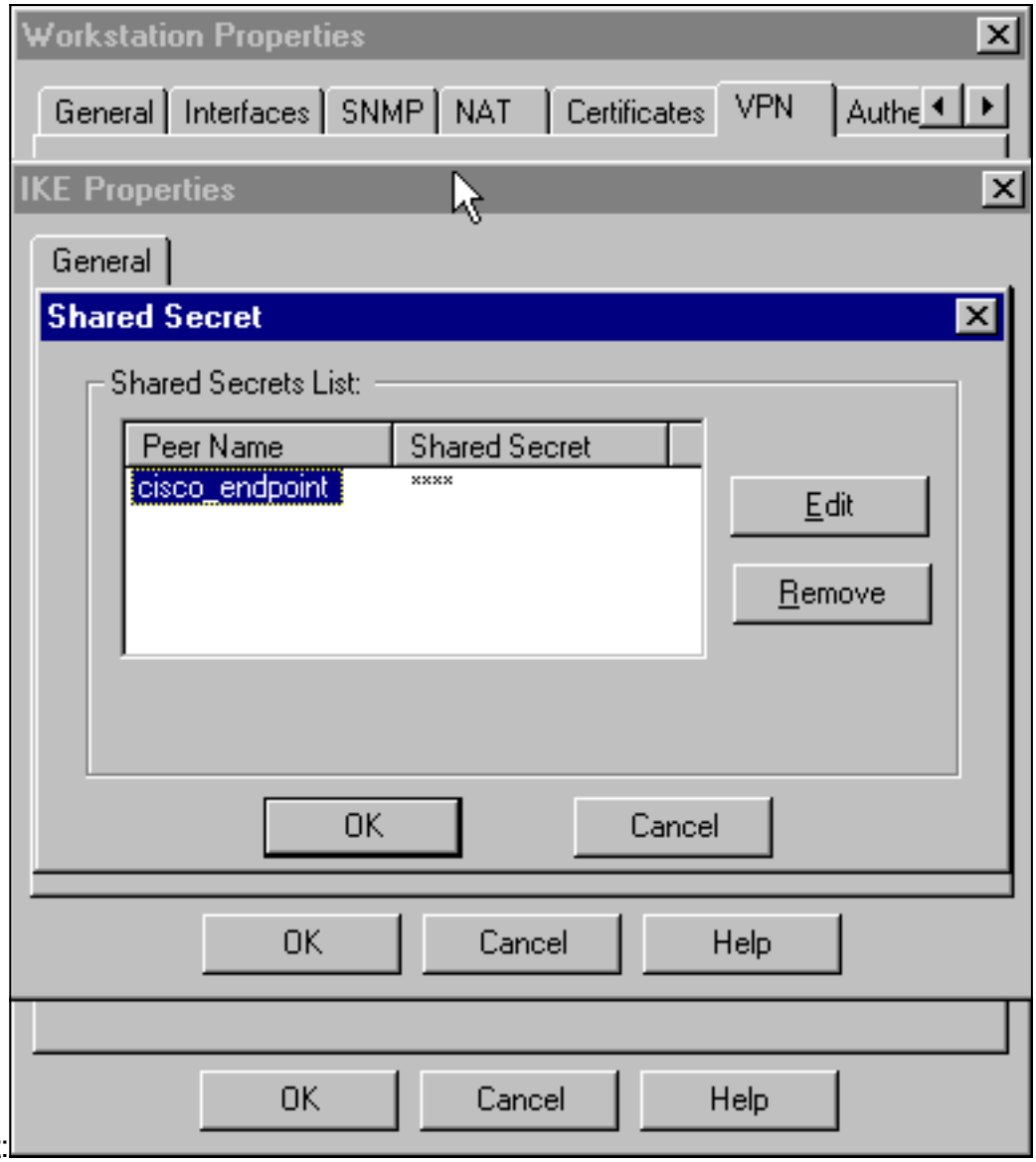
Bearbeiten.

7. Ändern Sie die IKE-Eigenschaften für die DES-Verschlüsselung, um diesen Befehlen zuzustimmen:**crypto isakmp policy #VerschlüsselungHinweis:** Die DES-Verschlüsselung ist die Standardeinstellung, daher ist sie in der Cisco Konfiguration nicht sichtbar.
8. Ändern Sie die IKE-Eigenschaften in SHA1-Hashing, um diesen Befehlen zuzustimmen:**crypto isakmp policy #Hash-ShaHinweis:** Der SHA-Hashing-Algorithmus ist die Standardeinstellung, sodass er in der Cisco Konfiguration nicht angezeigt wird.Ändern Sie diese Einstellungen:Deaktivieren Sie die **Option Aggressiver Modus**.Aktivieren Sie **Subnetze unterstützen**.Aktivieren Sie **Pre-Shared Secret** unter Authentication Method. Dies entspricht den folgenden Befehlen:**crypto isakmp policy #Authentifizierung Pre-**



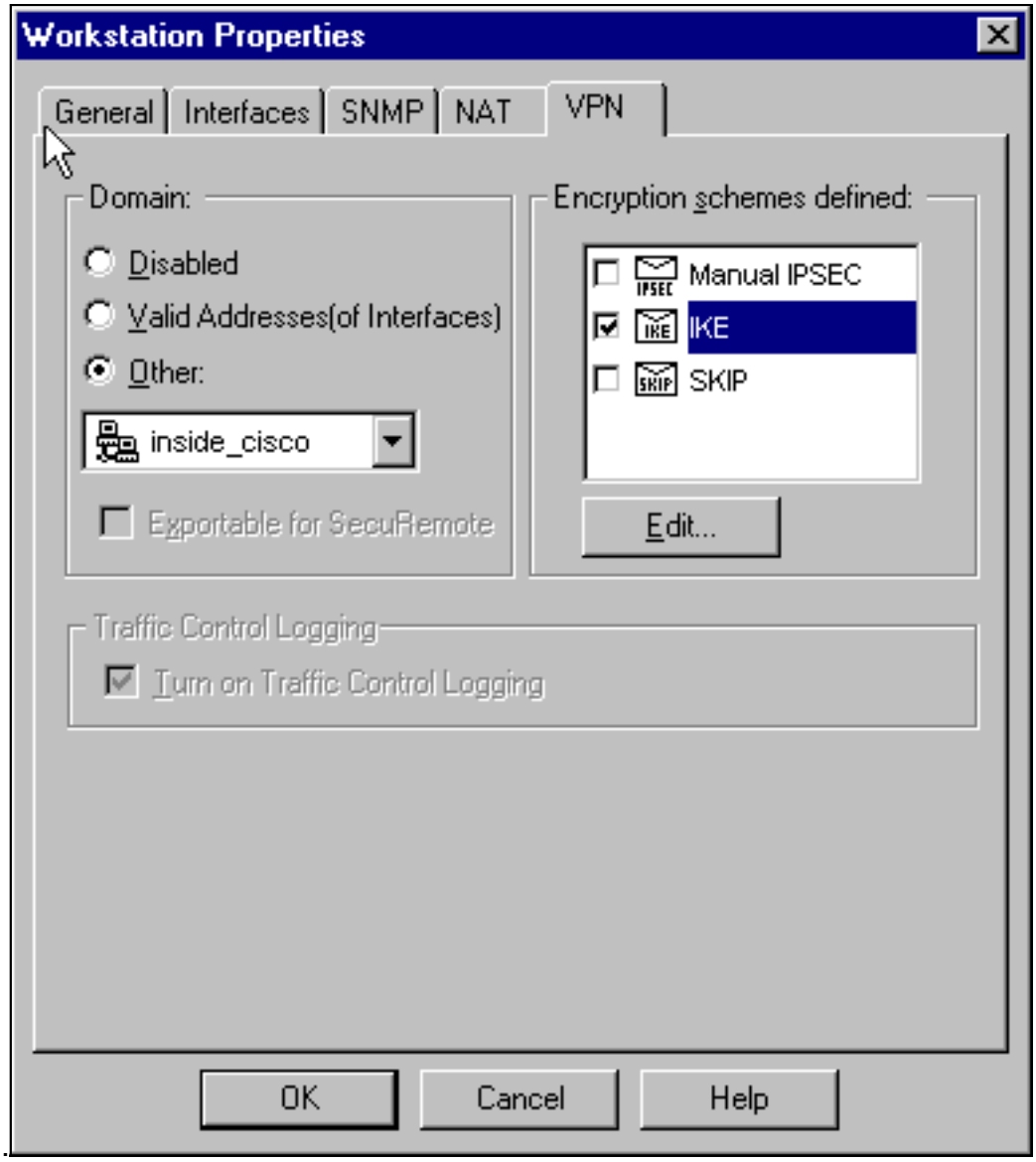
Share

9. Klicken Sie auf **Edit Secrets** (Geheimnisse **bearbeiten**), um den vorinstallierten Schlüssel so festzulegen, dass er mit dem **Befehl** Cisco **crypto isakmp key *address* address *address***



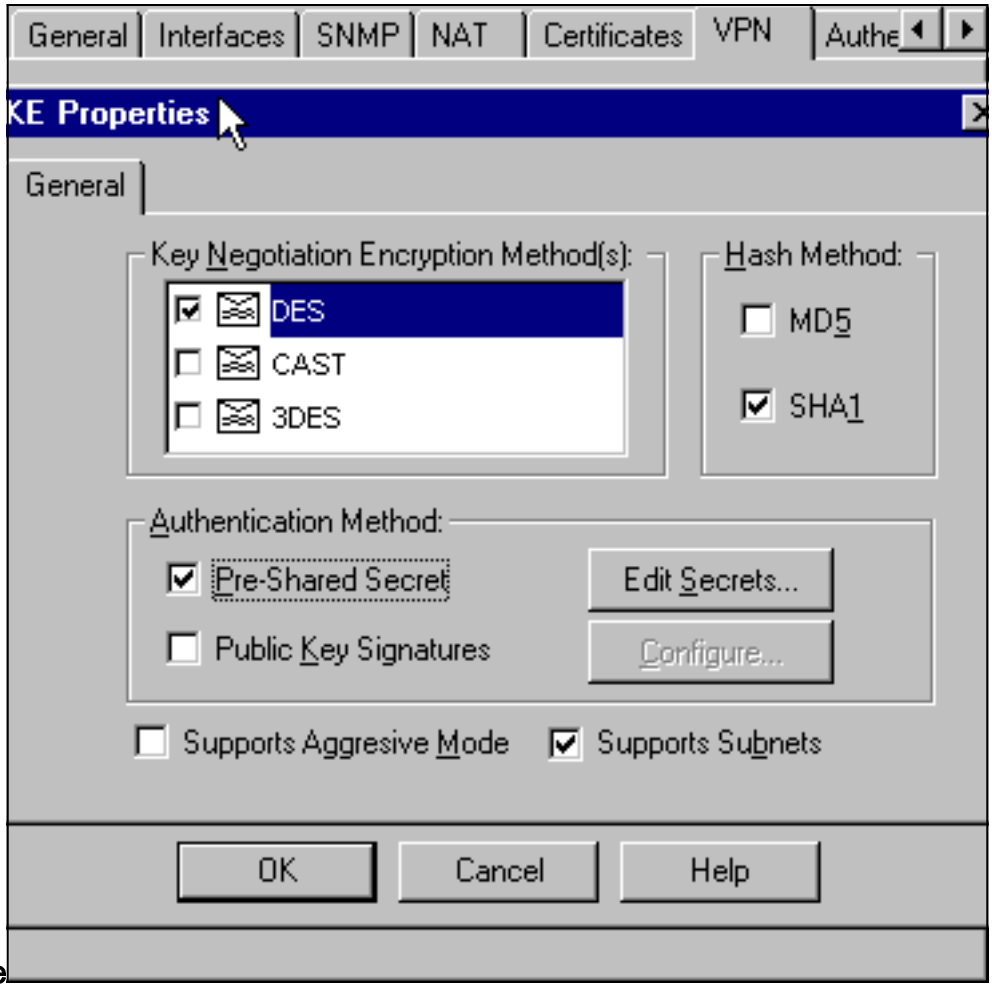
übereinstimmt:

10. Wählen Sie **Verwalten > Netzwerkobjekte > Bearbeiten**, um die Registerkarte "cisco_endpoint" für VPN zu bearbeiten. Wählen Sie unter Domain (Domäne) die Option **Other (Andere)** aus, und wählen Sie dann die interne Schnittstelle des Cisco Netzwerks aus (namens "inside_cisco"). Wählen Sie unter Definierte Verschlüsselungsschemata die Option **IKE aus**, und klicken Sie dann auf



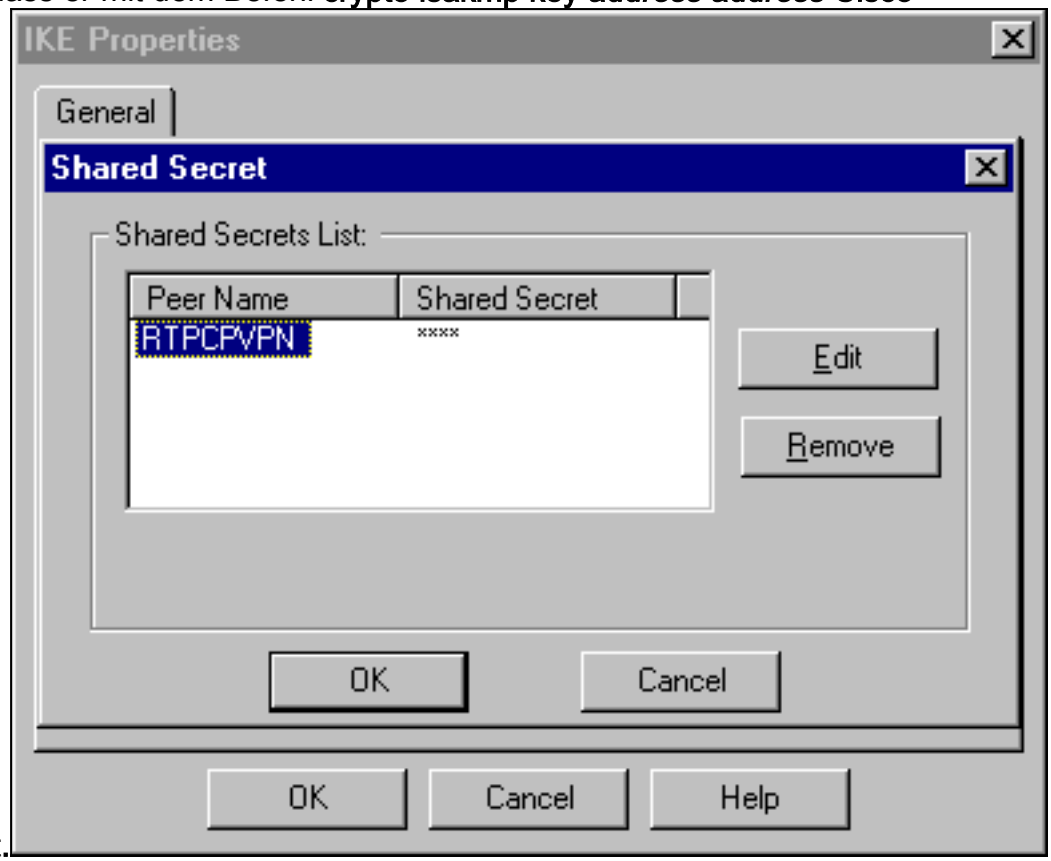
Bearbeiten.

11. Ändern Sie die IKE-Eigenschaften-DES-Verschlüsselung, um mit den folgenden Befehlen zuzustimmen:**crypto isakmp policy #VerschlüsselungHinweis:** Die DES-Verschlüsselung ist die Standardeinstellung, daher ist sie in der Cisco Konfiguration nicht sichtbar.
12. Ändern Sie die IKE-Eigenschaften in SHA1-Hashing, um diesen Befehlen zuzustimmen:**crypto isakmp policy #Hash-ShaHinweis:** Der SHA-Hashing-Algorithmus ist die Standardeinstellung, sodass er in der Cisco Konfiguration nicht angezeigt wird.Ändern Sie diese Einstellungen:Deaktivieren Sie die **Option Aggressiver Modus**.Aktivieren Sie **Subnetze unterstützen**.Aktivieren Sie **Pre-Shared Secret** unter Authentication Method. Dies entspricht den folgenden Befehlen:**crypto isakmp policy #Authentifizierung Pre-**



Share

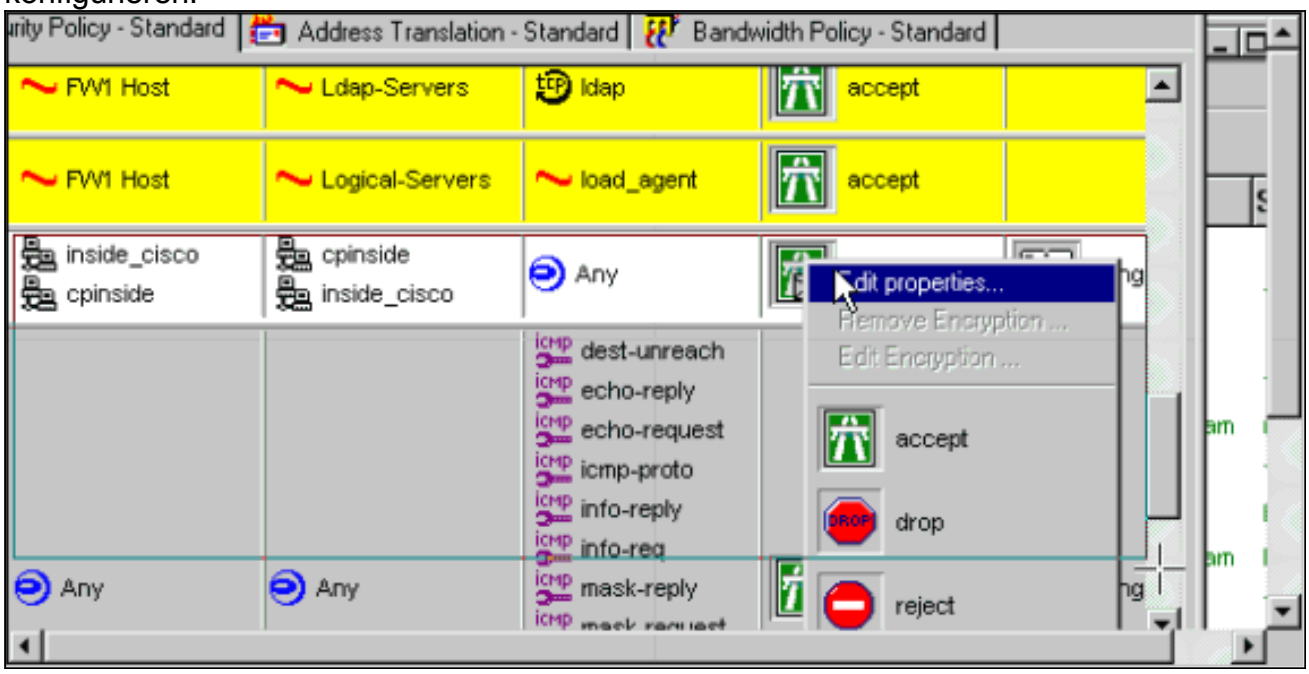
13. Klicken Sie auf **Edit Secrets** (Geheimnisse **bearbeiten)**, um den vorinstallierten Schlüssel so einzustellen, dass er mit dem Befehl **crypto isakmp key** ***address address*** **Cisco**



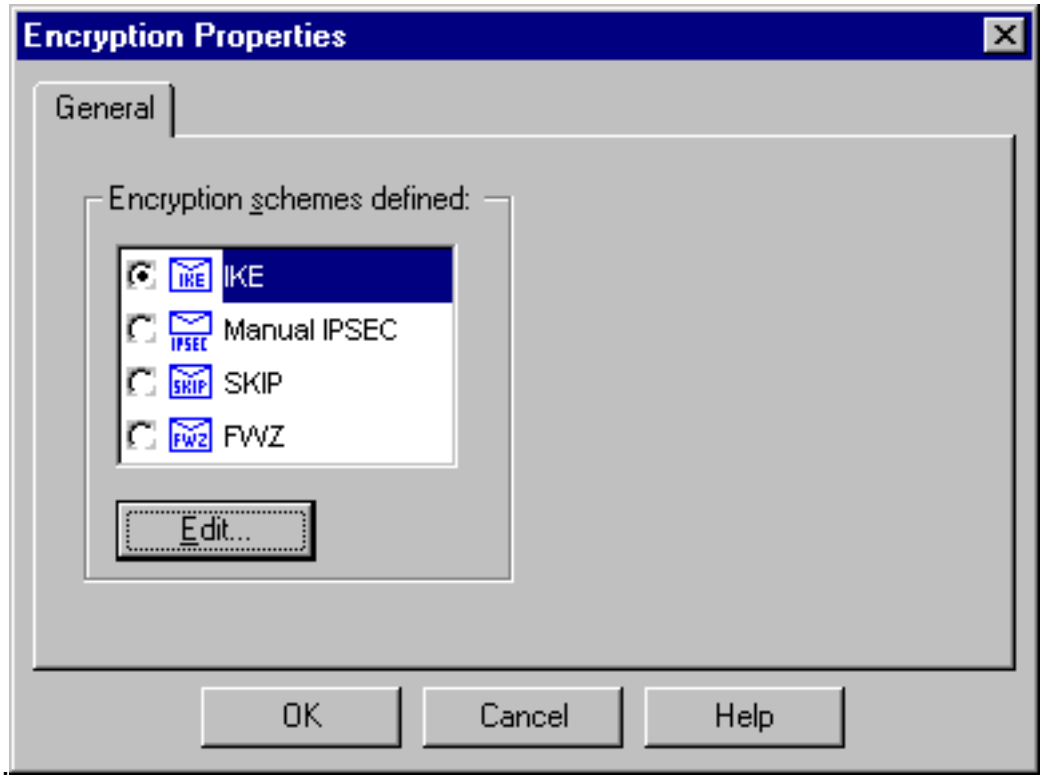
übereinstimmt.

14. Fügen Sie im Fenster des Richtlinien-Editors eine Regel mit Quelle und Ziel als "inside_cisco" und als "cpinside" (bidirektional) ein. Set **Service=Any**, **Action=Encrypt** und **Track=Long**.

15. Klicken Sie auf das grüne Symbol **Verschlüsseln**, und wählen Sie **Eigenschaften bearbeiten aus**, um Verschlüsselungsrichtlinien unter der Überschrift Aktion zu konfigurieren.

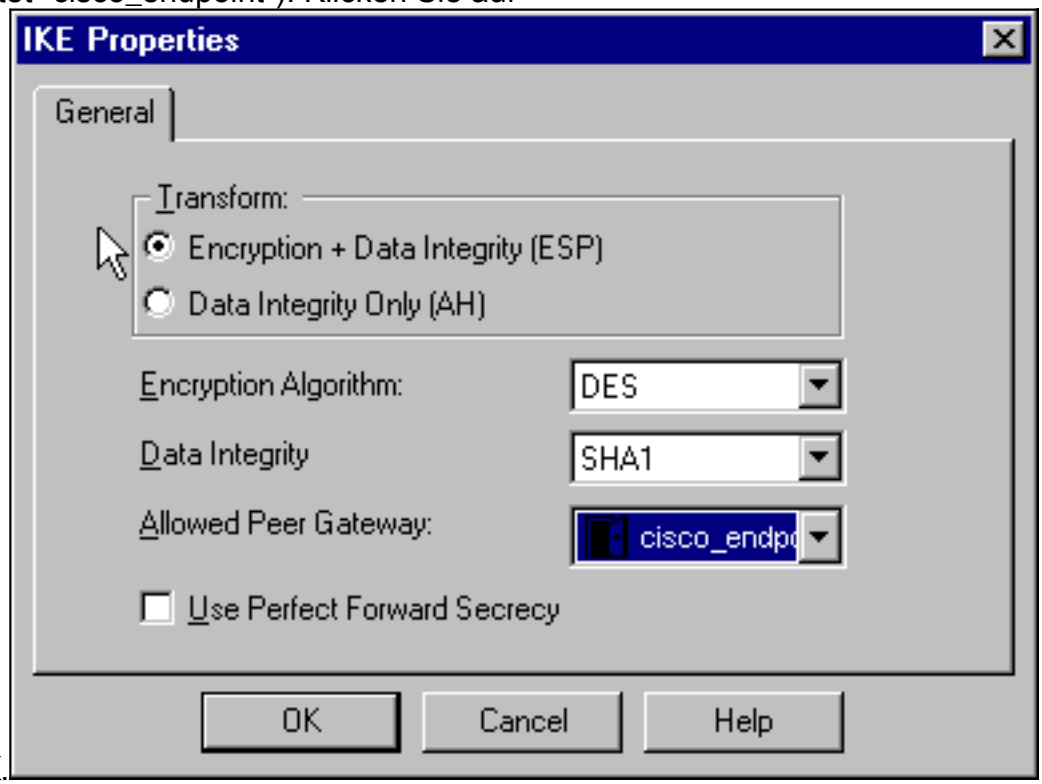


16. Wählen Sie **IKE aus**, und klicken Sie dann auf



Bearbeiten.

17. Ändern Sie im Fenster IKE-Eigenschaften diese Eigenschaften so, dass sie mit den Cisco IPsec-Transformationen im Befehl **crypto ipsec-transformation rtpset esp-des esp-sha-hmac** übereinstimmen:Wählen Sie unter Transform (Transform) **Encryption + Data Integrity (ESP)** aus. Der Verschlüsselungsalgorithmus muss **DES** sein, die Datenintegrität muss **SHA1** sein, und das zulässige Peer-Gateway muss das externe Router-Gateway sein (der Name lautet "cisco_endpoint"). Klicken Sie auf



OK.

18. Nachdem Sie den Checkpoint konfiguriert haben, wählen Sie im Checkpoint-Menü **Richtlinien > Installieren**, damit die Änderungen wirksam werden.

Überprüfen

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

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

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

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **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.

Netzwerkzusammenfassung

Wenn mehrere benachbarte Netzwerke in der Verschlüsselungsdomäne am Checkpoint konfiguriert sind, kann das Gerät diese automatisch in Bezug auf interessanten Datenverkehr zusammenfassen. Wenn der Router nicht so konfiguriert ist, dass er übereinstimmt, schlägt der Tunnel wahrscheinlich fehl. Wenn beispielsweise die internen Netzwerke 10.0.0.0 /24 und 10.0.1.0 /24 so konfiguriert sind, dass sie in den Tunnel eingeschlossen werden, können sie in 10.0.0.0 /23 zusammengefasst werden.

Prüfpunkt

Da die Nachverfolgung im Fenster des Policy Editor auf Long (Lang) festgelegt wurde, sollte der abgelehnte Datenverkehr in der Protokollanzeige rot angezeigt werden. Ausführlichere Debugging-Informationen finden Sie unter:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

und in einem anderen Fenster:

```
C:\WINNT\FW1\4.1\fwstart
```

Hinweis: Dies war eine Microsoft Windows NT-Installation.

Führen Sie diese Befehle aus, um SAs am Prüfpunkt zu löschen:

```
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
```

Beantworten Sie im Fenster "Sind Sie sicher?" mit Ja. eingeben.

Beispielausgabe für Debugging

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
cisco_endpoint#
20:54:06: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP:      encryption DES-CBC
20:54:06: ISAKMP:      hash SHA
20:54:06: ISAKMP:      default group 1
20:54:06: ISAKMP:      auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
   using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
20:54:06: ISAKMP (1): Total payload length: 12
```

```
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPSec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP:   attributes in transform:
20:54:06: ISAKMP:      encaps is 1
20:54:06: ISAKMP:      SA life type in seconds
20:54:06: ISAKMP:      SA life duration (basic) of 3600
20:54:06: ISAKMP:      SA life type in kilobytes
20:54:06: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
20:54:06: ISAKMP:      authenticator is HMAC-SHA
20:54:06: validate proposal 0
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
20:54:06: ISAKMP (0:1): Creating IPSec SAs
20:54:06:         inbound SA from 172.18.124.157 to 172.18.124.35
        (proxy 10.32.50.0 to 192.168.1.0)
20:54:06:         has spi 0xA29984CA and conn_id 2000 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06:         outbound SA from 172.18.124.35   to 172.18.124.157
   (proxy 192.168.1.0 to 10.32.50.0)
20:54:06:         has spi 404516441 and conn_id 2001 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
```

```
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.35, sa_prot= 50,
    sa_spi= 0xA29984CA(2727969994),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.157, sa_prot= 50,
    sa_spi= 0x181C6E59(404516441),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa

interface: Ethernet0/0
    Crypto map tag: rtp, local addr. 172.18.124.35

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0

     local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
     path mtu 1500, media mtu 1500
     current outbound spi: 181C6E59

     inbound esp sas:
      spi: 0xA29984CA(2727969994)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
 --More--                 sa timing: remaining key lifetime (k/sec):
    (4607998/3447)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x181C6E59(404516441)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4607997/3447)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:


cisco_endpoint#show crypto isakmp sa
    dst           src          state        conn-id   slot
172.18.124.157 172.18.124.35  QM_IDLE           1       0

cisco_endpoint#exit
```

Zugehörige Informationen

- IPsec-Aushandlung/IKE-Protokolle
- Konfigurieren der IPsec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Technischer Support und Dokumentation - Cisco Systems