Konfigurieren eines IPsec-Tunnels - Cisco VPN 5000 Concentrator für Checkpoint 4.1-Firewall

Inhalt

Einführung

In diesem Dokument wird veranschaulicht, wie ein IPsec-Tunnel mit vorinstallierten Schlüsseln aufgebaut wird, um zwei private Netzwerke miteinander zu verbinden. Sie verbindet ein privates Netzwerk im Cisco VPN 500 Concentrator (192.168.1.x) mit einem privaten Netzwerk innerhalb der Checkpoint 4.1-Firewall (10.32.50.x). Es wird davon ausgegangen, dass der Datenverkehr aus dem Inneren des VPN-Konzentrators und innerhalb des Prüfpunkts zum Internet (dargestellt in diesem Dokument durch die Netzwerke 172.18.124.x) fließt, bevor Sie mit dieser Konfiguration beginnen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

Hardwareversionen:

- Cisco VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator Software Version 5.2.19.0001
- 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 unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

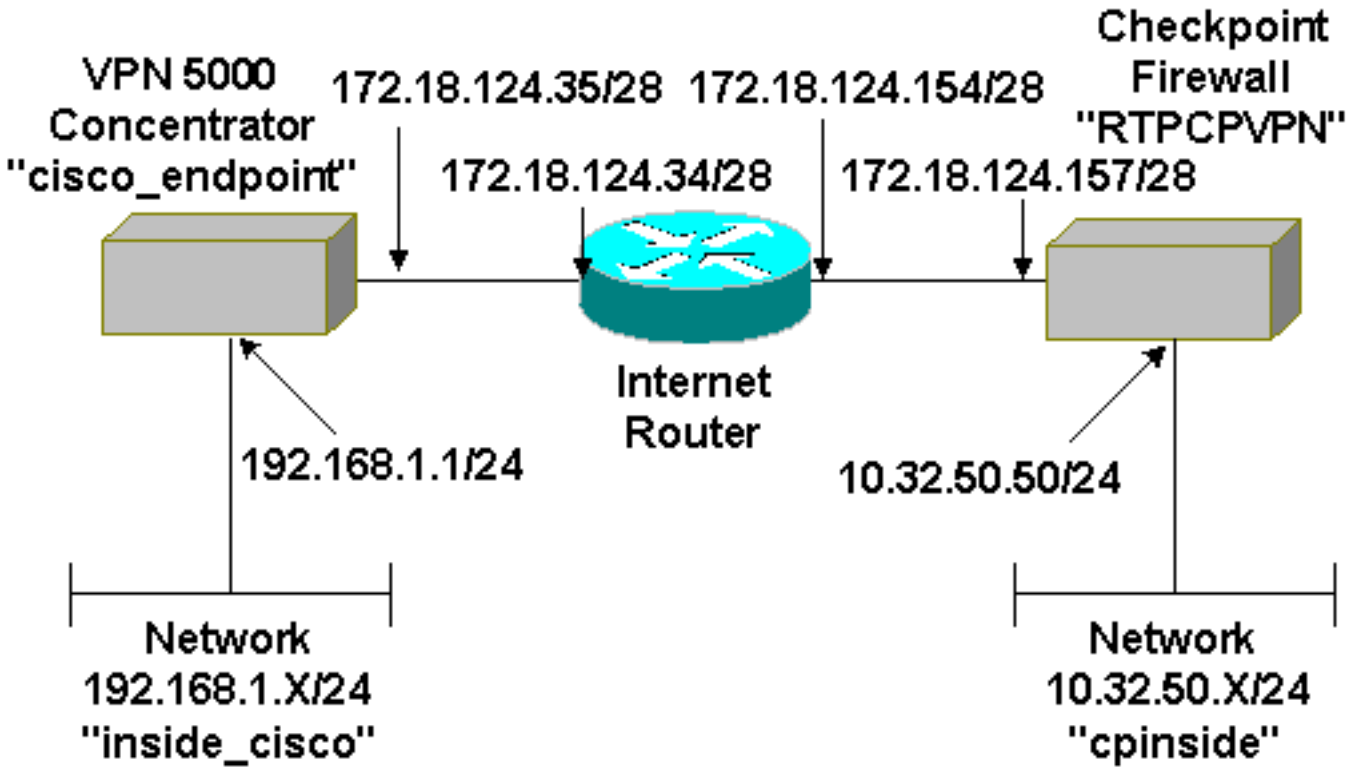
Konfigurieren

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 wird diese Konfiguration verwendet.

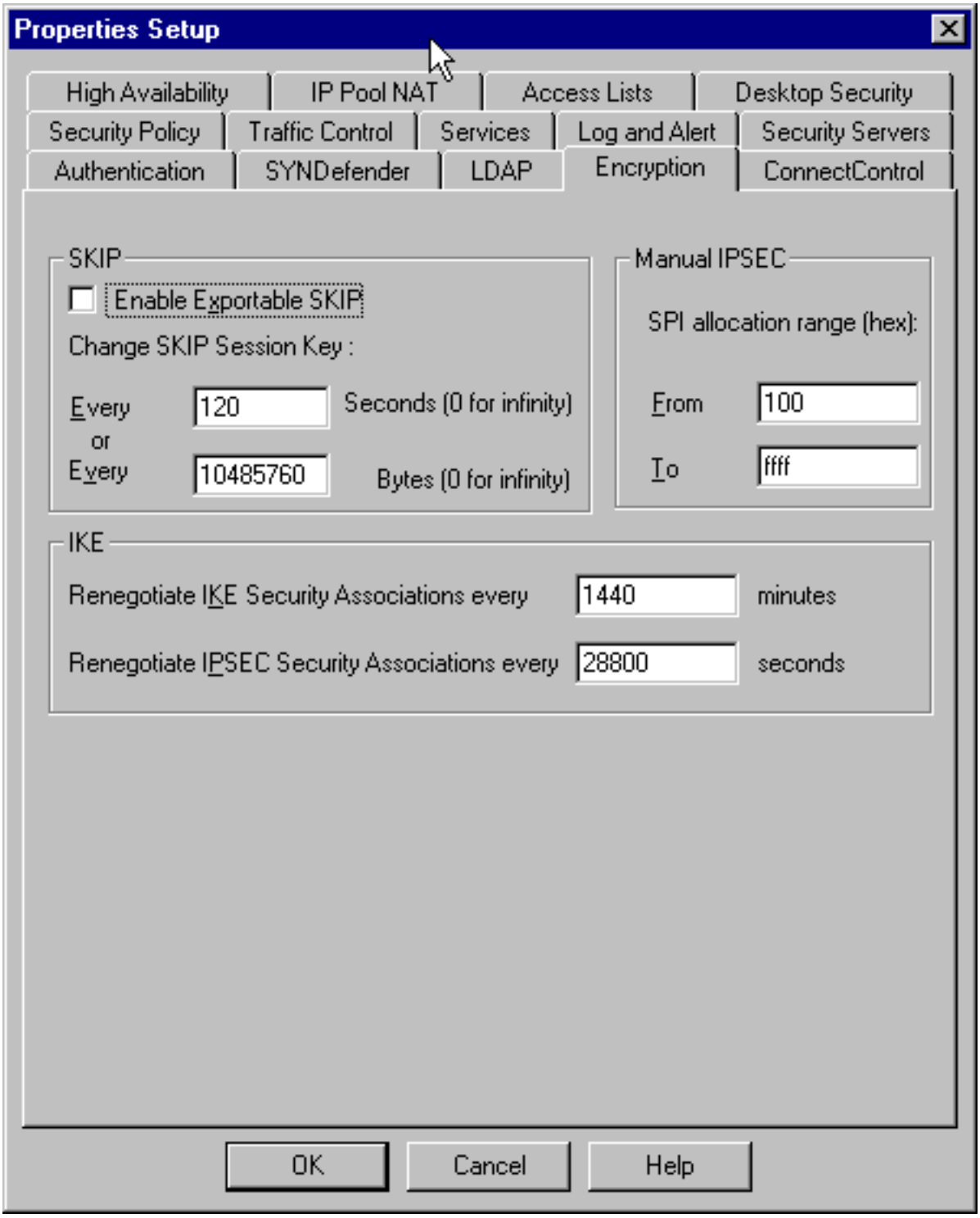
Cisco VPN 5000 Concentrator

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1

[ General ]
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console
DeviceName              = "cisco_endpoint"
IPSecGateway            = 172.18.124.34

[ IKE Policy ]
Protection              = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 28800
LocalAccess             = "192.168.1.0/24"
Peer                    = "10.32.50.0/24"
BindTo                  = "ethernet 1:0"
SharedKey               = "ciscorules"
KeyManage               = Auto
Transform               = esp(sha,des)
Partner                 = 172.18.124.157
Mode                    = Main

[ IP VPN 1 ]
Numbered                = Off
Mode                    = Routed

[ IP Ethernet 1:0 ]
IPAddress               = 172.18.124.35
SubnetMask              = 255.255.255.240
Mode                    = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

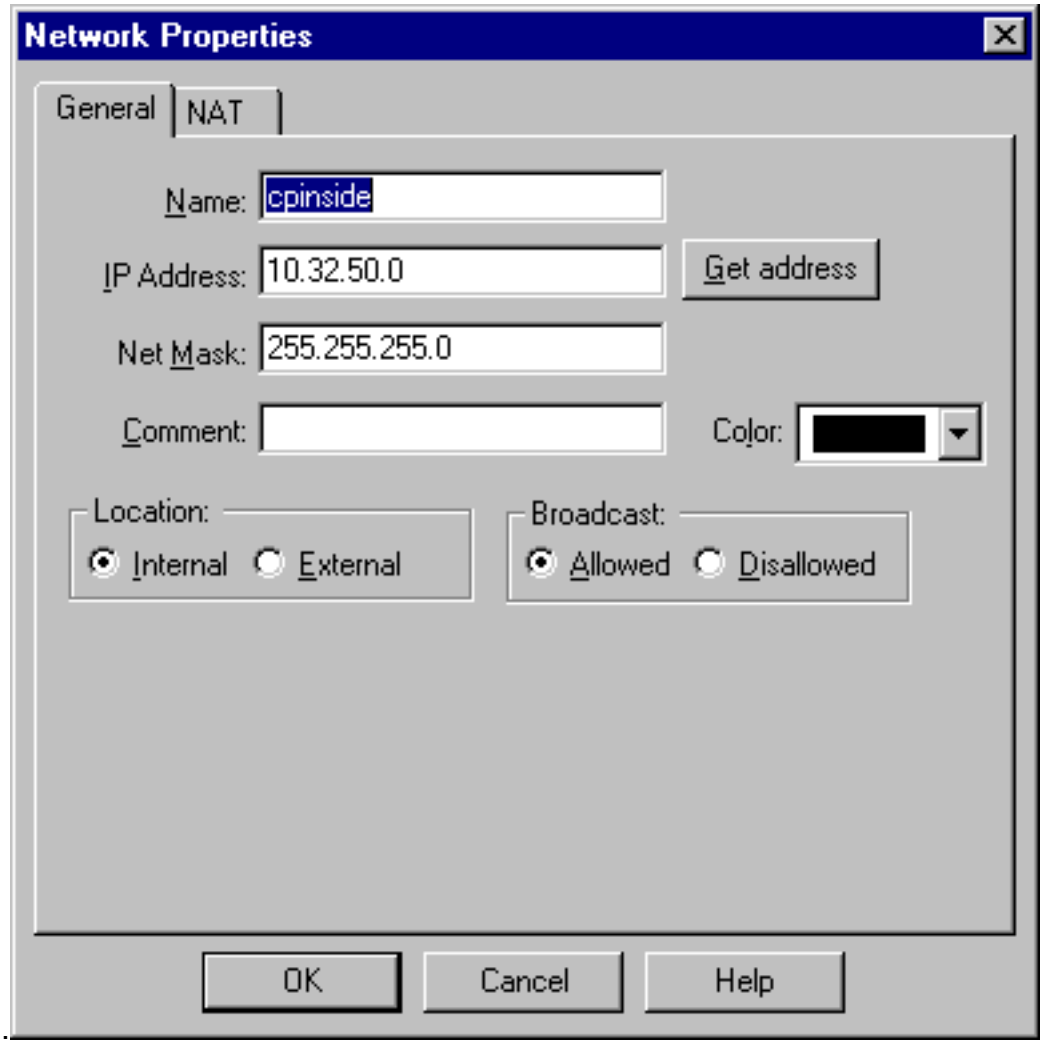
Checkpoint 4.1-Firewall

Führen Sie diese Schritte aus, um die Checkpoint 4.1-Firewall zu konfigurieren.

1. Wählen Sie **Eigenschaften > Verschlüsselung** aus, um die IPsec-Lebensdauer des Prüfpunkts so festzulegen, dass sie mit dem Befehl **KeyLifeSecs = 28800** VPN Concentrator übereinstimmt.**Hinweis:** Lassen Sie die Nutzungsdauer des Internet Key Exchange (IKE) des Prüfpunkts standardmäßig
unverändert.

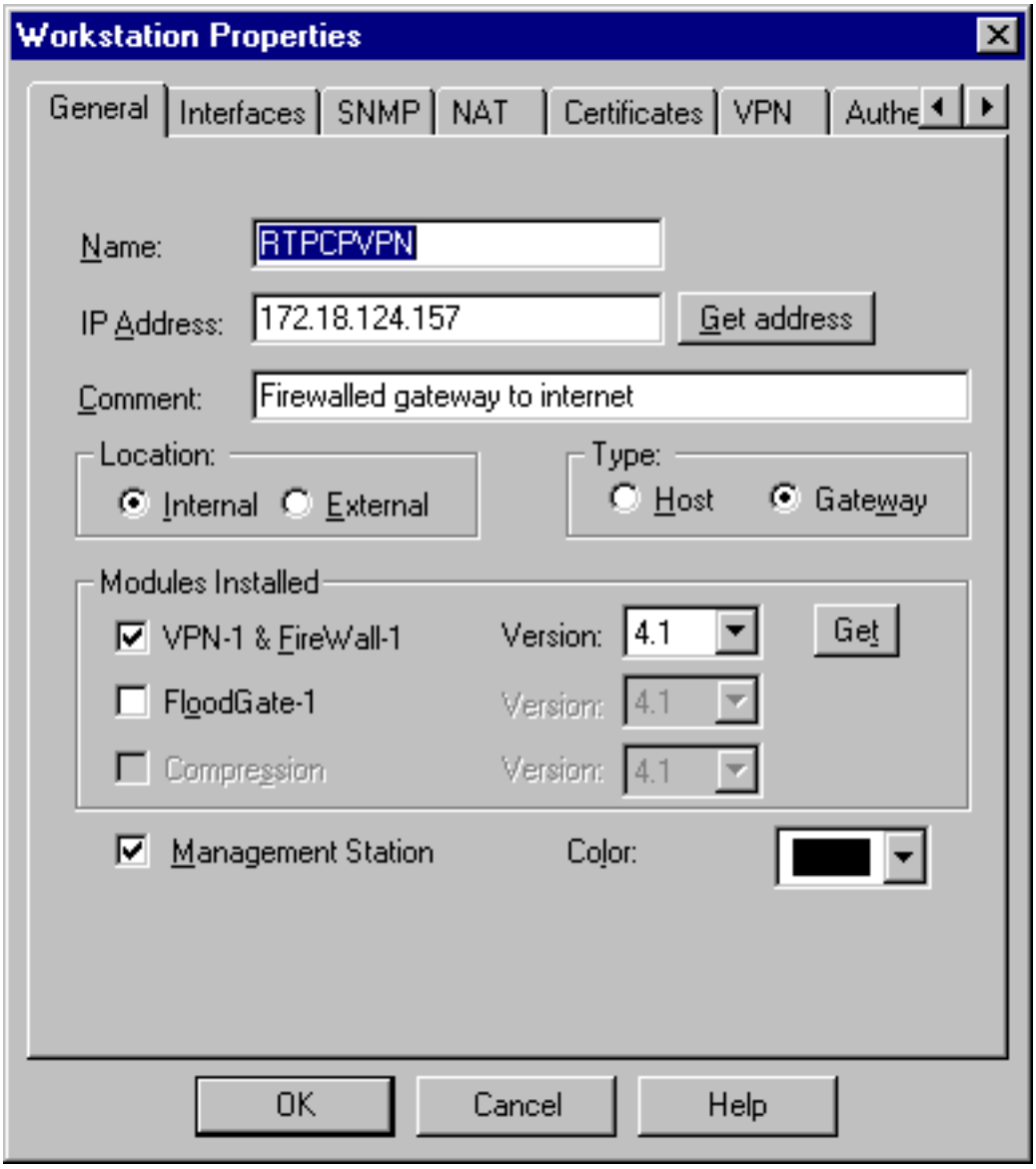


2. Wählen Sie **Verwalten > Netzwerkobjekte > Neu (oder Bearbeiten) > Netzwerk**, um das Objekt für das interne ("cpinside") Netzwerk hinter dem Prüfpunkt zu konfigurieren. Dies sollte mit dem Befehl **"Peer = "10.32.50.0/24"** VPN Concentrator

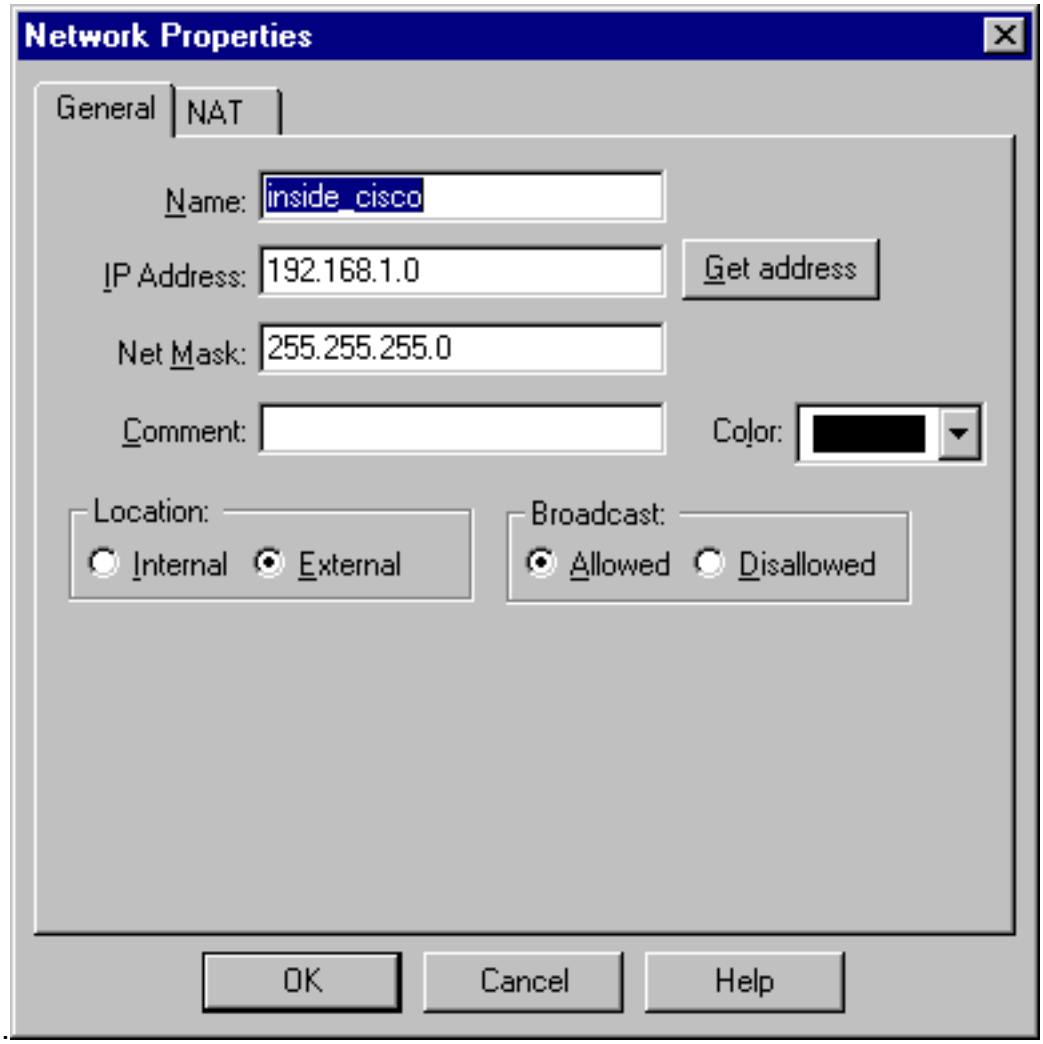


übereinstimmen.

3. Wählen Sie **Verwalten > Netzwerkobjekte > Bearbeiten**, um das Objekt für den Gateway-Endpunkt ("RTPCPVPN"-Prüfpunkt) zu bearbeiten, auf den der VPN-Konzentrator im **Partner = <ip>**-Befehl verweist.Wählen Sie **Interne** unter Speicherort aus.Wählen Sie **Gateway** als Typ aus.Unter **Installierte Module** finden Sie Informationen zu **VPN-1 und FireWall-1** und **Managementkonsole**.

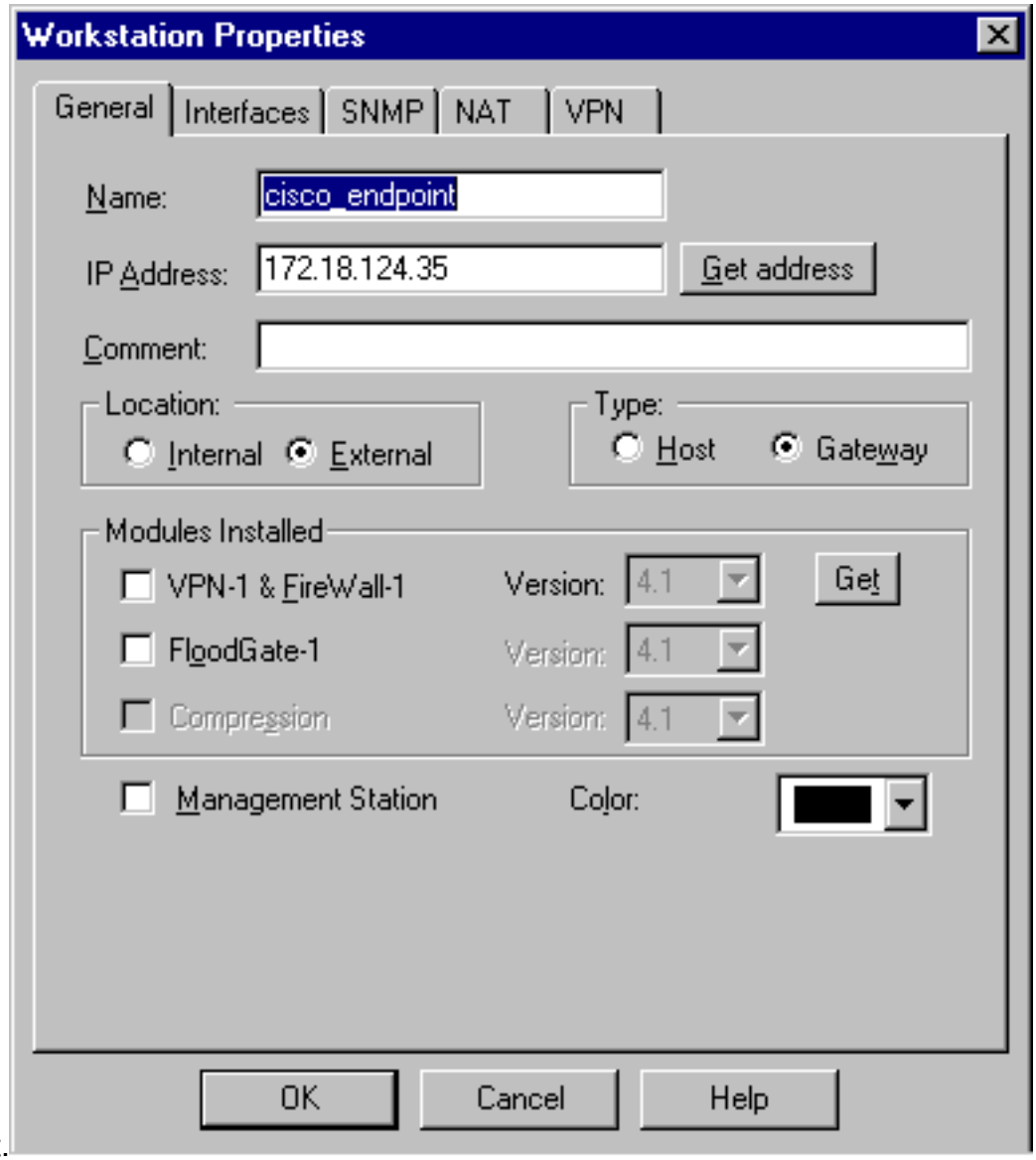


4. Wählen Sie **Verwalten > Netzwerkobjekte > Neu (oder Bearbeiten) > Netzwerk**, um das Objekt für das externe ("inside_cisco") Netzwerk hinter dem VPN-Konzentrator zu konfigurieren.Dies sollte mit dem Befehl **LocalAccess = <192.168.1.0/24>** VPN Concentrator



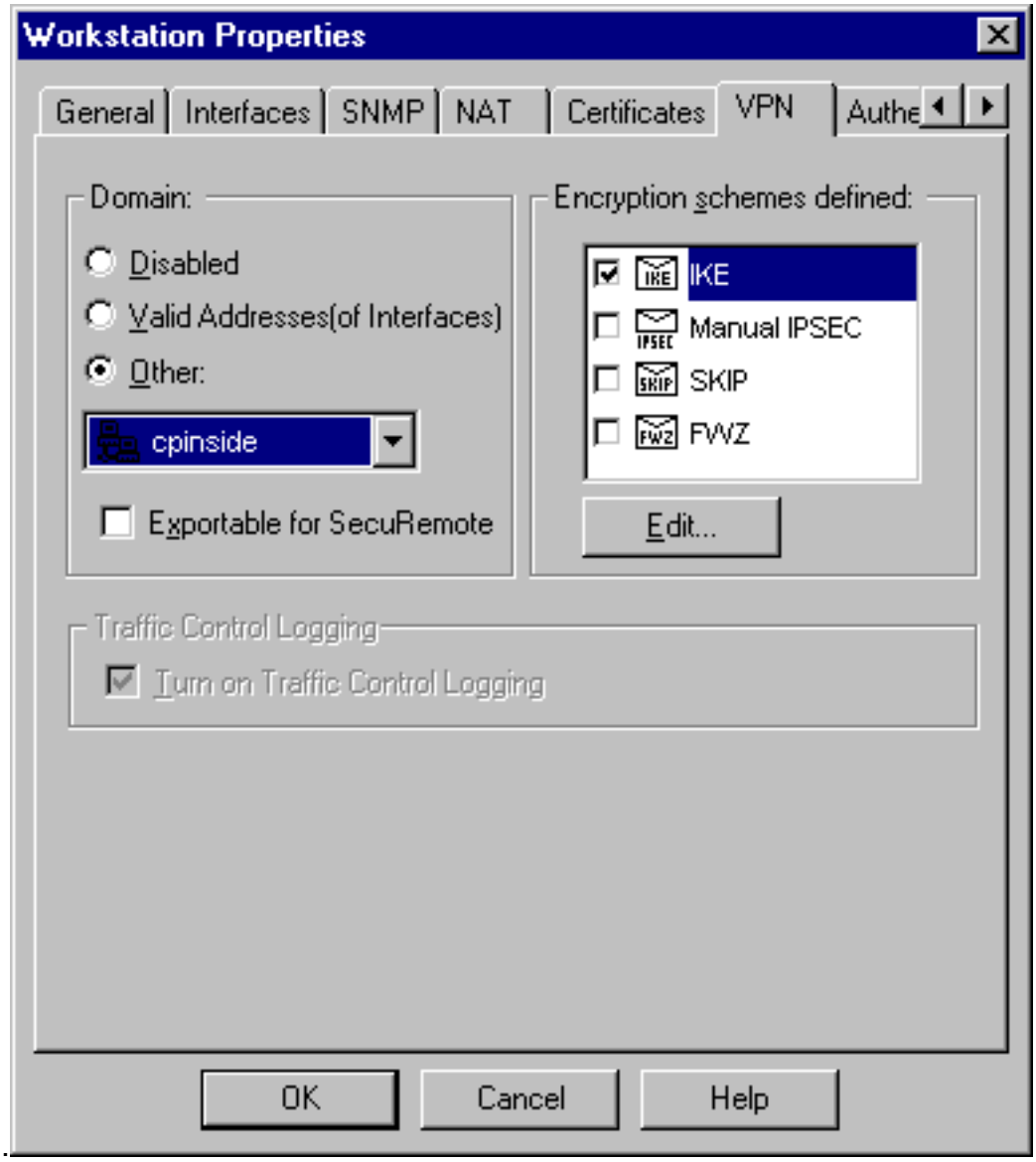
übereinstimmen.

5. Wählen Sie **Verwalten > Netzwerkobjekte > Neu > Workstation**, um ein Objekt für das externe VPN-Concentrator-Gateway ("cisco_endpoint") hinzuzufügen.Dies ist die "externe" Schnittstelle des VPN Concentrator mit Verbindung zum Checkpoint (in diesem Dokument ist 172.18.124.35 die IP-Adresse im **IPAddress = <ip>**-Befehl).Wählen Sie **Extern** unter Speicherort aus. Wählen Sie **Gateway** als Typ aus.**Hinweis:** Aktivieren Sie VPN-1/FireWall-1



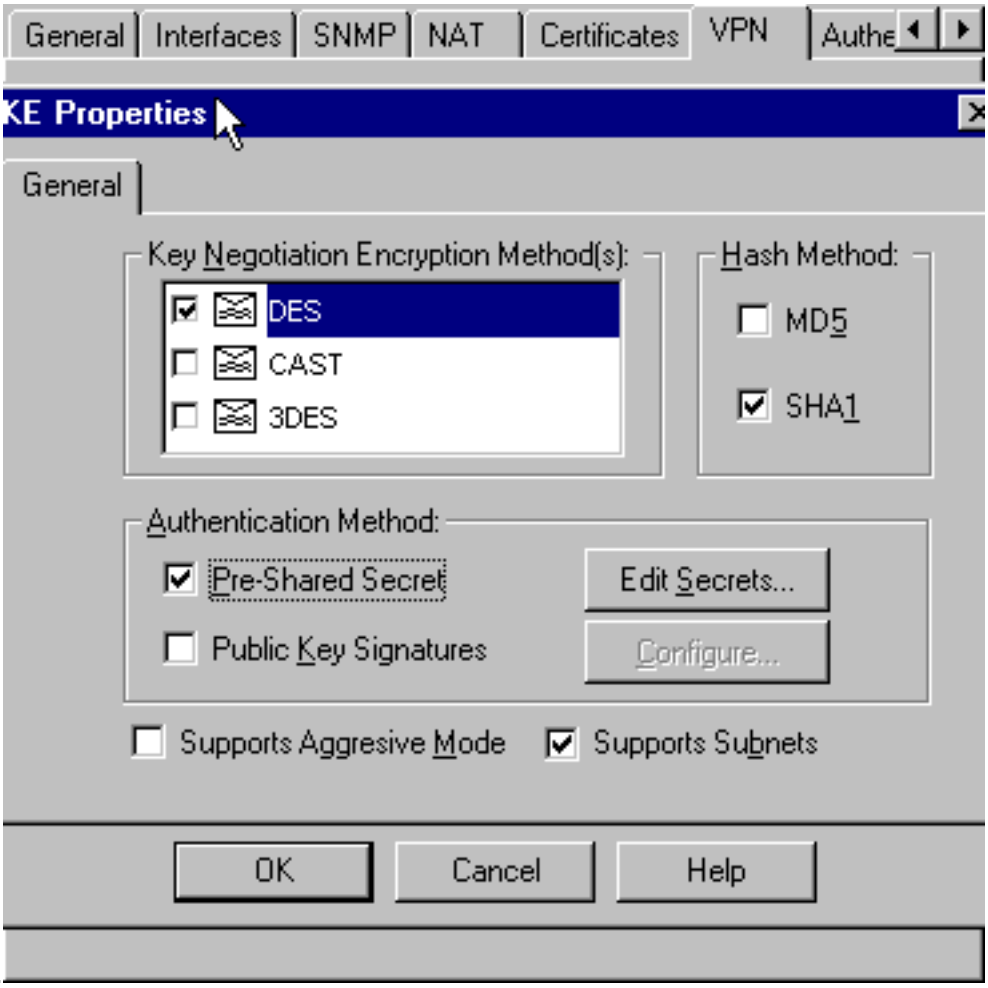
nicht.

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



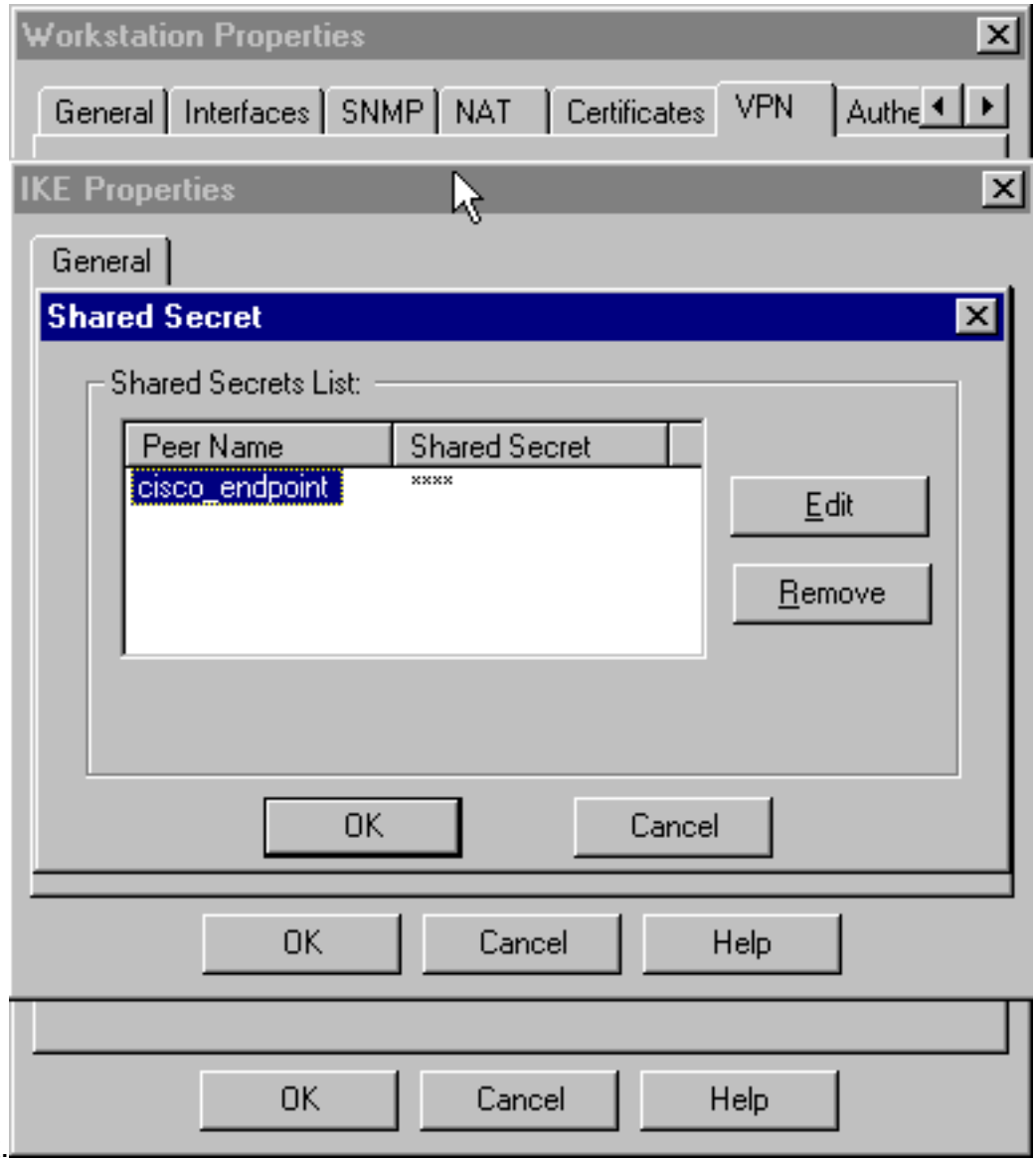
Bearbeiten.

7. Ändern Sie die IKE-Eigenschaften in **DES**-Verschlüsselung und **SHA1-**Hashing, um mit dem Befehl **SHA_DES_G2** VPN Concentrator zu übereinstimmen.**Hinweis:** "G2" bezieht sich auf die Diffie-Hellman-Gruppe 1 oder 2. Beim Testen wurde entdeckt, dass der Prüfpunkt entweder "G2" oder "G1" akzeptiert.Ändern Sie diese Einstellungen:Deaktivieren Sie die **Option Aggressiver Modus**.Aktivieren Sie **Subnetze unterstützen**.Aktivieren Sie **Pre-Shared Secret** unter Authentication



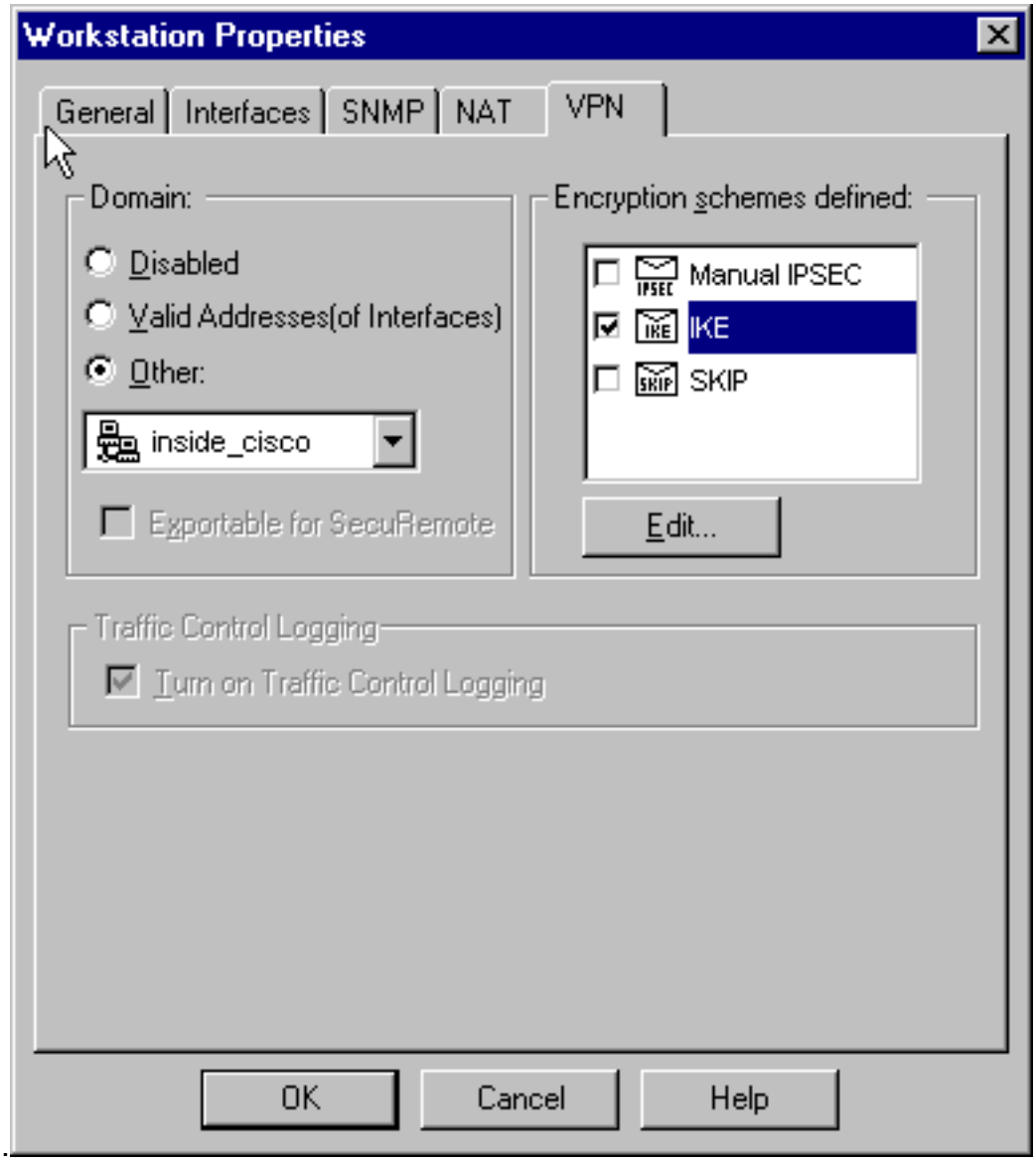
Method.

8. Klicken Sie auf **Edit Secrets** (Geheimnisse **bearbeiten**), um den vorinstallierten Schlüssel so festzulegen, dass er mit dem Befehl **SharedKey = <key>** VPN Concentrator



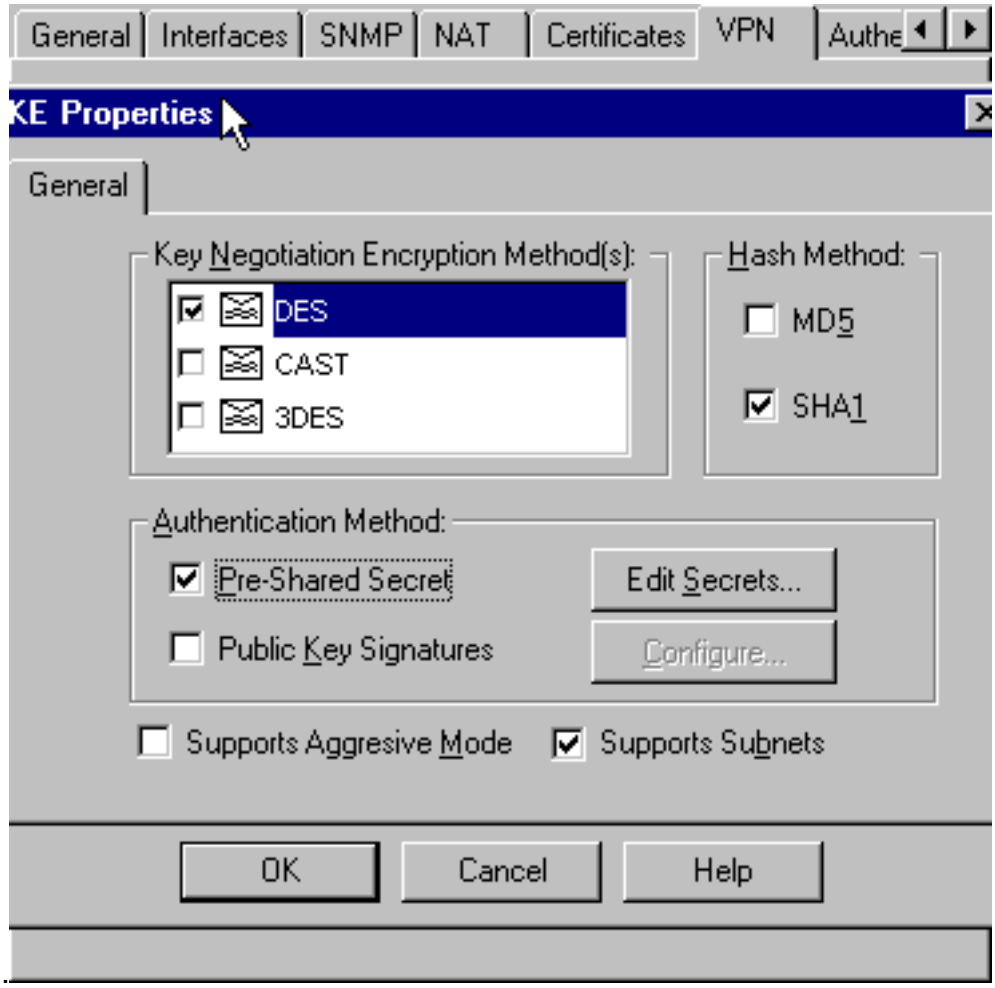
übereinstimmt.

9. 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 Komponente des VPN Concentrator-Netzwerks aus (die Bezeichnung "inside_cisco"). Wählen Sie unter Definierte Verschlüsselungsschemata die Option **IKE aus**, und klicken Sie dann auf



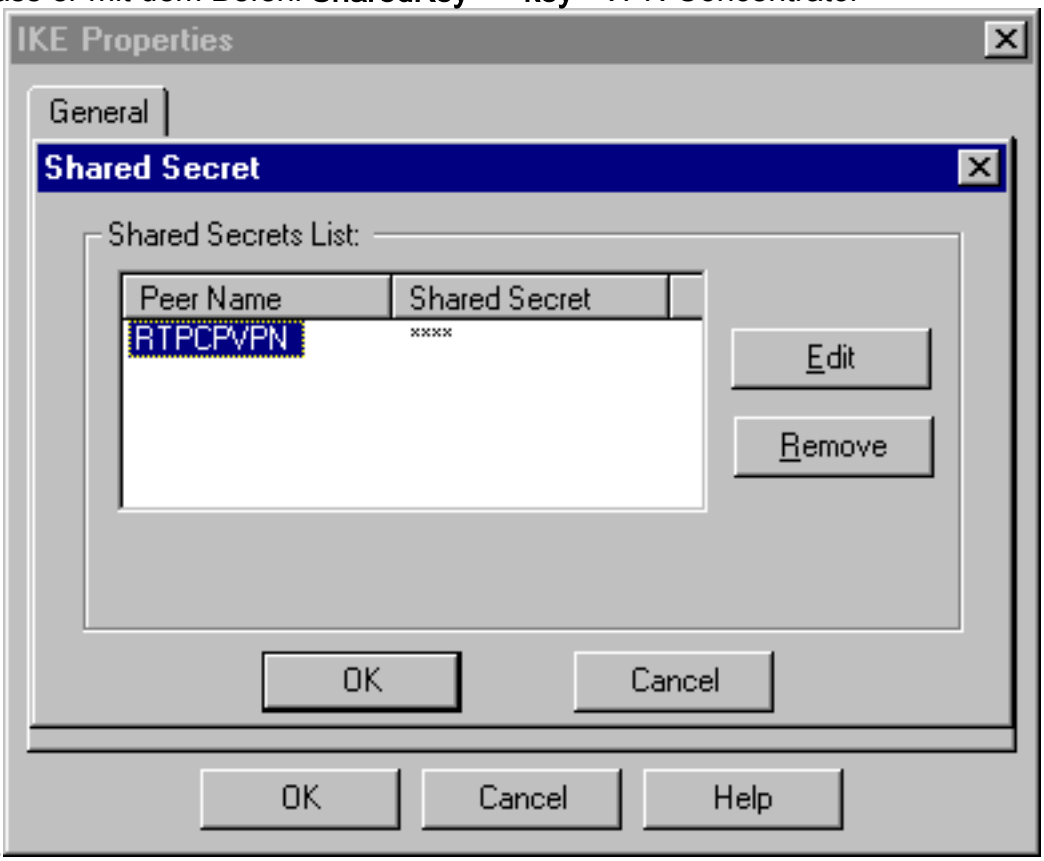
Bearbeiten.

10. Ändern Sie die IKE-Eigenschaften in **DES**-Verschlüsselung und **SHA1-**Hashing, um mit dem Befehl **SHA_DES_G2** VPN Concentrator zu übereinstimmen.**Hinweis:** "G2" bezieht sich auf die Diffie-Hellman-Gruppe 1 oder 2. Im Test wurde festgestellt, dass der Prüfpunkt entweder "G2" oder "G1" akzeptiert.Ändern Sie diese Einstellungen:Deaktivieren Sie die **Option Aggressiver Modus**.Aktivieren Sie **Subnetze unterstützen**.Aktivieren Sie **Pre-Shared Secret** unter Authentication



Method.

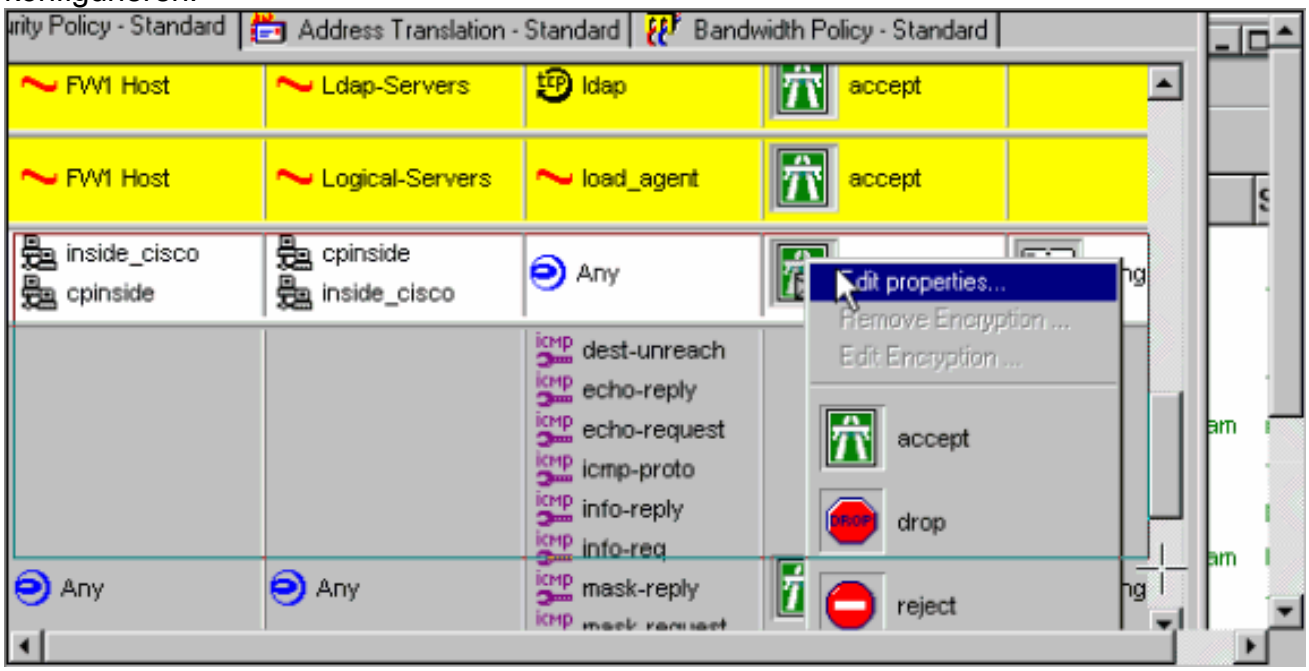
11. Klicken Sie auf **Edit Secrets** (Geheimnisse **bearbeiten**), um den vorinstallierten Schlüssel so festzulegen, dass er mit dem Befehl **SharedKey = <key>** VPN Concentrator



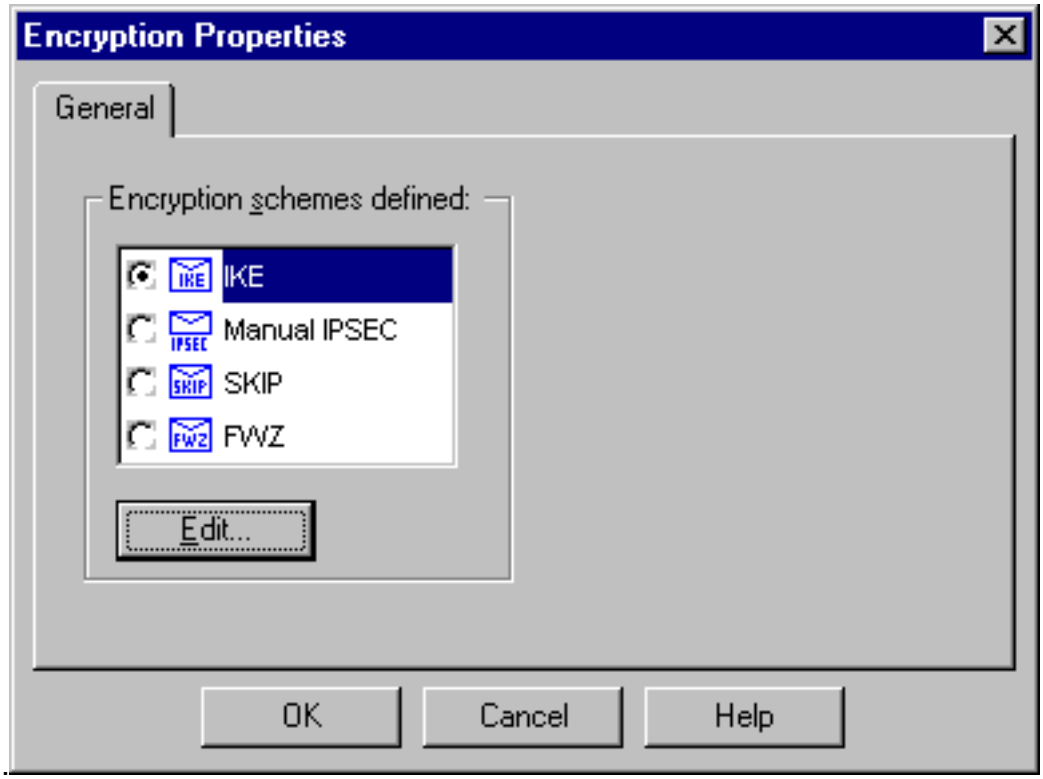
übereinstimmt.

12. 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**.

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

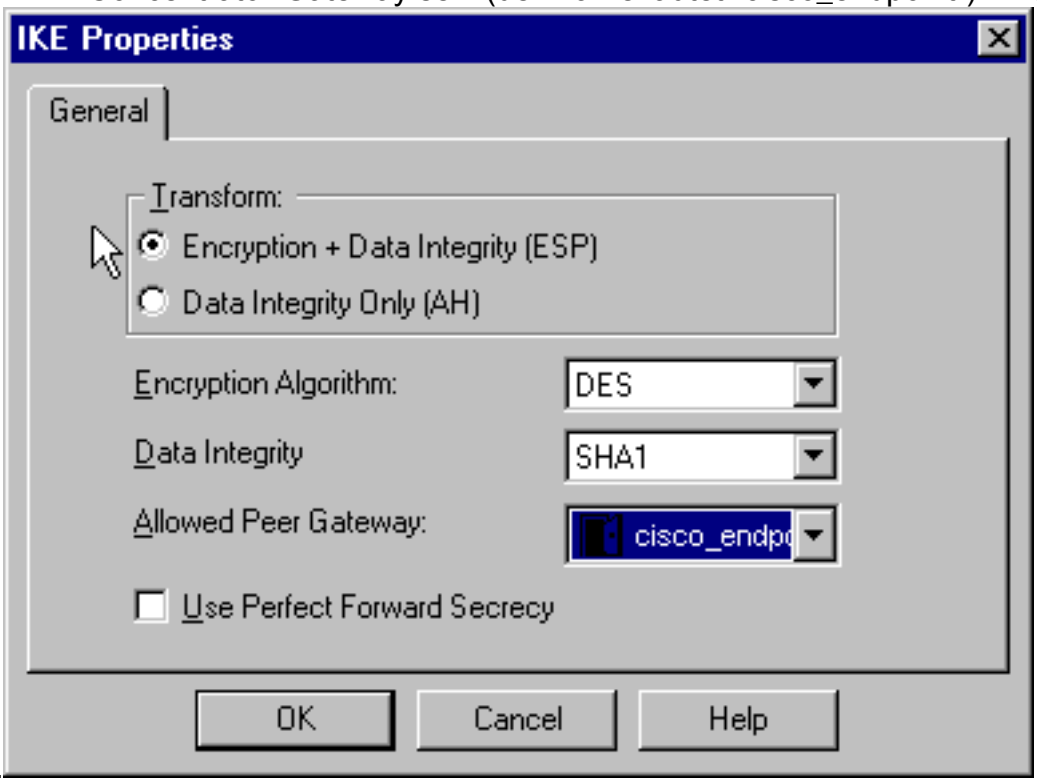


14. Wählen Sie **IKE aus**, und klicken Sie auf



Bearbeiten.

15. Ändern Sie im Fenster IKE-Eigenschaften diese Eigenschaften, um mit dem Befehl **Transform = esp(sha,des)** VPN Concentrator zuzustimmen.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 VPN-Concentrator-Gateway sein (der Name lautet "cisco_endpoint"). Klicken Sie



auf **OK**.

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

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Befehle zur Fehlerbehebung beim VPN 500 Concentrator

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**.

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

- **vpn trace dump all** - Zeigt Informationen über alle übereinstimmenden VPN-Verbindungen an, einschließlich Informationen über die Zeit, die VPN-Nummer, die tatsächliche IP-Adresse des Peers, die ausgeführten Skripts und im Falle eines Fehlers die Routine und Leitungsnummer des Software-Codes, in dem der Fehler aufgetreten ist.
- **show system log buffer** (Systemprotokollpuffer anzeigen) - Zeigt den Inhalt des internen Protokollpuffers an.
- **show vpn statistics** - Zeigt diese Informationen für Benutzer, Partner und die Gesamtsumme für beide. (Bei modularen Modellen umfasst das Display einen Bereich für jeden Modulsteckplatz. Weitere Informationen finden Sie im Abschnitt Beispieldebugausgabe.)`Current Active` - Die aktuell aktiven Verbindungen.`In Negot` - Die derzeit verhandelnden Verbindungen.`High Water` - Die höchste Anzahl gleichzeitiger aktiver Verbindungen seit dem letzten Neustart.`Running Total (Gesamt ausführen)`: Die Gesamtzahl erfolgreicher Verbindungen seit dem letzten Neustart.`Tunnel OK` (Tunnel OK): Die Anzahl der Tunnel, für die keine Fehler aufgetreten sind.`Tunnel Starts` (Tunnel wird gestartet): Die Anzahl der Tunnelstarts.`Tunnel Error` (Tunnel-Fehler): Die Anzahl der Tunnel mit Fehlern.
- **show vpn statistics ausführliche** - Zeigt Statistiken zur ISAKMP-Aushandlung und viele weitere aktive Verbindungsstatistiken an.

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 VPN-Concentrator 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 eingeschlossen werden, können sie in 10.0.0.0 /23 zusammengefasst werden.

Checkpoint 4.1 Firewall-Fehlerbehebung

Dies war eine Microsoft Windows NT-Installation. Da die Verfolgung im Fenster des Policy Editor (wie in Schritt 12 gezeigt) für `Long` 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
```

Führen Sie diese Befehle aus, um die Sicherheitszuordnungen (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 mit **Ja** im `Fenster Sind Sie sicher?` eingeben.

Beispielausgabe für Debugging

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)


cisco_endpoint#show vpn stat

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ---------------------------------------------------------------
```

```
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

cisco_endpoint#show vpn stat verb

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

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

Input VPN pkts dropped due to no SA: 0

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

ISAKMP Negotiation stats
Admin packets in        4
Fastswitch packets in   0
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      1
Inserted cookie(R)      0
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        0
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
```

```
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

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

ISAKMP Negotiation stats
Admin packets in        0
Fastswitch packets in   3
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      0
Inserted cookie(R)      1
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        3
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
```

```
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0
```

Zugehörige Informationen

- Cisco VPN Concentrators der Serie 5000 - Ankündigung des Vertriebsendes
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems