Konfigurieren eines IPSec-Tunnels - Cisco Secure PIX Firewall zur Checkpoint 4.1-Firewall

Inhalt

Einführung

Diese Beispielkonfiguration veranschaulicht die Erstellung eines IPSec-Tunnels mit vorinstallierten Schlüsseln zum Verbinden von zwei privaten Netzwerken. In unserem Beispiel handelt es sich bei den verbundenen Netzwerken um das private Netzwerk 192.168.1.X innerhalb der Cisco Secure Pix Firewall (PIX) und das private Netzwerk 10.32.50.X im Checkpoint. Es wird davon ausgegangen, dass vor Beginn dieser Konfiguration der Datenverkehr aus dem PIX und innerhalb der Checkpoint 4.1-Firewall zum Internet (dargestellt durch die Netzwerke 172.18.124.X) fließt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- PIX Softwareversion 5.3.1
- Checkpoint 4.1-Firewall

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 in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

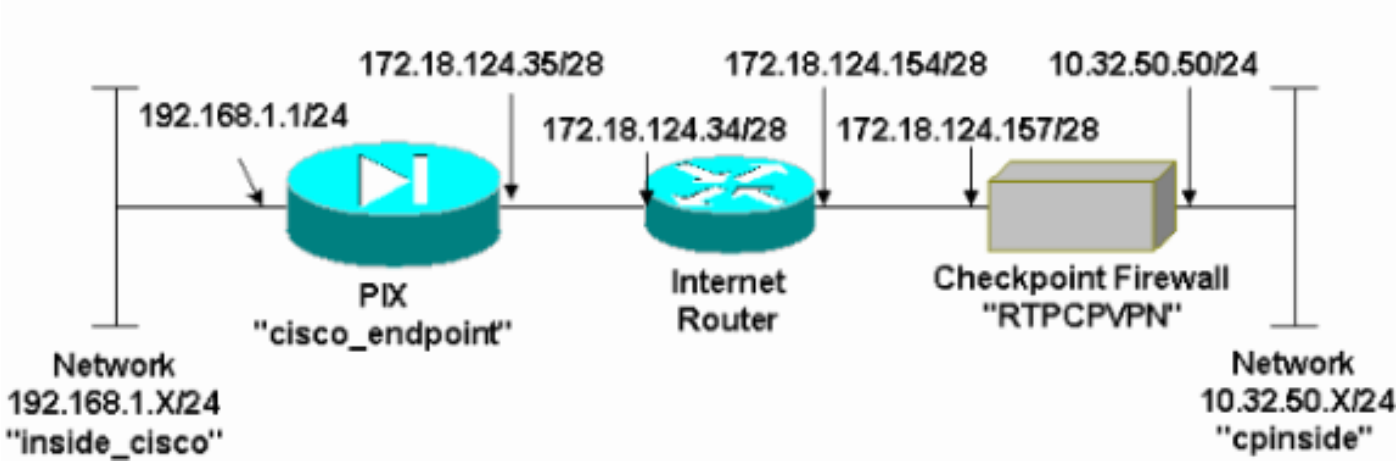
Konfigurieren

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

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

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden die in diesem Abschnitt beschriebenen Konfigurationen verwendet.

PIX-Konfiguration

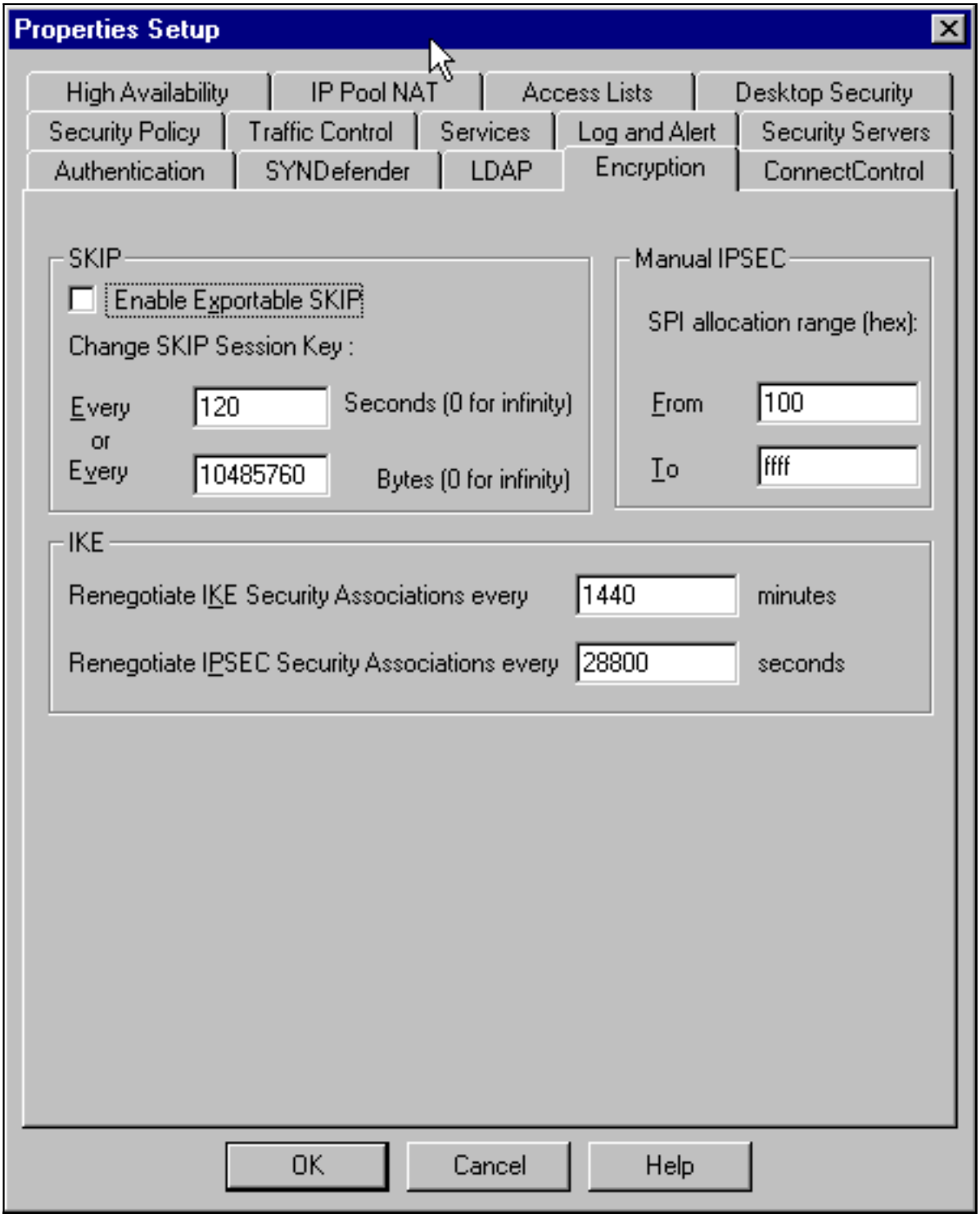
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
```

```
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
10.32.50.0 255.255.255.0
access-list 115 deny ip 192.168.1.0 255.255.255.0 any
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
logging monitor debugging
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.35 255.255.255.240
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.36
nat (inside) 0 access-list 115
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.34 1
timeout xlate 3:00:00g SA 0x80bd6a10, conn_id = 0
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- IPSec configuration sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp
crypto map rtpmap 10 match address 115
crypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap 10 set security-association lifetime
seconds
3600 kilobytes 4608000
crypto map rtpmap interface outside
!--- IKE configuration isakmp enable outside
isakmp key ******** address 172.18.124.157 netmask
255.255.255.240
```

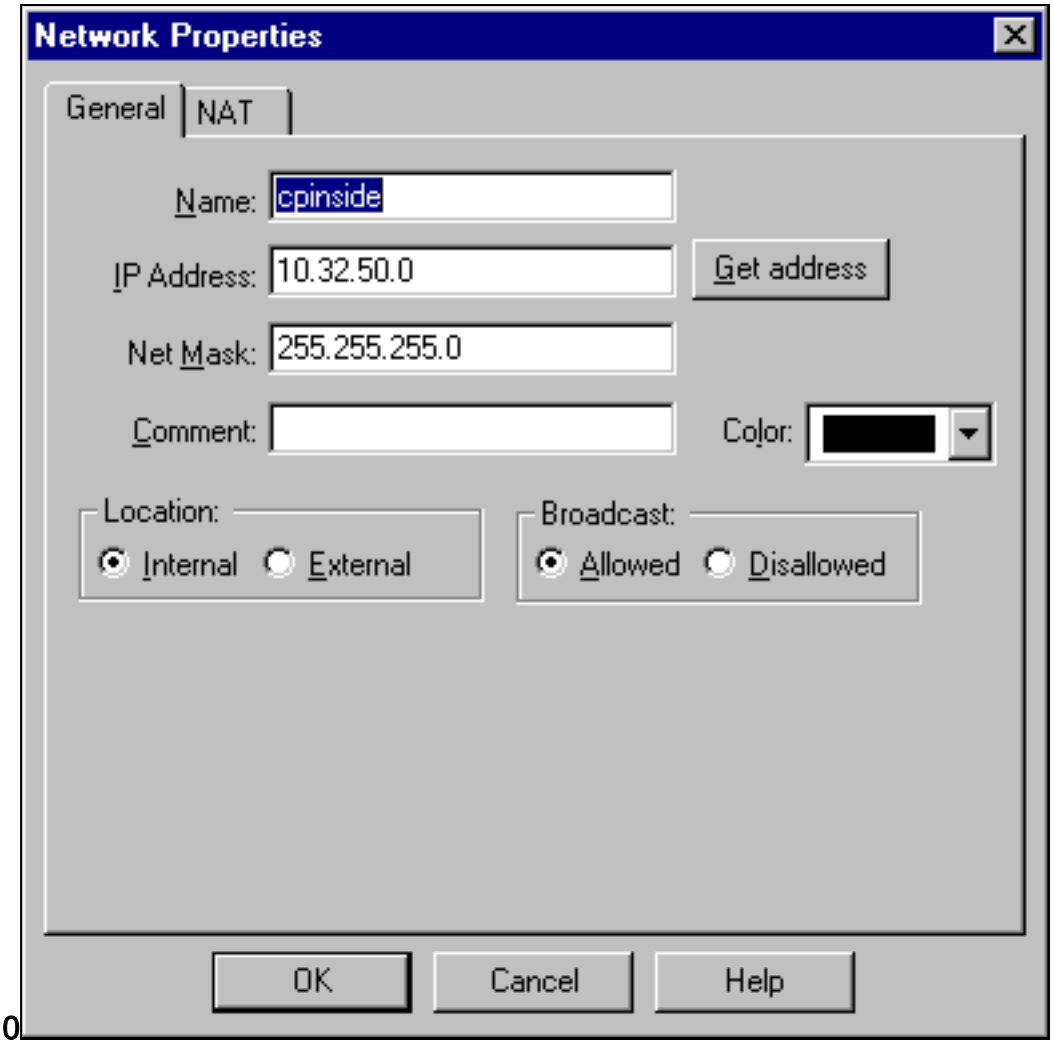
```
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

Checkpoint-Firewall

1. Da sich die IKE- und IPSec-Standardlebensdauer von Anbieter unterscheiden, wählen Sie **Eigenschaften > Verschlüsselung**, um die Prüfpunktlebensdauer so einzustellen, dass sie den PIX-Standardeinstellungen entspricht.Die IKE-Standardlebensdauer für PIX beträgt 86400 Sekunden (= 1440 Minuten), die mit dem folgenden Befehl geändert werden kann: **isakmp-Richtlinie Nr. lebenslange 86400**Die PIX IKE-Lebensdauer kann zwischen 60 und 86.400 Sekunden konfiguriert werden.Die PIX-Standard-IPSec-Lebensdauer beträgt 28.800 Sekunden, die mit dem folgenden Befehl geändert werden kann: **crypto ipsec-Lebensdauer der Sicherheitszuordnung #**Sie können eine PIX IPSec-Lebensdauer zwischen 120 und 86.400 Sekunden
   konfigurieren.

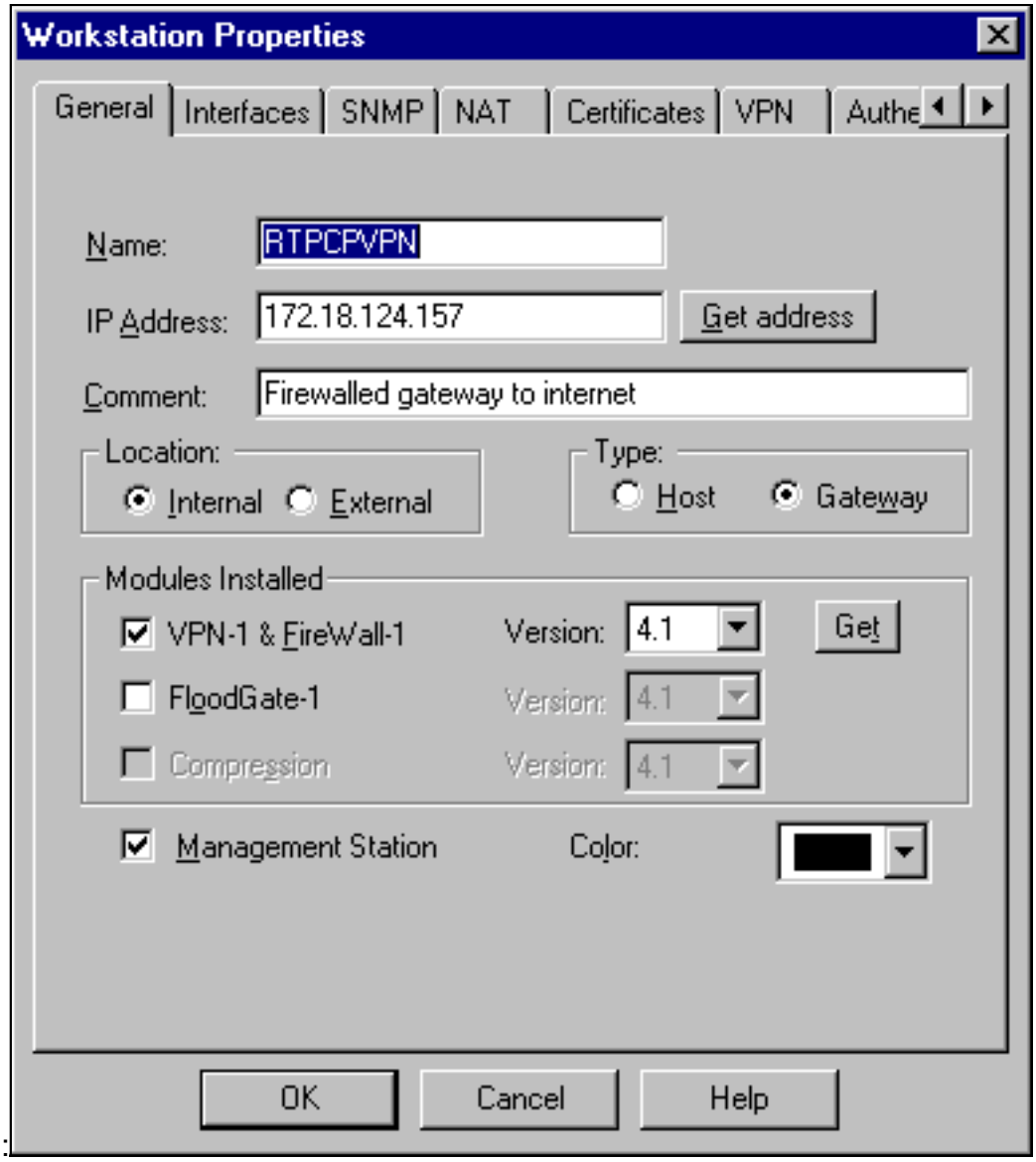


2. Wählen Sie **Verwalten > Netzwerkobjekte > Neu (oder Bearbeiten) > Netzwerk**, um das Objekt für das interne ("cpinside") Netzwerk hinter dem Prüfpunkt zu konfigurieren.Dies muss mit dem (zweiten) Ziel-Netzwerk in diesem PIX-Befehl übereinstimmen: **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**



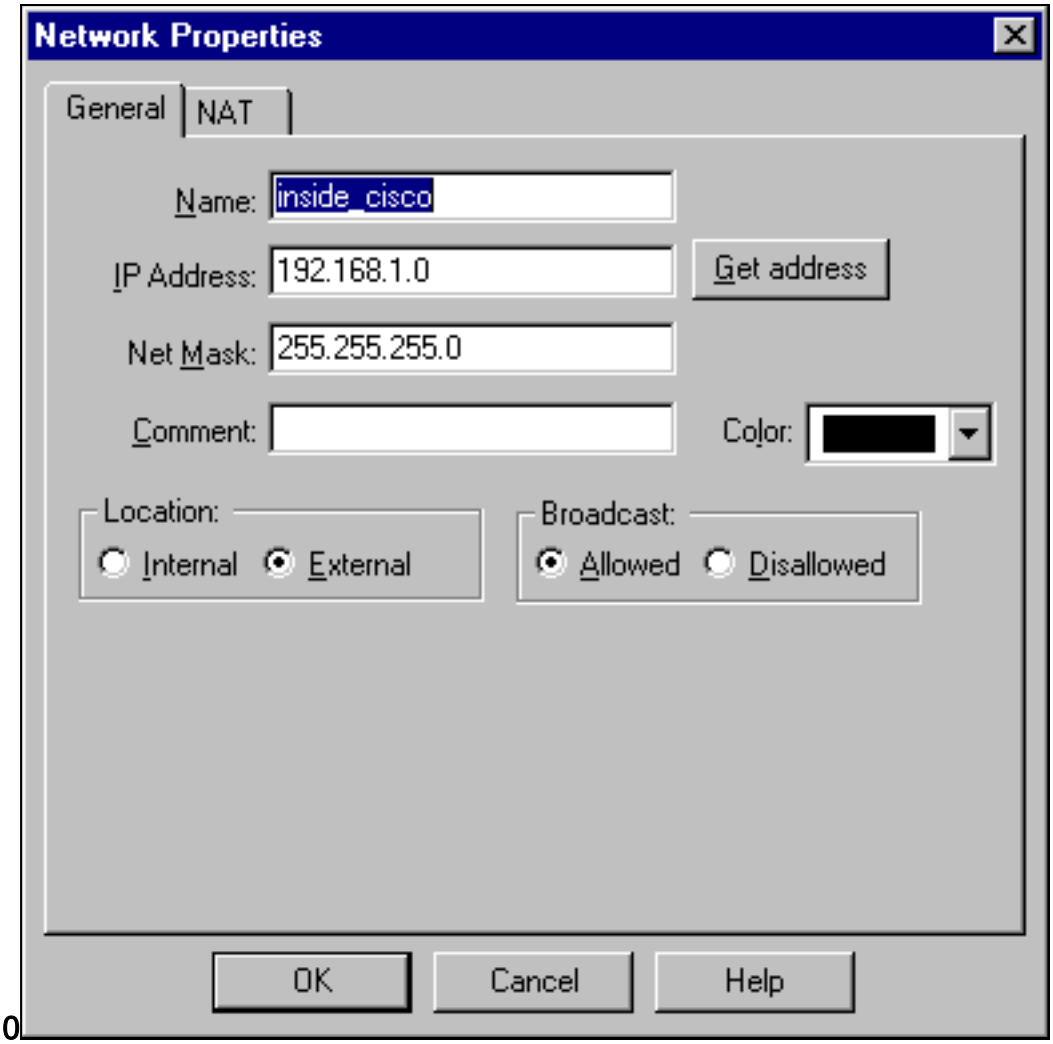
255.255.255.0

3. Wählen Sie **Verwalten > Netzwerkobjekte > Bearbeiten**, um das Objekt für den Gateway-Endpunkt ("RTPCPVPN"-Prüfpunkt) zu bearbeiten, auf den das PIX in diesem Befehl verweist: **crypto map name # set peer ip_address**Wählen Sie unter Speicherort die Option **Intern 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**



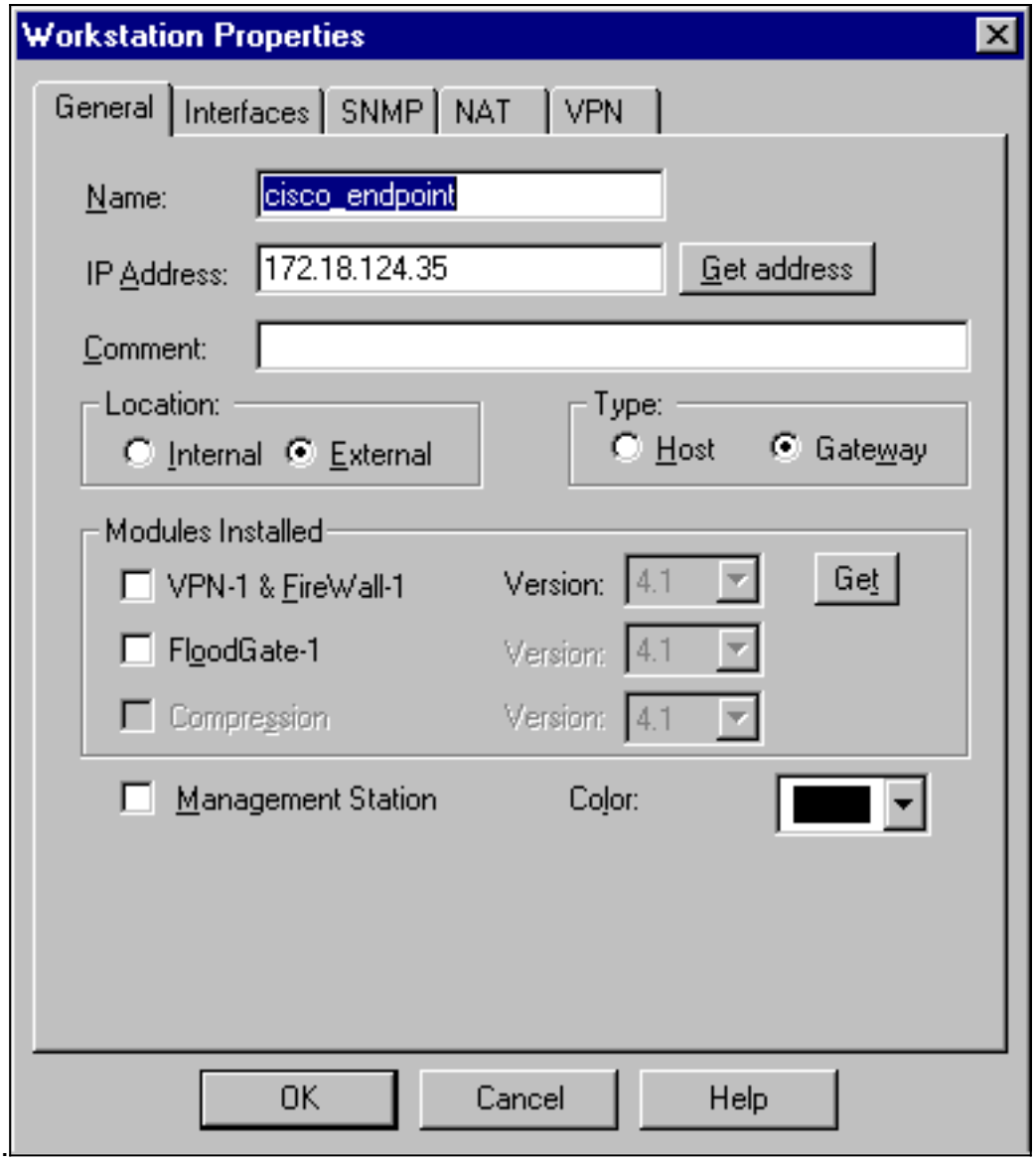
Station:

4. Wählen Sie **Manage > Network objects > New > Network** aus, um das Objekt für das externe ("inside_cisco") Netzwerk hinter dem PIX zu konfigurieren.Dies muss mit dem (ersten) Quell-Netzwerk in diesem PIX-Befehl übereinstimmen: **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**

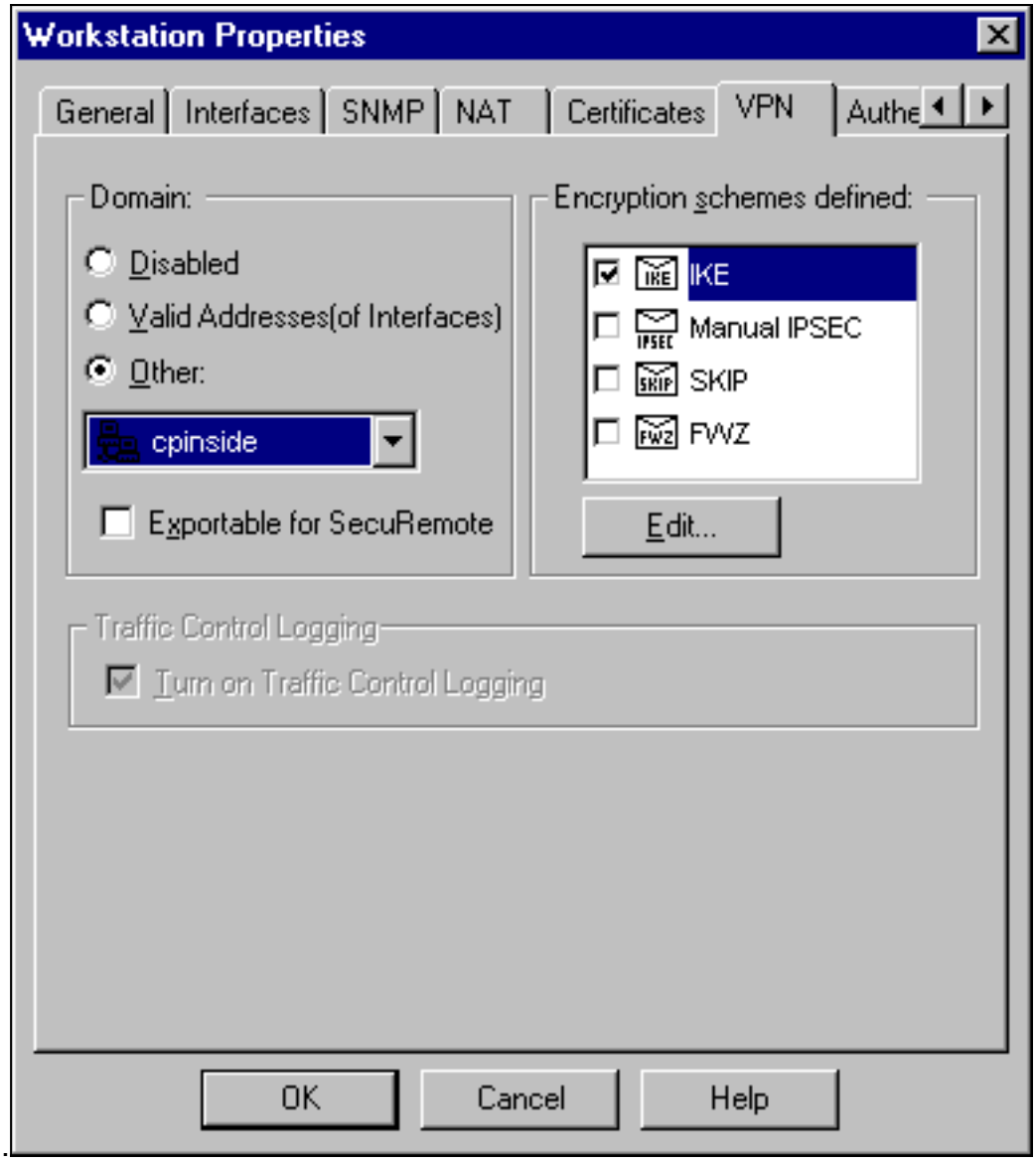


255.255.255.0

5. Wählen Sie **Manage > Network objects > New > Workstation** aus, um ein Objekt für das externe PIX-Gateway ("cisco_endpoint") hinzuzufügen. Dies ist die PIX-Schnittstelle, auf die dieser Befehl angewendet wird: **crypto map *name* interface außerhalb**Wählen Sie unter Speicherort die Option **Extern aus**. Wählen Sie als Typ **Gateway** aus.**Hinweis:** Aktivieren Sie nicht das Kontrollkästchen VPN-1/FireWall-

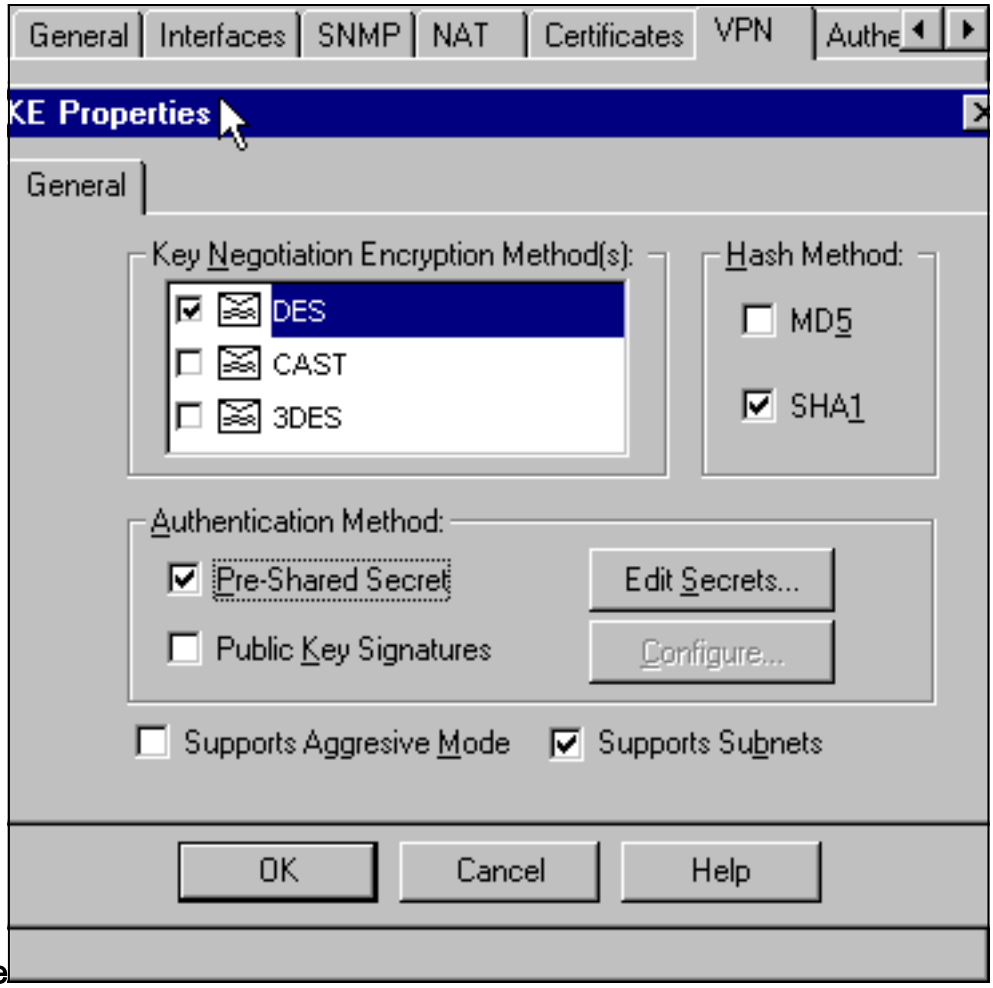
1. 

6. Wählen Sie die Registerkarte **Manage > Network objects > Edit** aus, um den Checkpoint Gateway-Endpunkt (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



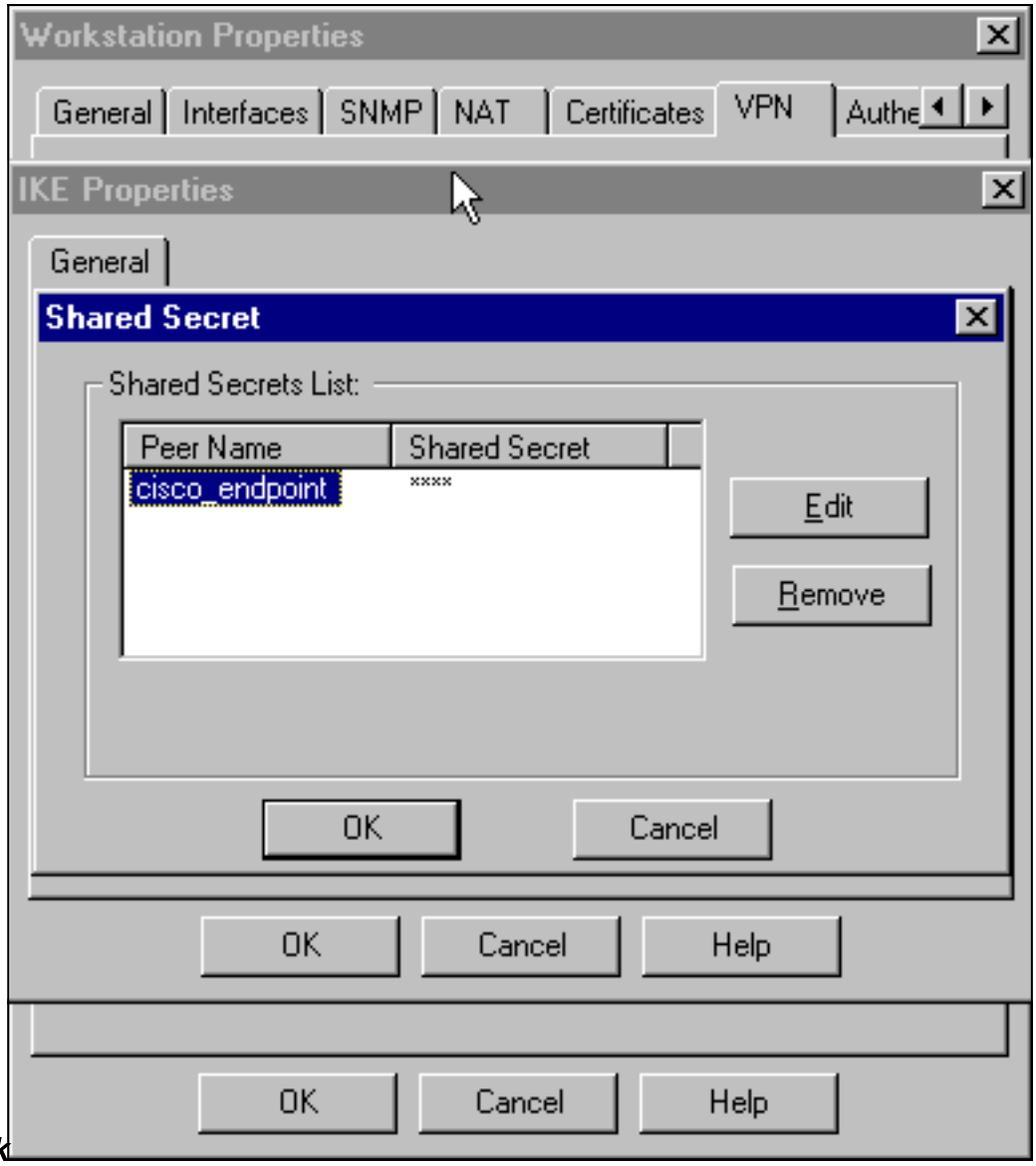
Bearbeiten.

7. Ändern Sie die IKE-Eigenschaften für die DES-Verschlüsselung, um mit dem folgenden Befehl zuzustimmen:**isakmp policy # verschlüsselung des**
8. Ändern Sie die IKE-Eigenschaften in SHA1-Hashing, um diesem Befehl zuzustimmen:**isakmp-Richtlinie # Hash Sha**Ändern Sie diese Einstellungen:Deaktivieren Sie die **Option Aggressiver Modus**.Aktivieren Sie das Kontrollkästchen **Supports Subnets**.Aktivieren Sie unter Authentication Method (Authentifizierungsmethode) das Kontrollkästchen **Pre-Shared Secret (Vorinstallierter geheimer Schlüssel)**. Dies stimmt mit diesem Befehl überein:**isakmp policy # Authentifizierung Pre-**



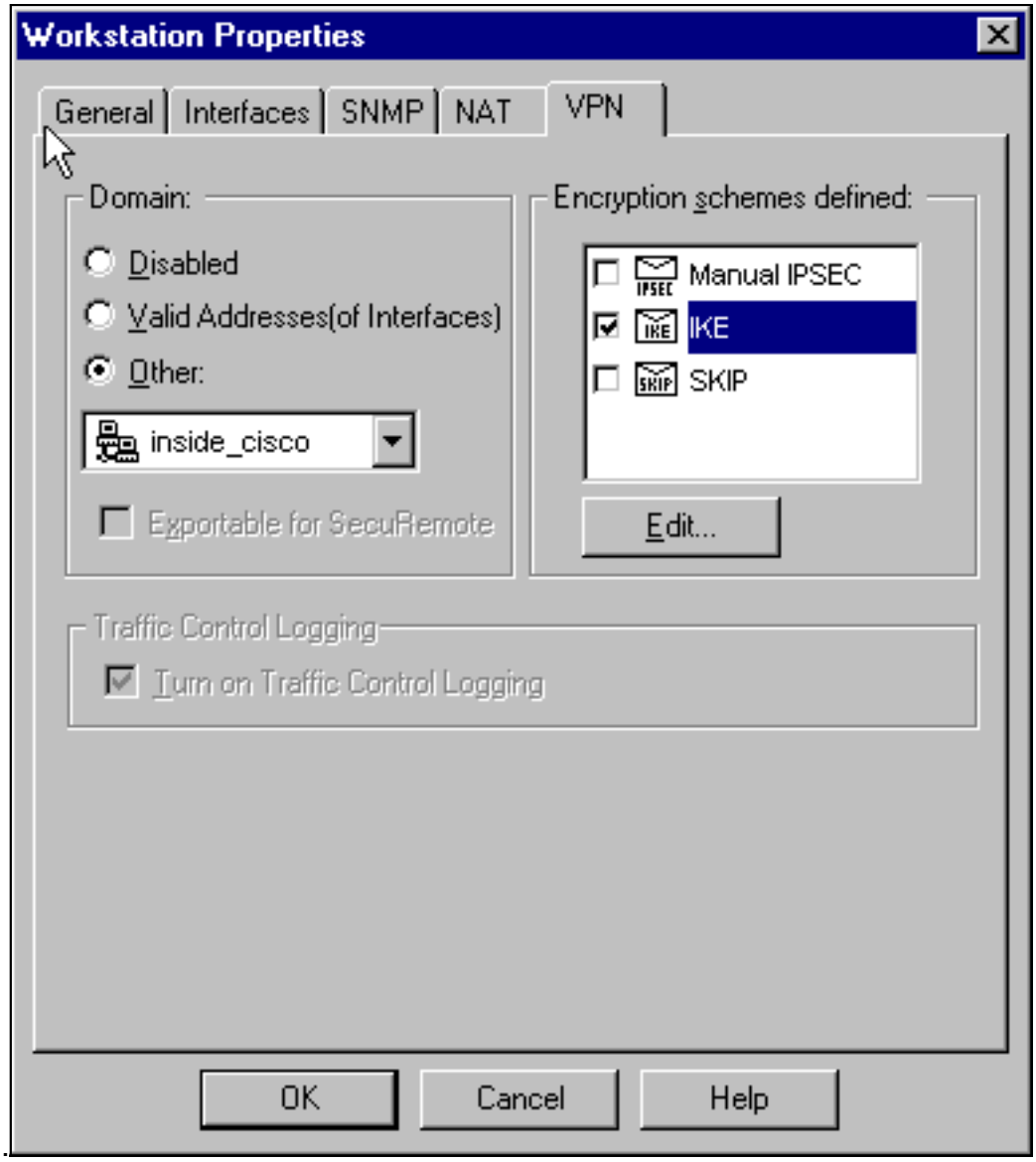
Share

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



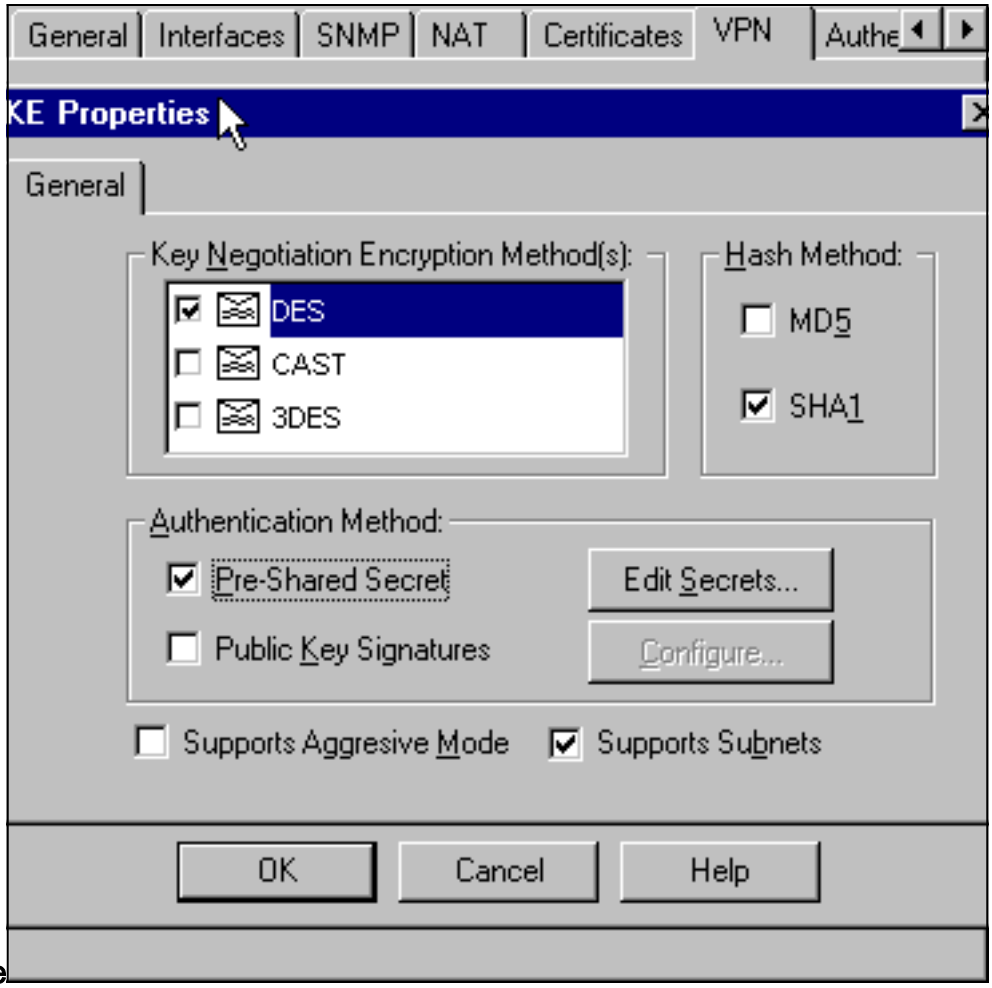
netmask *netmask*

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 PIX-Netzwerks aus (namens "inside_cisco"). Wählen Sie unter Definierte Verschlüsselungsschemata die Option **IKE aus**, und klicken Sie dann auf



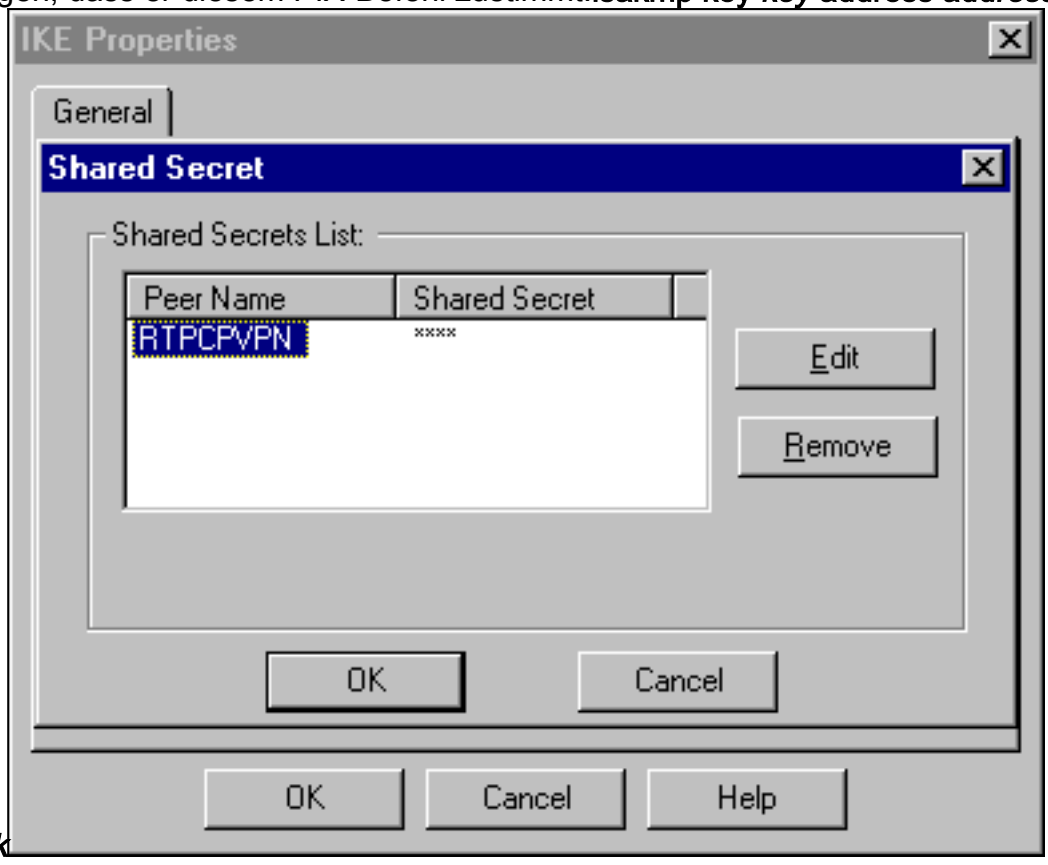
Bearbeiten.

11. Ändern Sie die IKE-Eigenschaften DES-Verschlüsselung, um mit dem folgenden Befehl zuzustimmen:**isakmp policy # verschlüsselung des**
12. Ändern Sie die IKE-Eigenschaften in SHA1-Hashing, um diesem Befehl zuzustimmen:**crypto isakmp policy # Hash shash sha**Ändern Sie diese Einstellungen:Deaktivieren Sie die **Option Aggressiver Modus**.Aktivieren Sie das Kontrollkästchen **Supports Subnets**.Aktivieren Sie unter Authentication Method (Authentifizierungsmethode) das Kontrollkästchen **Pre-Shared Secret** (Vorinstallierter geheimer Schlüssel). Diese Aktion stimmt mit diesem Befehl überein:**isakmp policy # Authentifizierung Pre-**



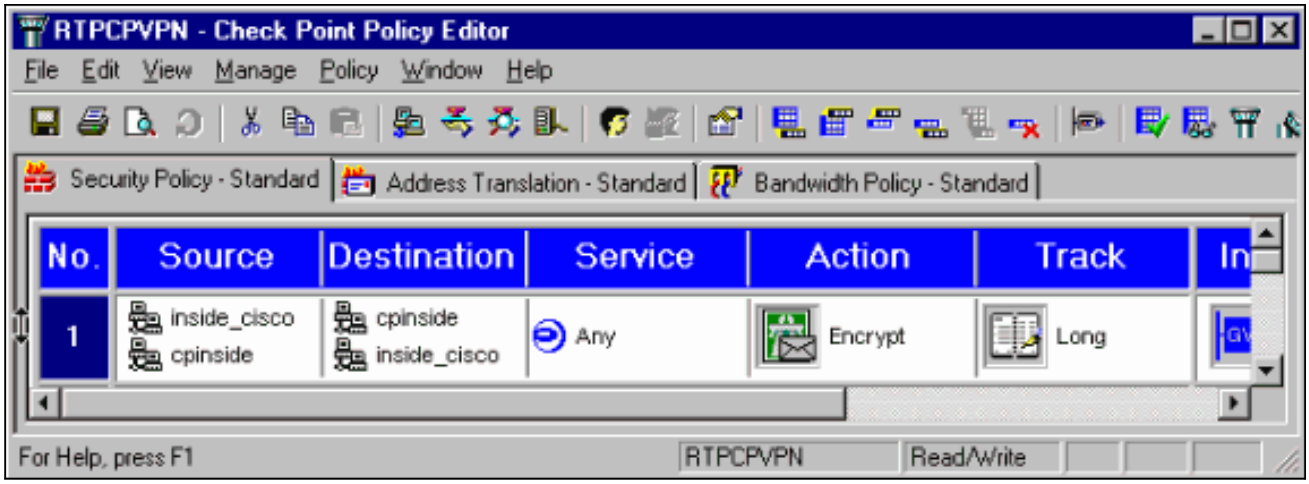
Share

13. Klicken Sie auf **Edit Secrets** (Geheimnisse **bearbeiten**), um den vorinstallierten Schlüssel so festzulegen, dass er diesem PIX-Befehl zustimmt:**isakmp key *key* address *address* netmask**

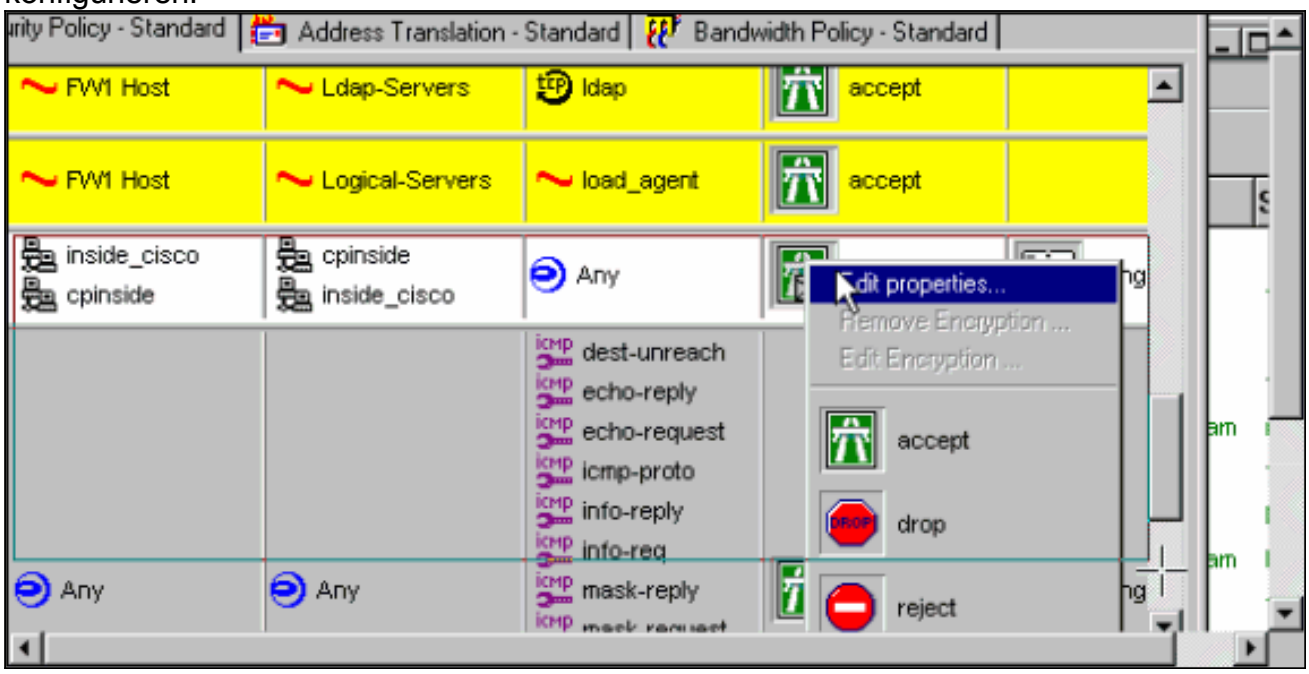


netmask

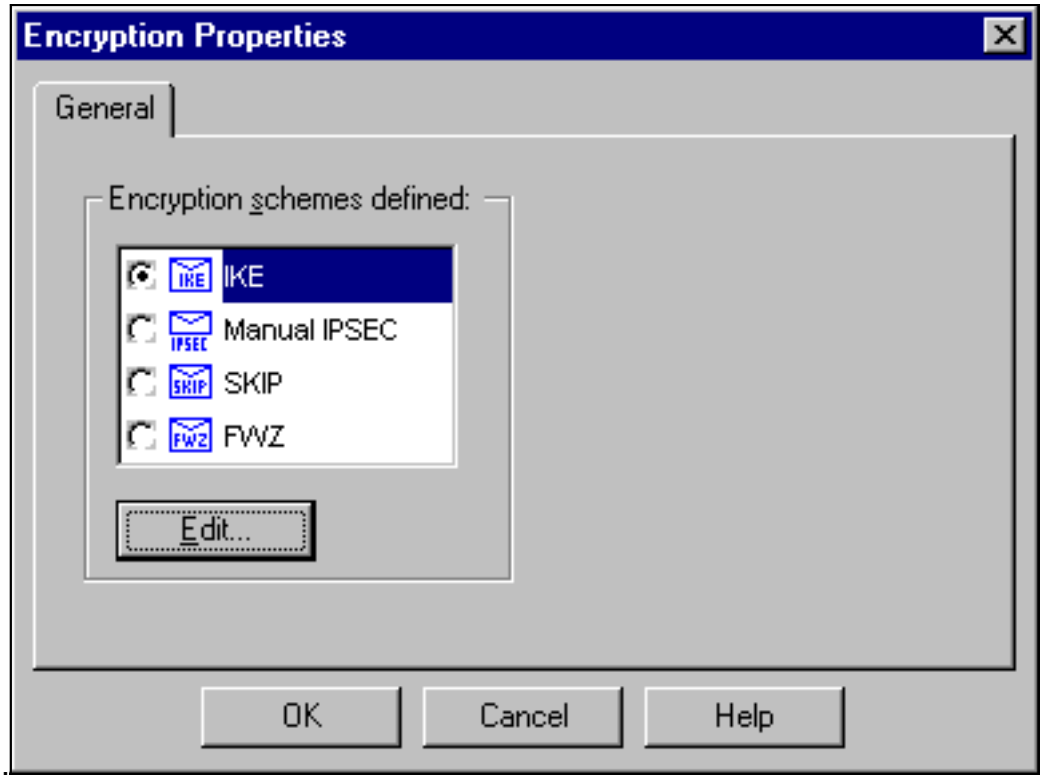
14. Fügen Sie im Fenster des Richtlinien-Editors eine Regel mit Quelle und Ziel als "inside_cisco" und als "cpinside" (bidirektional) ein. Set **Service=Any**, **Action=Encrypt** und **Track=Long**.



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

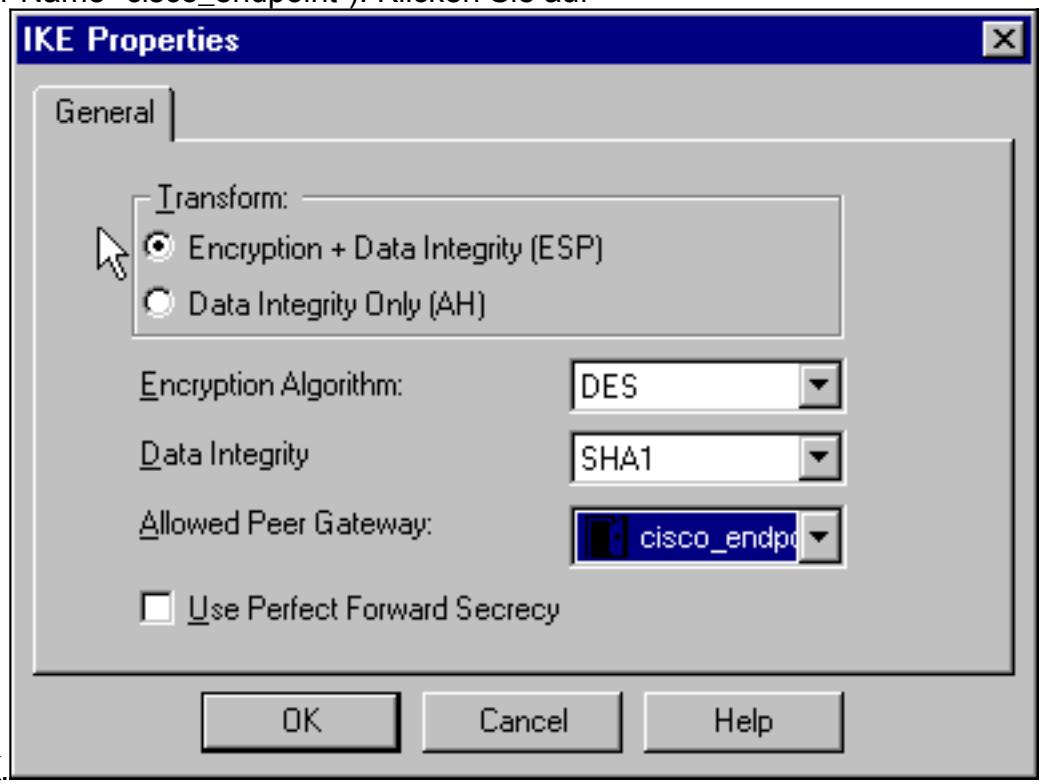


16. Wählen Sie **IKE aus**, und klicken Sie dann auf



Bearbeiten.

17. Ändern Sie im Bildschirm "IKE-Eigenschaften" diese Eigenschaften, um mit den PIX IPSec-Transformationen in diesem Befehl zu übereinstimmen:**crypto ipsec-Transformationssatz myset esp-des esp-sha-hmac**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 PIX-Gateway sein (der Name "cisco_endpoint"). Klicken Sie auf



OK.

18. Nachdem der Prüfpunkt konfiguriert wurde, wählen Sie im Checkpoint-Menü die Option **Policy > Install**, damit die Änderungen wirksam werden.

Befehle debug, anzeigen und löschen

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

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Bevor Sie **Debug-**Befehle ausgeben, lesen Sie die Informationen unter Wichtige Informationen über Debug-Befehle.

Cisco PIX-Firewall

- **debug crypto engine** - Zeigt Debugmeldungen über Krypto Engines an, die Verschlüsselung und Entschlüsselung ausführen.
- **debug crypto isakmp** - Zeigt Meldungen über IKE-Ereignisse an.
- **debug crypto ipsec** - Zeigt IPSec-Ereignisse an.
- **show crypto isakmp sa** - Zeigen Sie alle aktuellen IKE-Sicherheitszuordnungen (SAs) auf einem Peer an.
- **show crypto ipsec sa**: Zeigen Sie die von aktuellen Sicherheitszuordnungen verwendeten Einstellungen an.
- **clear crypto isakmp sa**— (from configuration mode) Clear all active IKE connections.
- **clear crypto ipsec sa**— (aus dem Konfigurationsmodus) Löschen Sie alle IPSec-Sicherheitszuordnungen.

Prüfpunkt:

Da die Nachverfolgung im Fenster des Policy Editor, wie in Schritt 14 gezeigt, für Long (Lang) festgelegt wurde, wird in der Protokollanzeige der Verkehr als "Abgelehnt" angezeigt. Ein ausführlicheres Debuggen kann durch folgende Eingabe abgerufen werden:

```
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.

Sie können SAs am Prüfpunkt mithilfe der folgenden Befehle 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
```

und "**yes**" im Fenster "Are you sure? eingeben.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Netzwerkzusammenfassung

Wenn mehrere benachbarte Netzwerke in der Verschlüsselungsdomäne am Checkpoint konfiguriert werden, kann das Gerät diese automatisch in Bezug auf interessanten Datenverkehr zusammenfassen. Wenn die Krypto-ACL auf dem PIX nicht für eine Übereinstimmung konfiguriert ist, 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 aufgenommen werden, können sie in 10.0.0.0 /23 zusammengefasst werden.

Beispielausgabe für Debugging aus dem PIX

```
cisco_endpoint# show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
        tx      Off
        rx      Off
        open    Off
        cable   Off
        txdmp   Off
        rxdmp   Off
        ifc     Off
        rxip    Off
        txip    Off
        get     Off
        put     Off
        verify  Off
        switch  Off
        fail    Off
        fmsg    Off
cisco_endpoint# term mon
cisco_endpoint#
ISAKMP (0): beginning Quick Mode exchange,
M-ID of 2112882468:7df00724IPSEC(key_engine):
 got a queue event...
IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA
        from  172.18.124.157 to   172.18.124.35 for prot 3
70
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.35
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2112882468

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
```

```
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-SHA
ISAKMP (0): atts are acceptable.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

ISAKMP (0): processing NONCE payload. message ID = 2112882468

ISAKMP (0): processing ID payload. message ID = 2112882468
ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (0): Creating IPSec SAs
        inbound SA from  172.18.124.157 to   172.18.124.35 (proxy
      10.32.50.0 to 192.168.1.0)
        has spi 2641490588 and conn_id 3 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.18.124.35 to  172.18.124.157 (proxy
     192.168.1.0 to 10.32.50.0)
        has spi 3955804195 and conn_id 4 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
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= 28800s and 4608000kb,
    spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
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= 28800s and 4608000kb,
    spi= 0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR2303: 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= 28800s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0,
flags= 0x4004

602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi=
0x9d71f29c(2641490588),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3

602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi=
0xebc8c823(3955804195),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4

cisco_endpoint# sho cry ips sa

interface: outside
```

```
 Crypto map tag: rtpmap, 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): (0.0.0.0/0.0.0.0/0/0)
current_peer: 172.18.124.157
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
 #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.: 172.18.124.35,
  remote crypto endpt.: 172.18.124.157
  path mtu 1500, ipsec overhead 0, media mtu 1500
  current outbound spi: 0

  inbound esp sas:

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:

  outbound ah sas:

  outbound pcp sas:

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: 4, #pkts encrypt: 4, #pkts digest 4
 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
 #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, ipsec overhead 56, media mtu 1500
  current outbound spi: ebc8c823

  inbound esp sas:
   spi: 0x9d71f29c(2641490588)
     transform: esp-des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 3, crypto map: rtpmap
     sa timing: remaining key lifetime (k/sec): (4607999/28777)
     IV size: 8 bytes
     replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0xebc8c823(3955804195)
     transform: esp-des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 4, crypto map: rtpmap
     sa timing: remaining key lifetime (k/sec): (4607999/28777)
     IV size: 8 bytes
     replay detection support: Y
```

```
     outbound ah sas:

     outbound pcp sas:

cisco_endpoint# sho cry is sa
        dst             src          state     pending    created
  172.18.124.157   172.18.124.35    QM_IDLE         0            2
```

Zugehörige Informationen

- PIX-Support-Seite
- PIX-Befehlsreferenz
- Anforderungen für Kommentare (RFCs)
- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- PIX 5.2: Konfigurieren von IPSec
- PIX 5.3: Konfigurieren von IPSec
- IPSec-Support-Seite
- Technischer Support - Cisco Systems