Een IPSec-tunnels configureren - Cisco VPN 3000 Concentrator om controlepunt 4.1-firewall te configureren

Inhoud

Inleiding

Dit document toont aan hoe u een IPsec-tunnel met vooraf gedeelde toetsen kunt vormen om zich aan twee particuliere netwerken aan te sluiten:

- Een privaat netwerk binnen Cisco VPN 3000 Concentrator (192.168.1.x).
- Een privaat netwerk binnen de Checkpoint 4.1 Firewall (10.32.50.x).

Er wordt aangenomen dat het verkeer van binnen de VPN-centrator en binnen het checkpoint naar het internet (in dit document weergegeven door de 172.18.124.x-netwerken) toeneemt voordat de configuratie begint.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

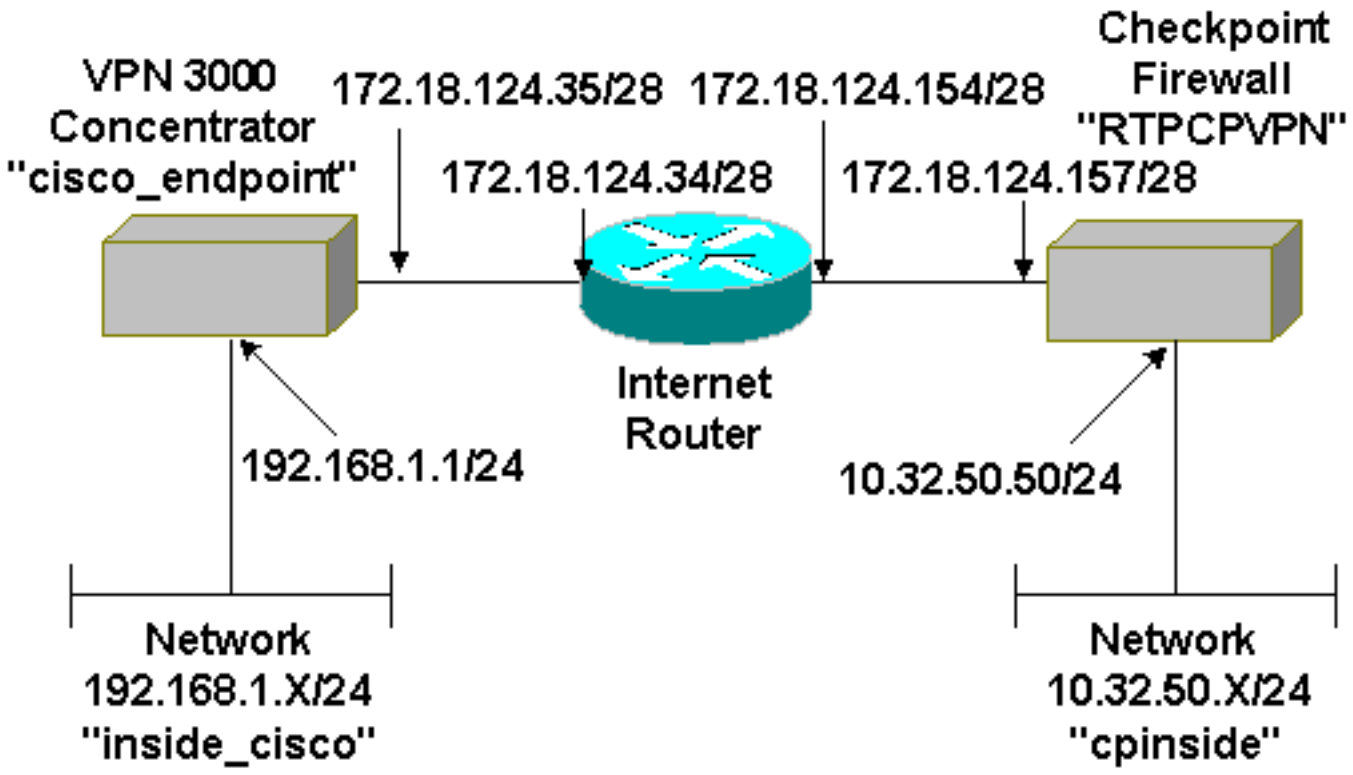
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VPN 3000 Concentrator
- VPN 3000 Concentrator-softwarerelease 2.5.2.F
- Control-point 4.1-firewall

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Conventies

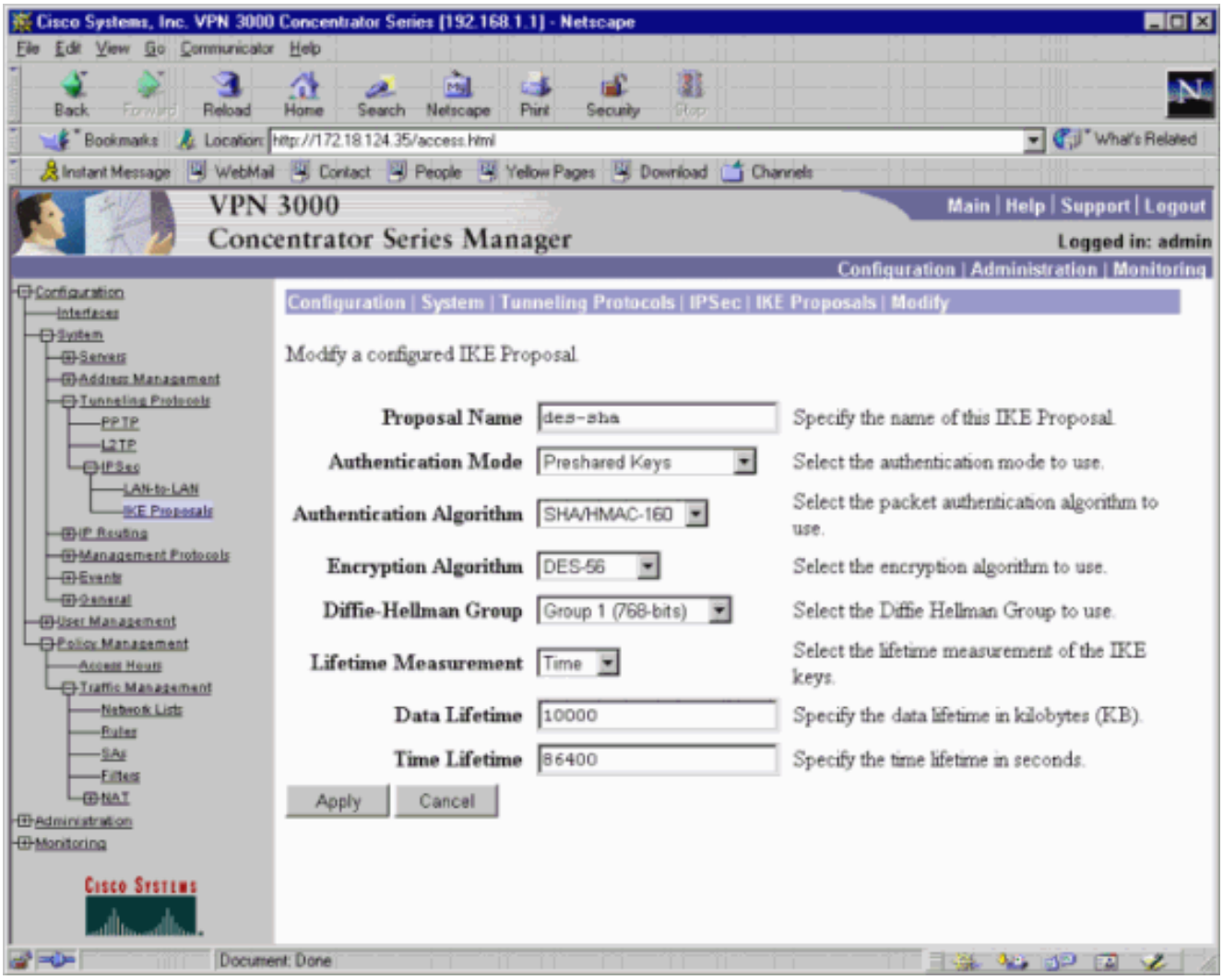
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

De VPN 3000-concentratie configureren

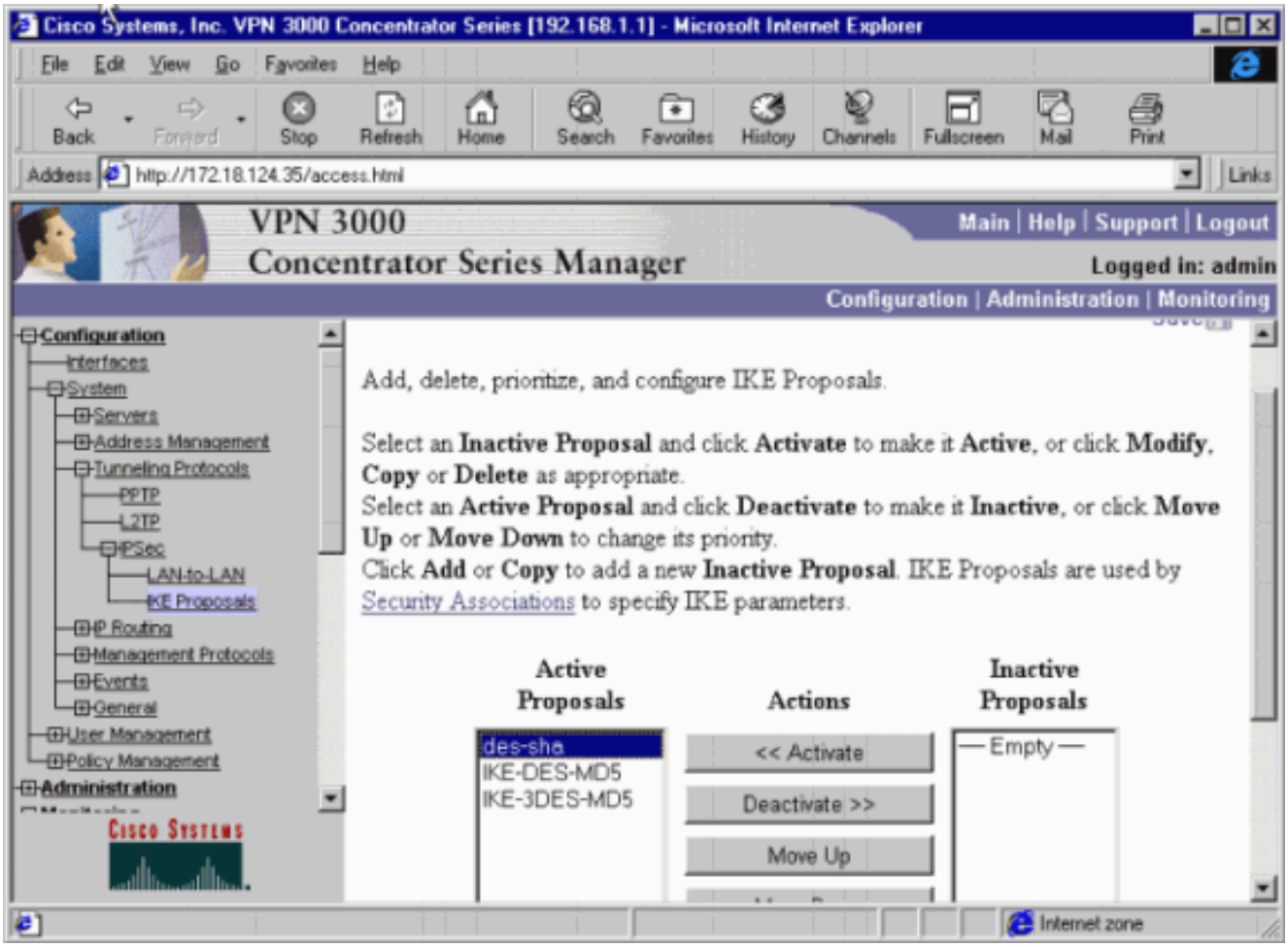
Volg deze stappen om de VPN 3000 Concentrator te configureren.

1. Selecteer **Configuration > System > Tunneling Protocols > IPSec > IKE Voorstellen > Wijzigen** om een voorstel voor Internet Key Exchange (IKE) met de naam "des-sha" met Secure Hash Algorithm (SHA), Data Encryption Standard (DES) en Diffie-Hellman groep 1 te maken. Laat de Time Liftime op de standaard 8640 seconden.**Opmerking:** het geldige bereik voor de VPN-Concentrator IKE-levensduur is 60-2147483647

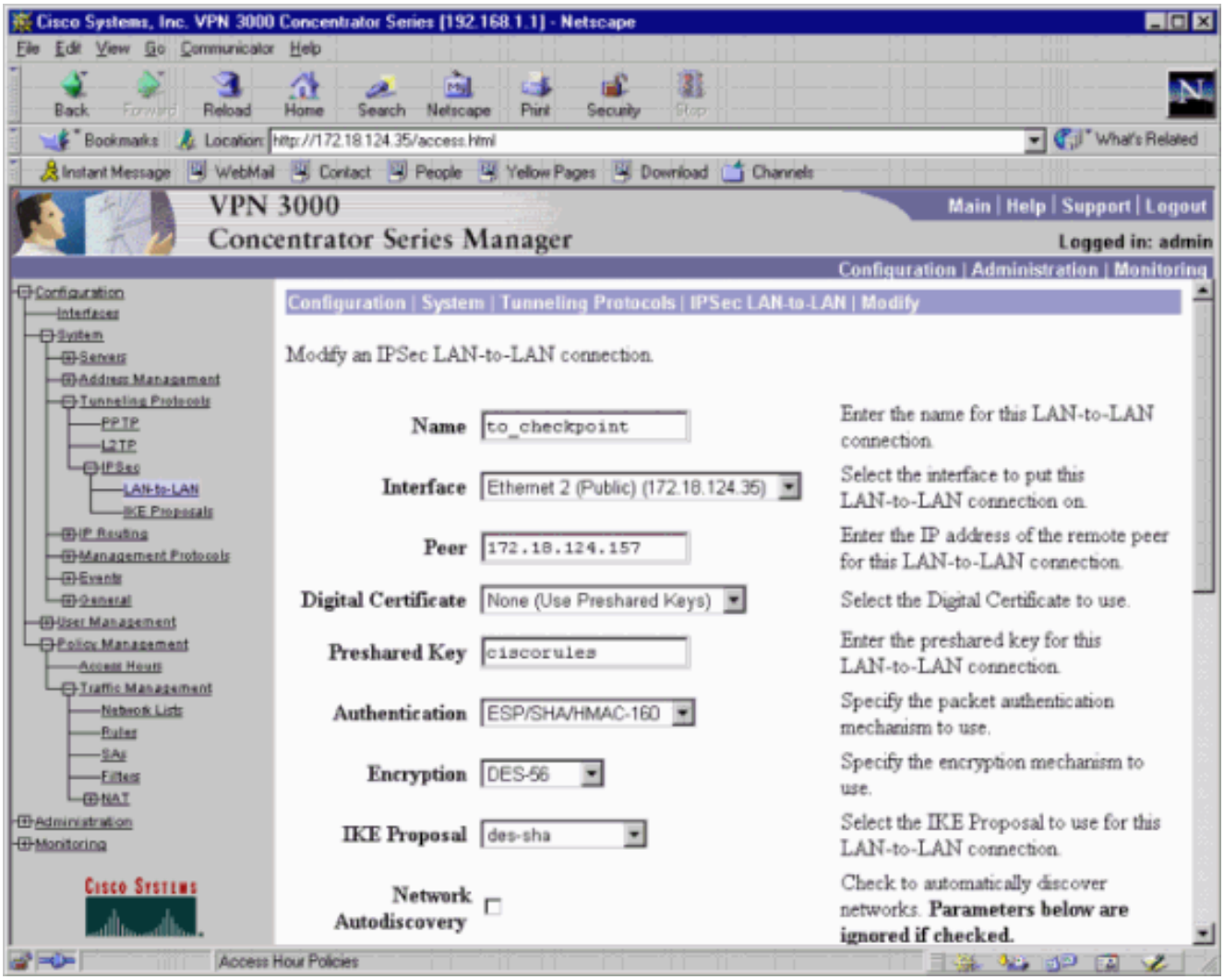
seconden.

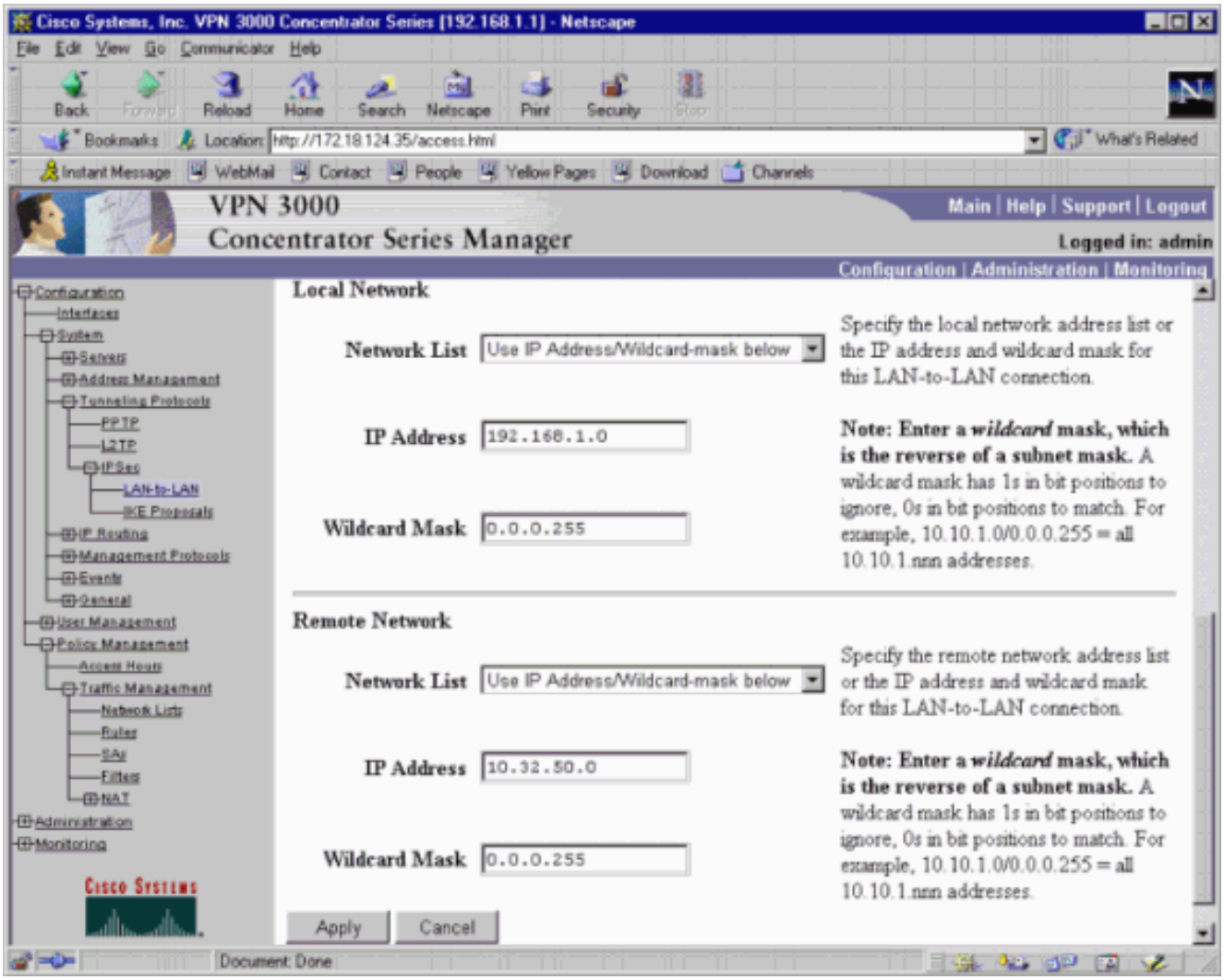


2. Selecteer **Configuration > System > Tunneling Protocols > IPSec > IKE-voorstellen**. Selecteer "descrambler" en klik op **Activeren** om het IKE-voorstel te activeren.

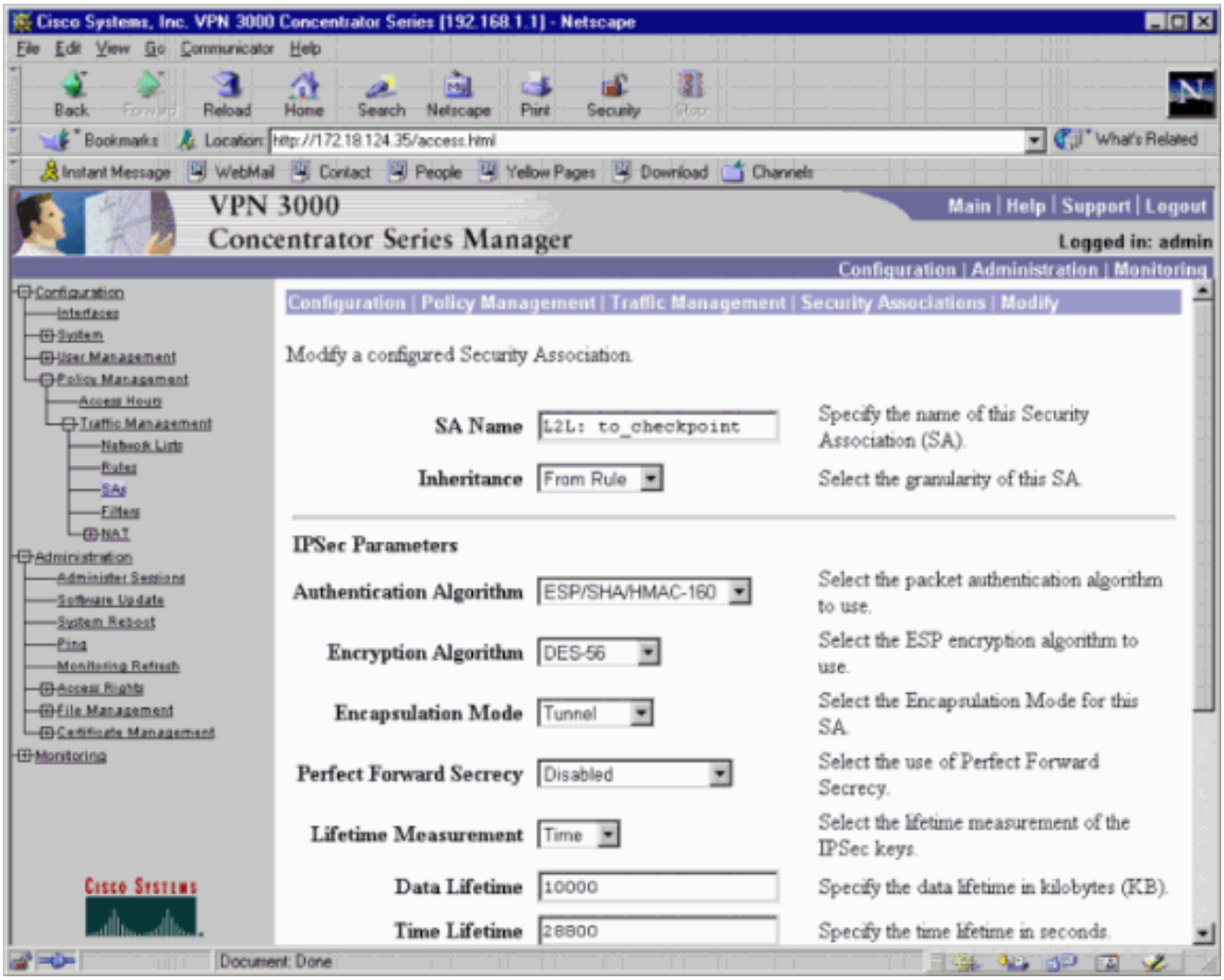


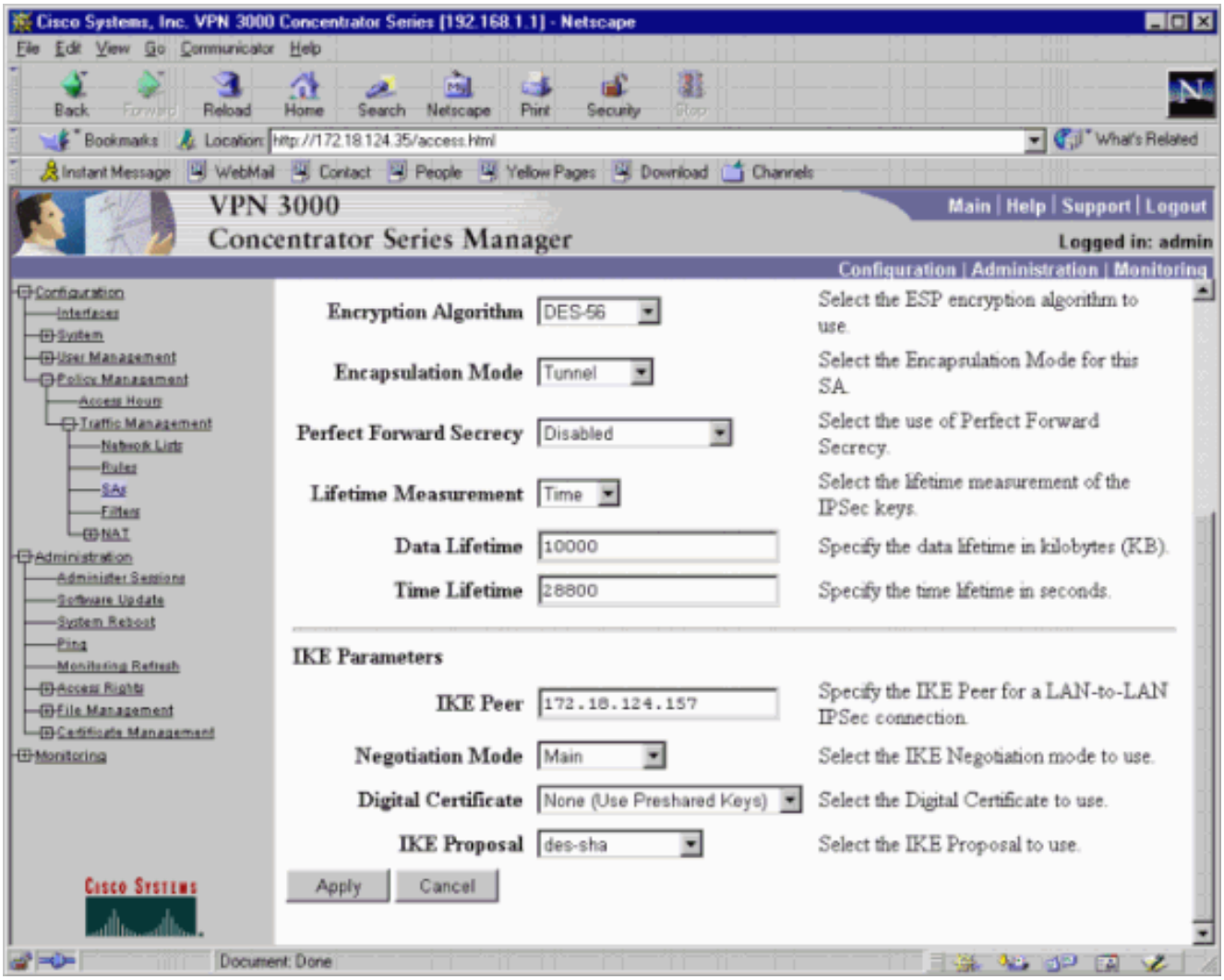
3. Selecteer **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add**.Stel een IPsec-tunnel in die "to_checkpoint" wordt genoemd, met het checkpoint adres als peer. Typ de eigenlijke sleutel voor de PreShared Key. Selecteer onder Verificatie ESP/SHA/HMAC-160 en selecteer DES-56 voor Encryptie. Voer het IKE-voorstel ("des-sha" in dit voorbeeld) en de lokale en afstandsnetwerken
in.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
IP Routing
Management Protocols
Events
General
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify
Modify an IPSec LAN-to-LAN connection.
Name
to_checkpoint
Enter the name for this LAN-to-LAN connection.
Interface
Ethernet 2 (Public) (172.18.124.35)
Select the interface to put this LAN-to-LAN connection on.
Peer
172.18.124.157
Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate
None (Use Preshared Keys)
Select the Digital Certificate to use.
Preshared Key
ciscorules
Enter the preshared key for this LAN-to-LAN connection.
Authentication
ESP/SHA/HMAC-160
Specify the packet authentication mechanism to use.
Encryption
DES-56
Specify the encryption mechanism to use.
IKE Proposal
des-sha
Select the IKE Proposal to use for this LAN-to-LAN connection.
Network Autodiscovery
Check to automatically discover networks. Parameters below are ignored if checked.
Access Hour Policies



4. Selecteer **Configuratie > Beleidsbeheer > Verkeersbeheer > Beveiligingsassociaties > Wijzigen**. Controleer dat Perfect Forward SecRITY **uitgeschakeld** is en laat de IPsec Time Liftime tijdens de standaard **28800** seconden vrij.**Opmerking:** het geldige bereik voor het VPN-Concentrator IPsec-leven is 60-2147483647
seconden.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Administer Sessions
Software Update
System Reboot
Ping
Monitoring Refresh
Access Rights
File Management
Certificate Management
Monitoring
Cisco Systems
Configuration | Policy Management | Traffic Management | Security Associations | Modify
Modify a configured Security Association.
SA Name L2L: to_checkpoint Specify the name of this Security Association (SA).
Inheritance From Rule Select the granularity of this SA.
IPSec Parameters
Authentication Algorithm ESP/SHA/HMAC-160 Select the packet authentication algorithm to use.
Encryption Algorithm DES-56 Select the ESP encryption algorithm to use.
Encapsulation Mode Tunnel Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy Disabled Select the use of Perfect Forward Secrecy.
Lifetime Measurement Time Select the lifetime measurement of the IPSec keys.
Data Lifetime 10000 Specify the data lifetime in kilobytes (KB).
Time Lifetime 28800 Specify the time lifetime in seconds.
Document: Done

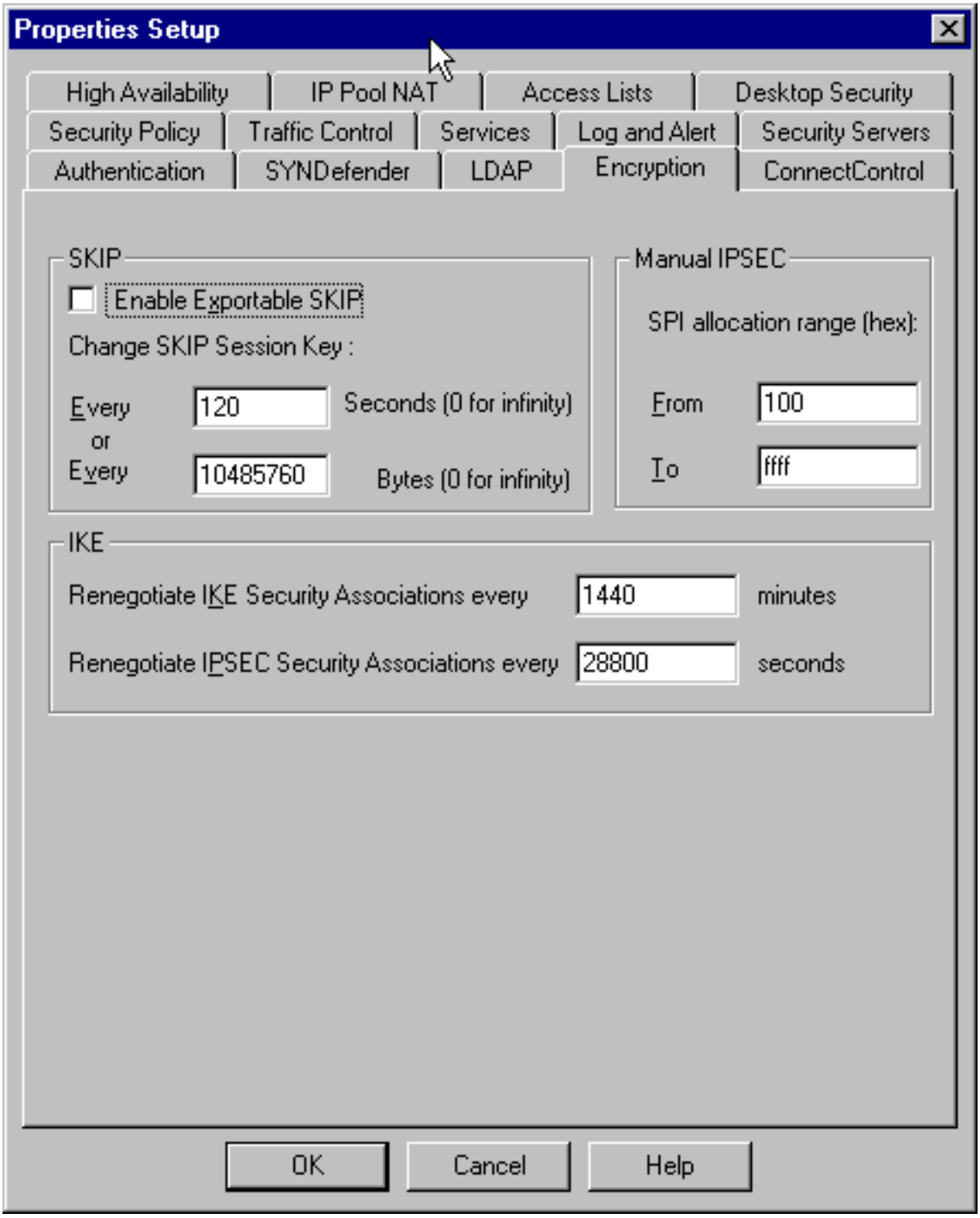


5. Bewaar de configuratie.

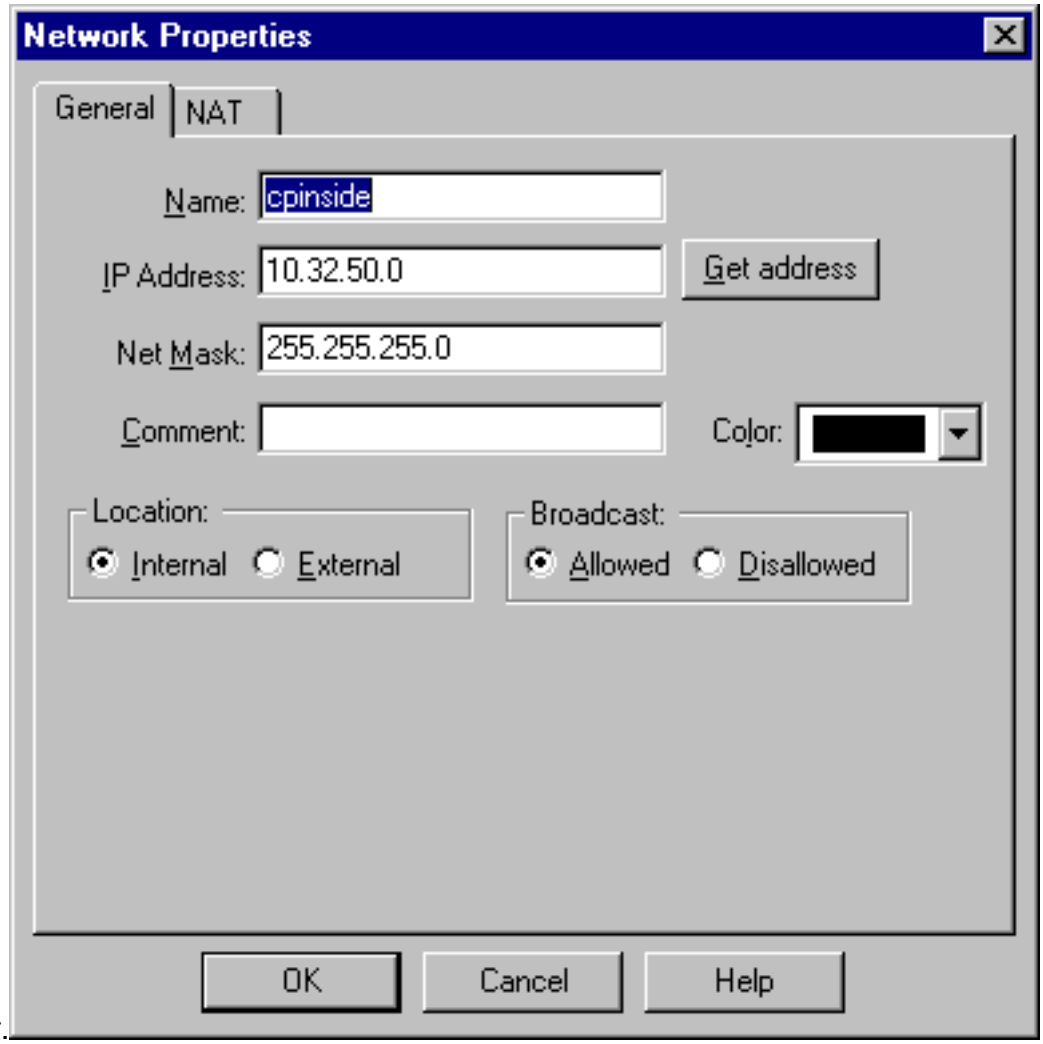
Configureer de controlepunt 4.1-firewall

Volg deze stappen om de firewall van checkpoint 4.1 te configureren.

1. Aangezien de standaard IKE- en IPsec-levens van elke verkoper verschillen, selecteert u **Eigenschappen > Encryption** om de leven van het checkpoint in te stellen om met de standaardwaarden van VPN Concentrator akkoord te gaan.De standaard IKE-levensduur van VPN Concentrator is 8640 seconden (=1440 minuten).De standaard IPsec-levensduur van VPN Concentrator is 2800
seconden.

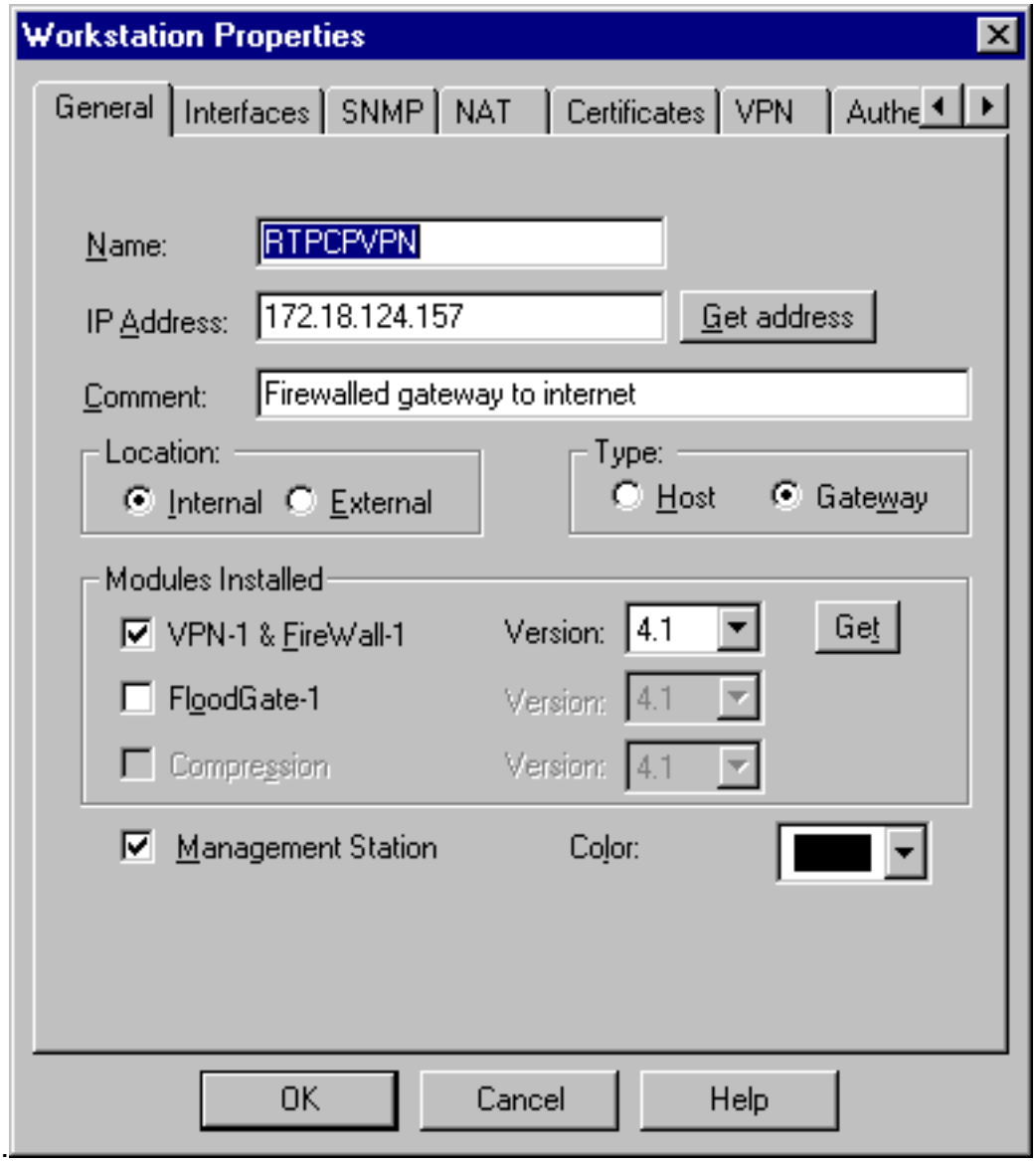


2. Selecteer **Manager > Netwerkobjecten > Nieuw (of Bewerken) > Netwerk** om het object voor het interne netwerk ("component") achter het Selectieteken te configureren. Dit moet overeenkomen met de "Remote Network" in de VPN-



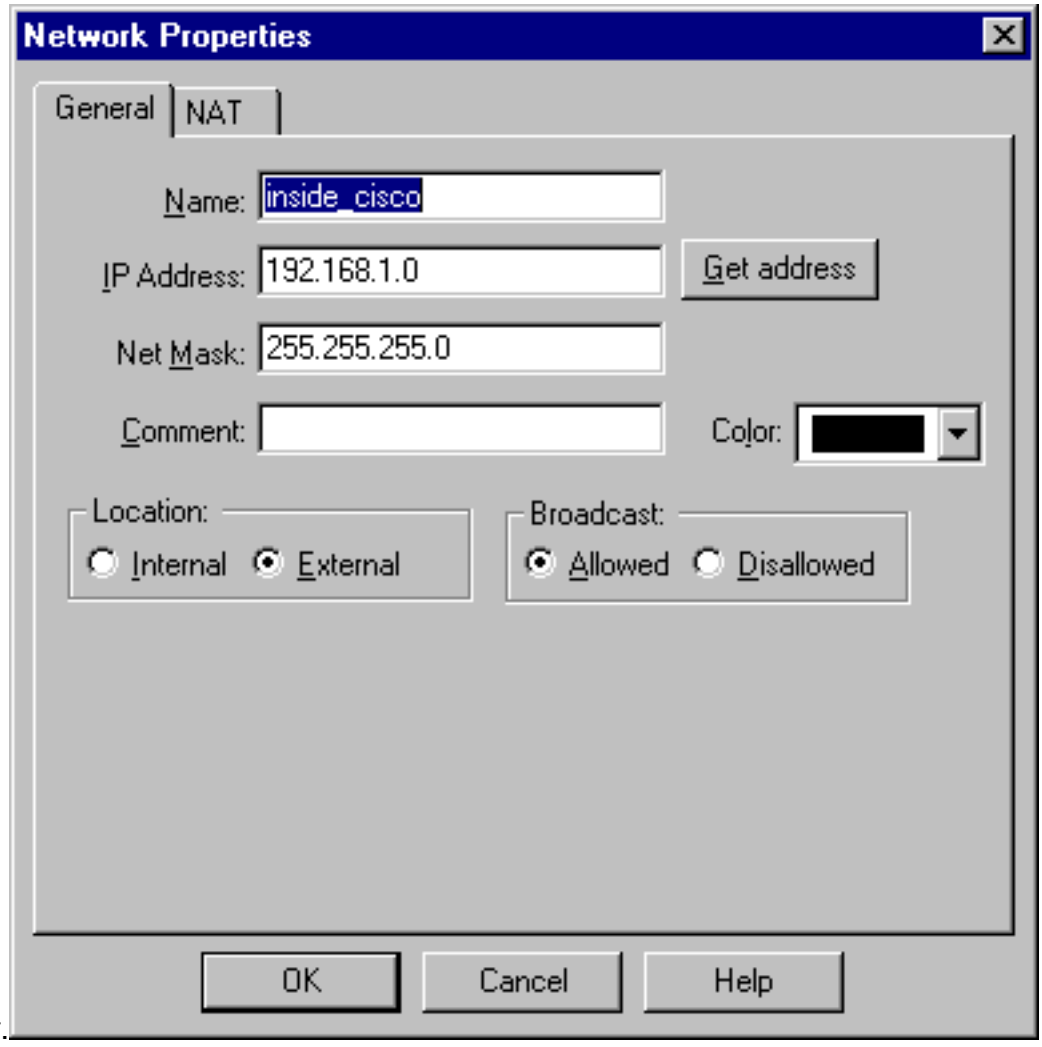
centrator.

3. Selecteer **Manager > Netwerkobjecten > Bewerken** om het object te bewerken voor het eindpunt van de gateway ("RTPC VPN"-controle) dat de VPN-Concentrator in zijn peer parameter heeft.Selecteer onder Locatie de optie **Interne**. Selecteer voor type de optie **Gateway**. Controleer onder geïnstalleerde modules **VPN-1 en FireWall-1** en controleer **het**



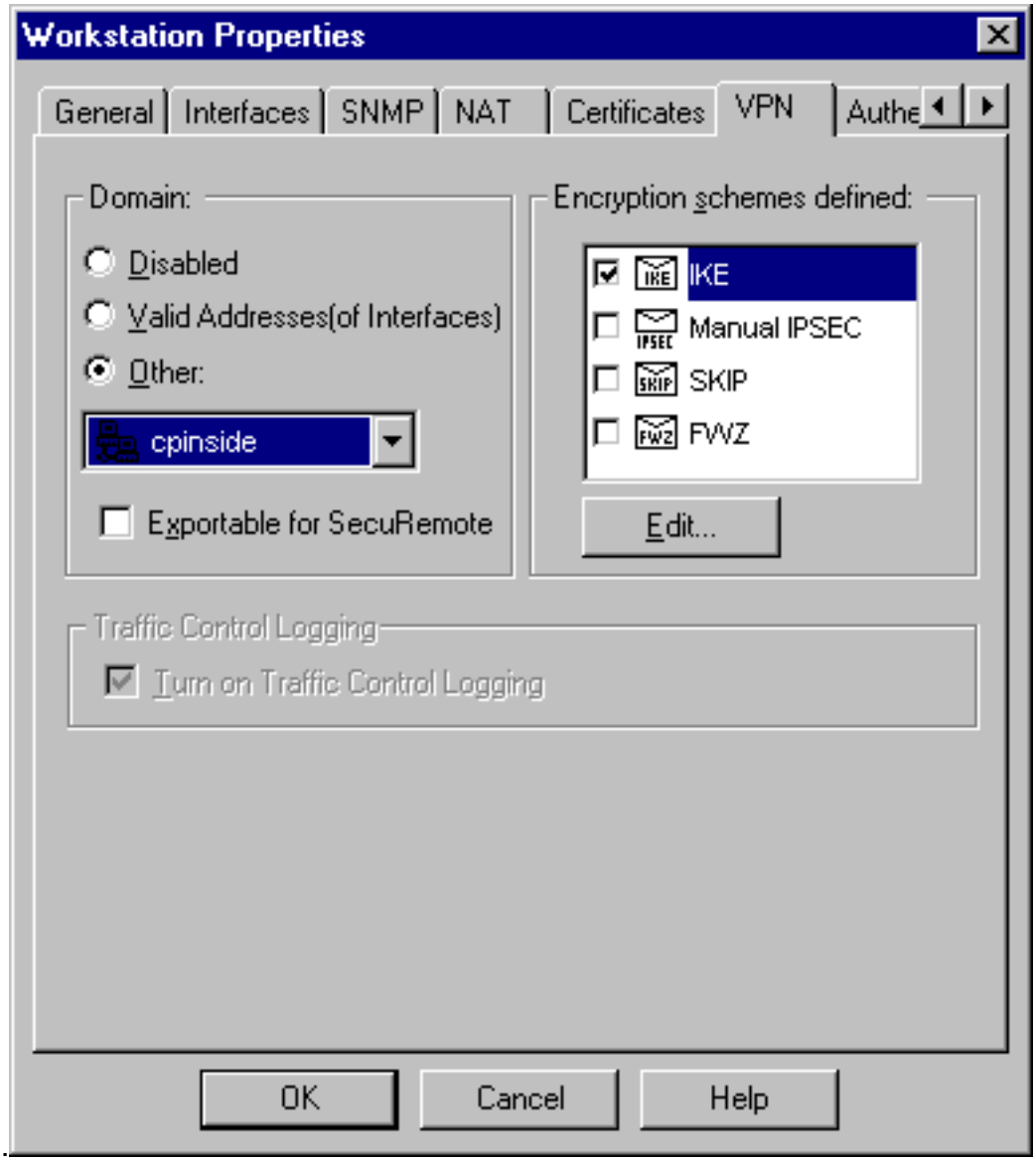
beheerstation.

4. Selecteer **Manager > Netwerkobjecten > Nieuw (of Bewerken) > Netwerk** om het object voor het externe netwerk ("interne_cisco") achter de VPN-centrator te configureren. Dit moet overeenkomen met het "Local" netwerk in de VPN



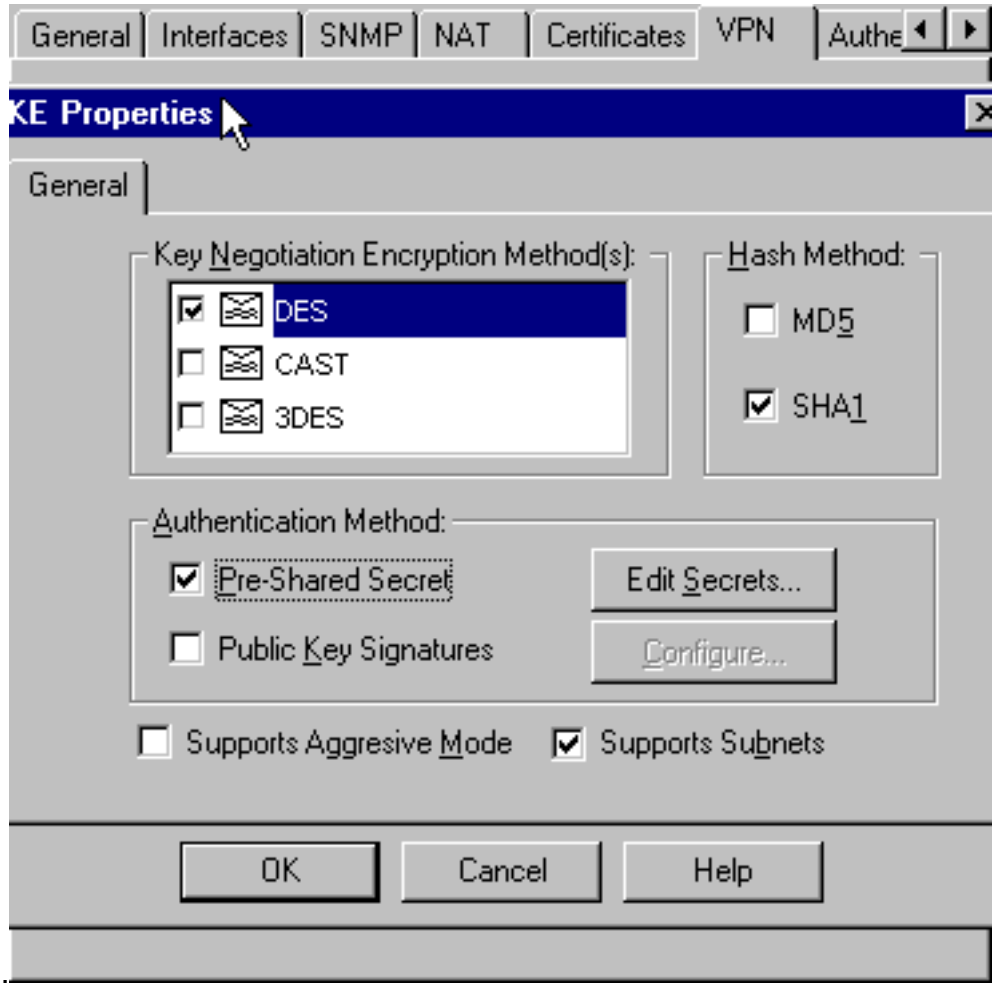
Concentrator.

5. Selecteer **Manager > Netwerkobjecten > Nieuw > Workstation** om een object voor de externe ("cisco_endpoints") VPN Concentrator-gateway toe te voegen. Dit is de VPN Concentrator "Openbare" interface.Selecteer onder Locatie de optie **Extern**. Selecteer voor type de optie **Gateway**.**Opmerking:** selecteer niet het aankruisvakje VPN-1/FireWall-1.
6. Selecteer **Manager > Netwerkobjecten > Bewerken** om het tabblad Selectiepunt te bewerken (genaamd "RTPVPN") VPN-tabblad. Selecteer onder Domain, Andere en selecteer dan de binnenkant van het Selectietwerk (genoemd "component") van de vervolgkeuzelijst. Selecteer onder Encryption schemes die worden gedefinieerd **IKE** en klik vervolgens op



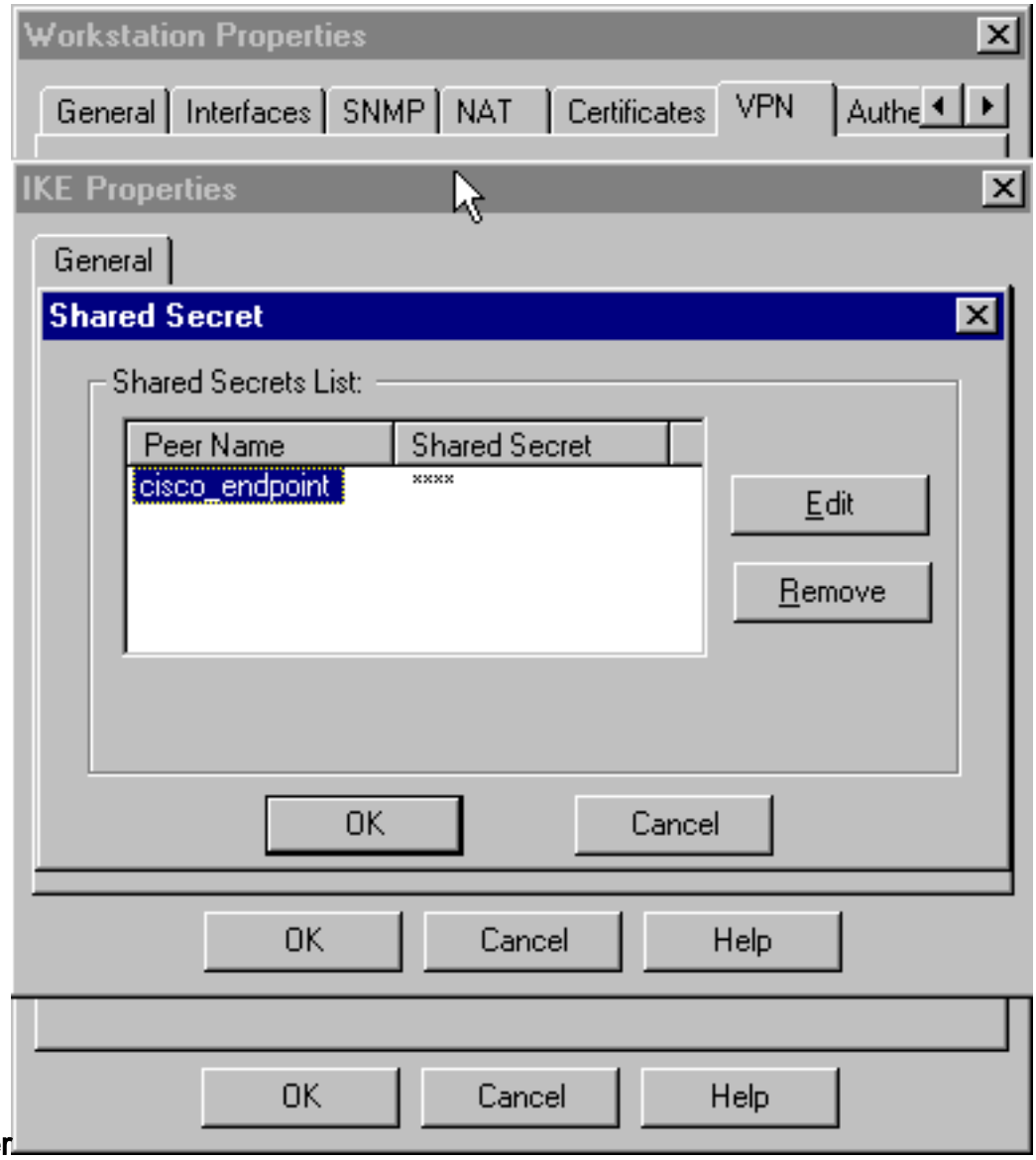
Bewerken.

7. Wijzig de IKE-eigenschappen voor DES-encryptie om met het **DES-56** en het **Encryption Algorithm** op de VPN-centrator akkoord te gaan.
8. Verander de IKE eigenschappen in SHA1 hashing om met het **SHA/HMAC-160** algoritme in de VPN Concentrator in te stemmen.De selectie van de **aggregatieroute** opheffen.Controleer **Ondersteunen subnetten**.Controleer **vooraf gedeeld geheim** onder verificatiemethode. Dit is het eens met de VPN Concentrator Verificatiemodus, PreShared



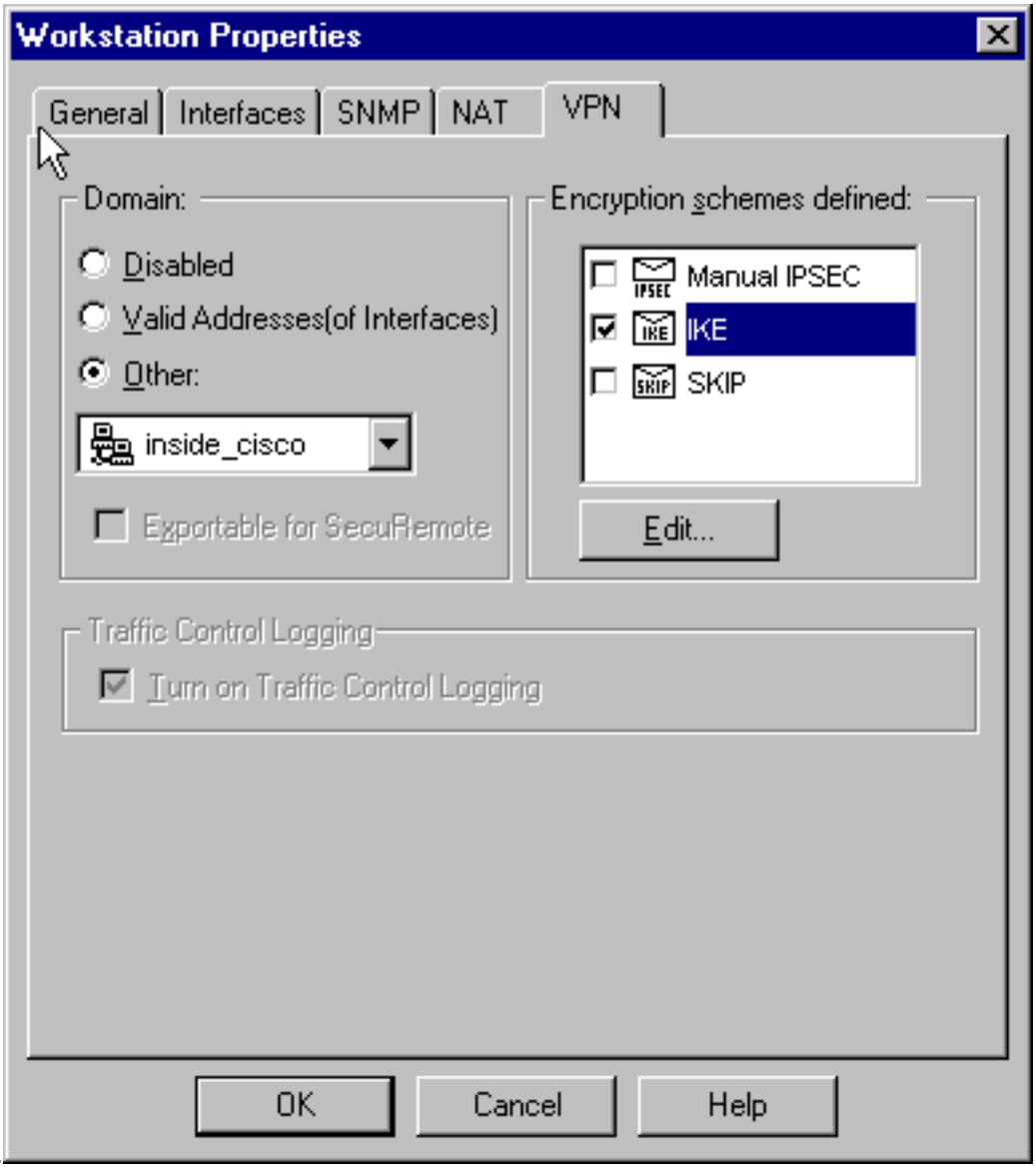
Keys.

9. Klik op **Geheimen bewerken** om de voorgedeelde sleutel in te stellen om met de eigenlijke VPN-**Concentrator PreShared Key** te akkoord te gaan.**isakmp-toets voor**



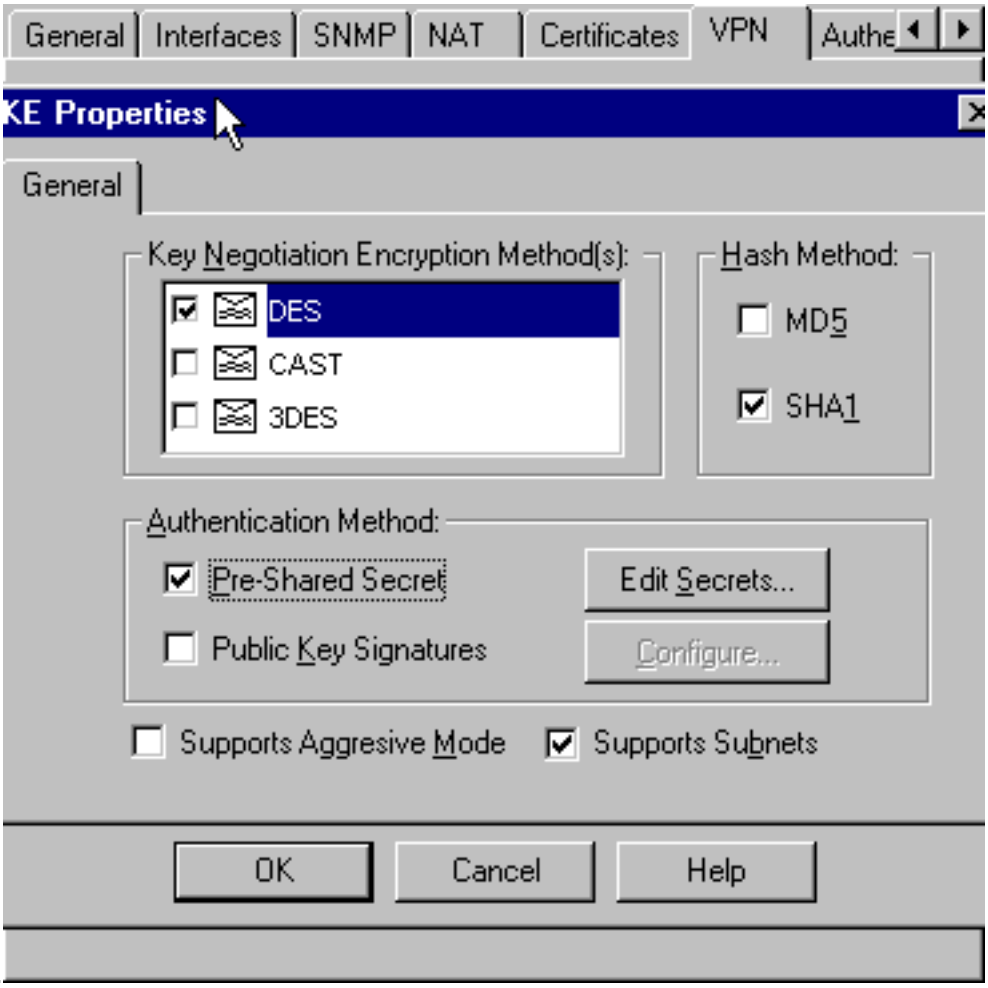
netmasker

10. Selecteer **Manager > Netwerkobjecten > Bewerken** om het tabblad "cisco_end" VPN te bewerken. Selecteer onder Domain, **Andere**, en selecteer dan de binnenkant van het netwerk van Cisco (genoemd "binnenkant_cisco"). Selecteer onder Encryption schemes die worden gedefinieerd **IKE** en klik vervolgens op



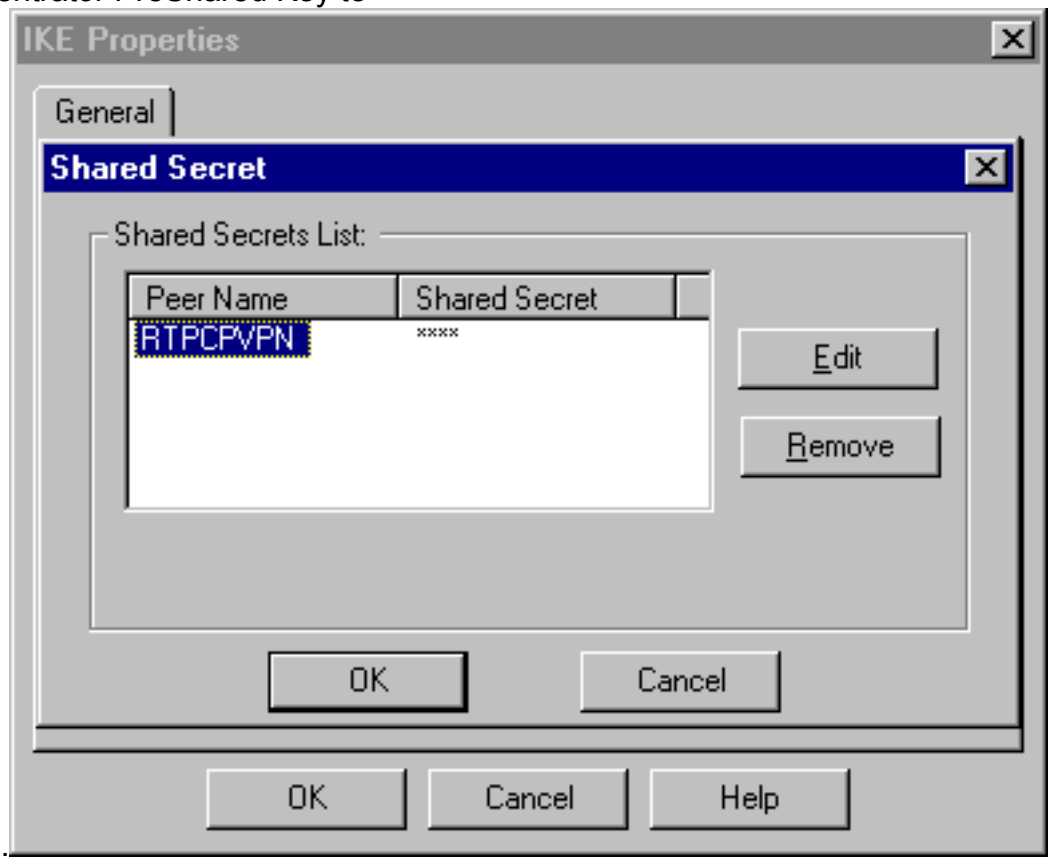
Bewerken.

11. Wijzig de IKE-eigenschappen DES-encryptie om in te stemmen met **DES-56, Encryption Algorithm** op VPN Concentrator.
12. Verander de IKE eigenschappen in SHA1 hashing om met het **SHA/HMAC-160** algoritme in de VPN Concentrator in te stemmen.Wijzig deze instellingen:**Deselecteer de agressieve modus**.Controleer **Ondersteunen subnetten**.Controleer **vooraf gedeeld geheim** onder verificatiemethode. Dit is het eens met de VPN Concentrator Verificatiemodus van



PreShared Keys.

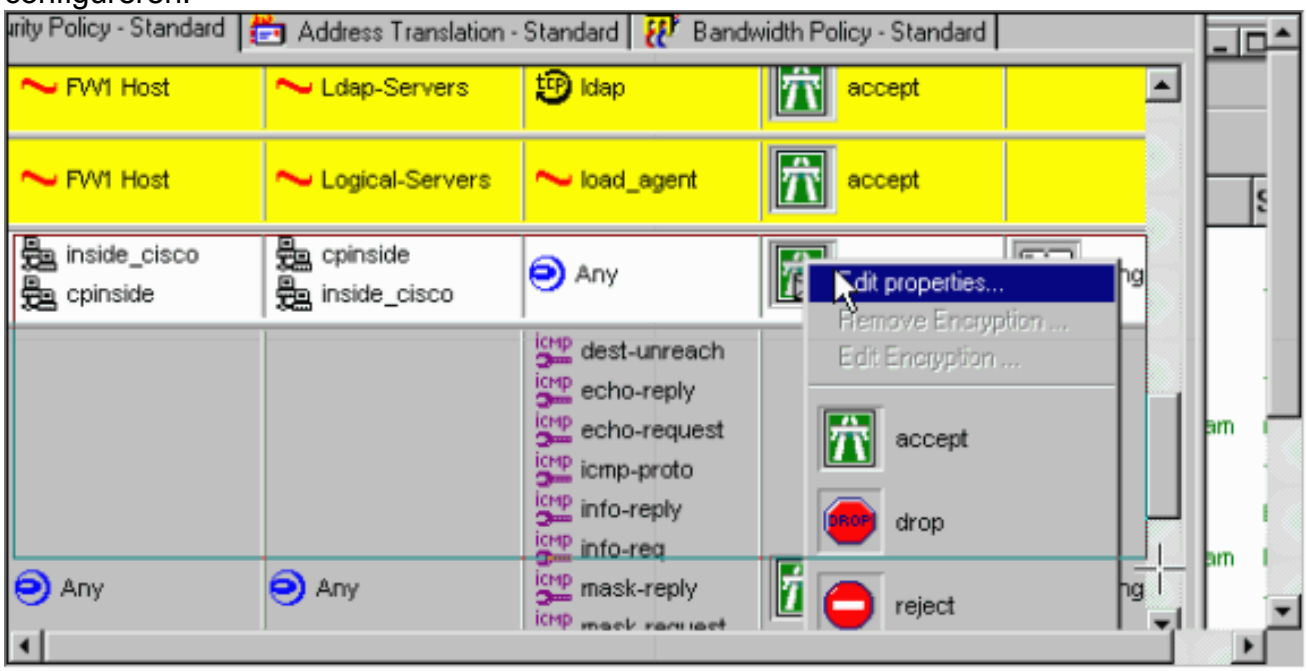
13. Klik op **Geheimen bewerken** om de voorgedeelde toets in te stellen om met de eigenlijke VPN-Concentrator PreShared Key te



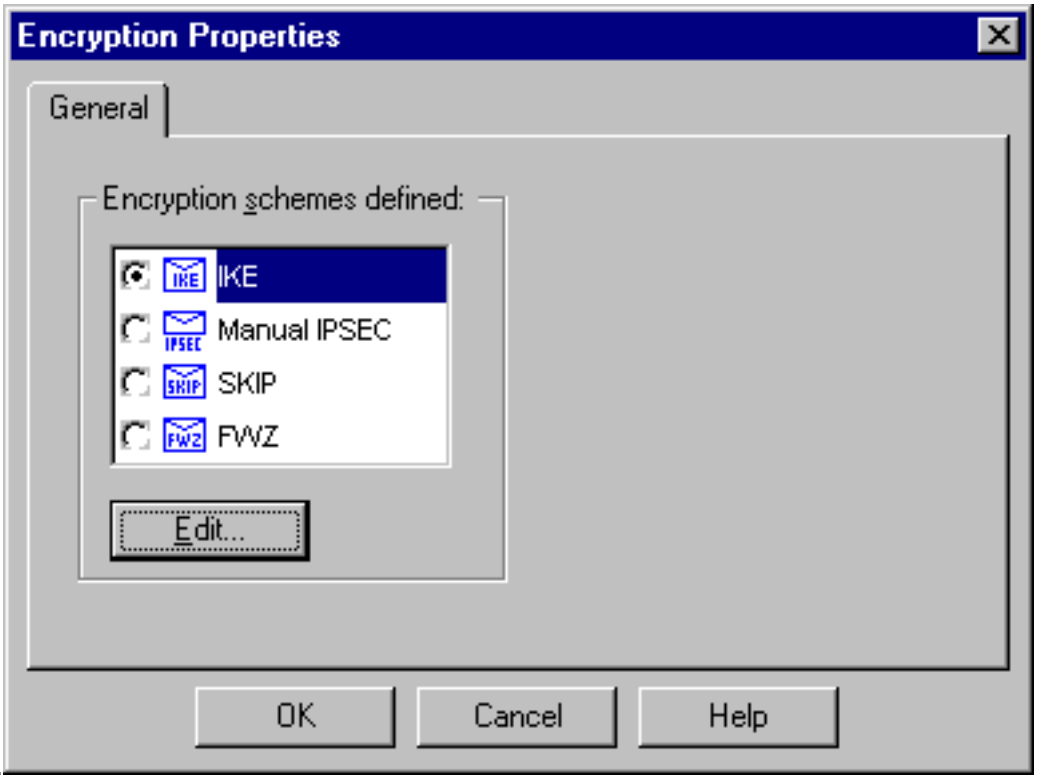
instemmen.

14. Typ in het venster Policy Editor een regel met zowel Bron als Destination als "interne_cisco" en "cpinto" (bidirectioneel). Service=Any, Action=Encrypt en Track=Long instellen.

15. Klik onder het kopje Actie op het pictogram groene **versleuteling** en selecteer **Eigenschappen bewerken** om het coderingsbeleid te configureren.

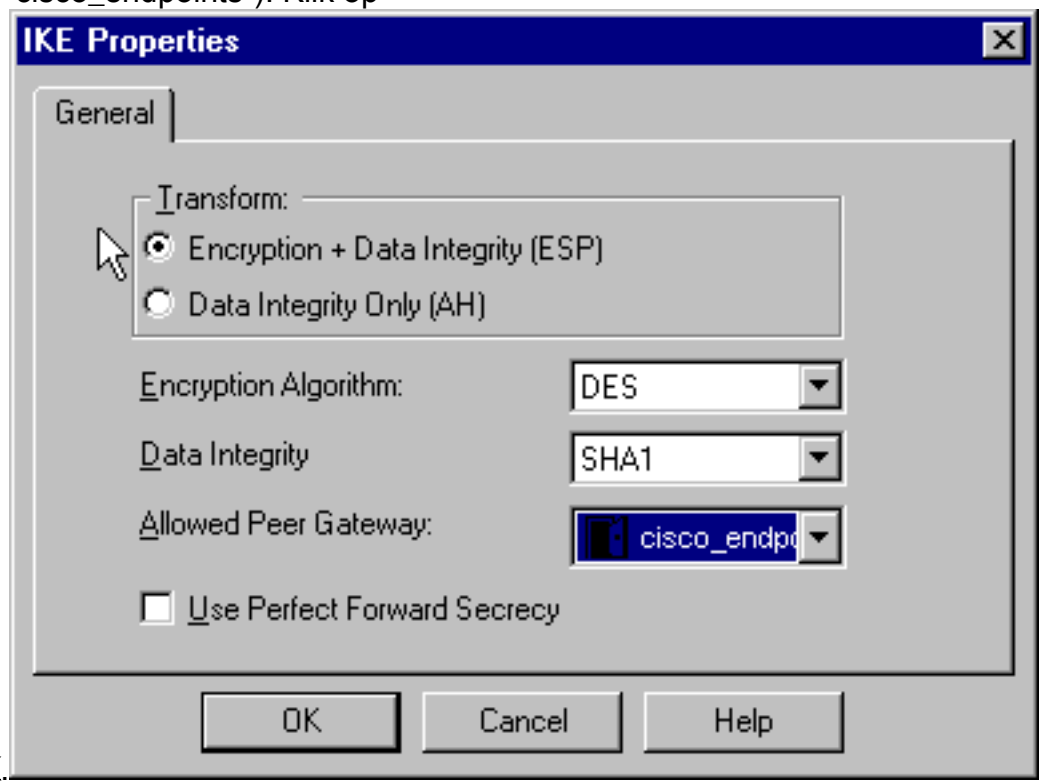


16. Selecteer **IKE** en klik vervolgens op



Bewerken.

17. Wijzig deze eigenschappen in het venster IKE Properties om met de VPN Concentrator IPsec transformaties overeen te komen.Selecteer onder Omzetten de optie **Encryption + Data Integrity (ESP)**. Het Encryption Algorithm moet **DES** zijn, de gegevensintegriteit moet SHA1 zijn en de toegestane peer Gateway moet de externe Cisco-gateway zijn (aangeduid als "cisco_endpoints"). Klik op



OK.

18. Nadat u het selectieteken aanpast, selecteert u **Beleidsbeleid > Installatie** in het menu Selectieteken om de wijzigingen van kracht te laten worden.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

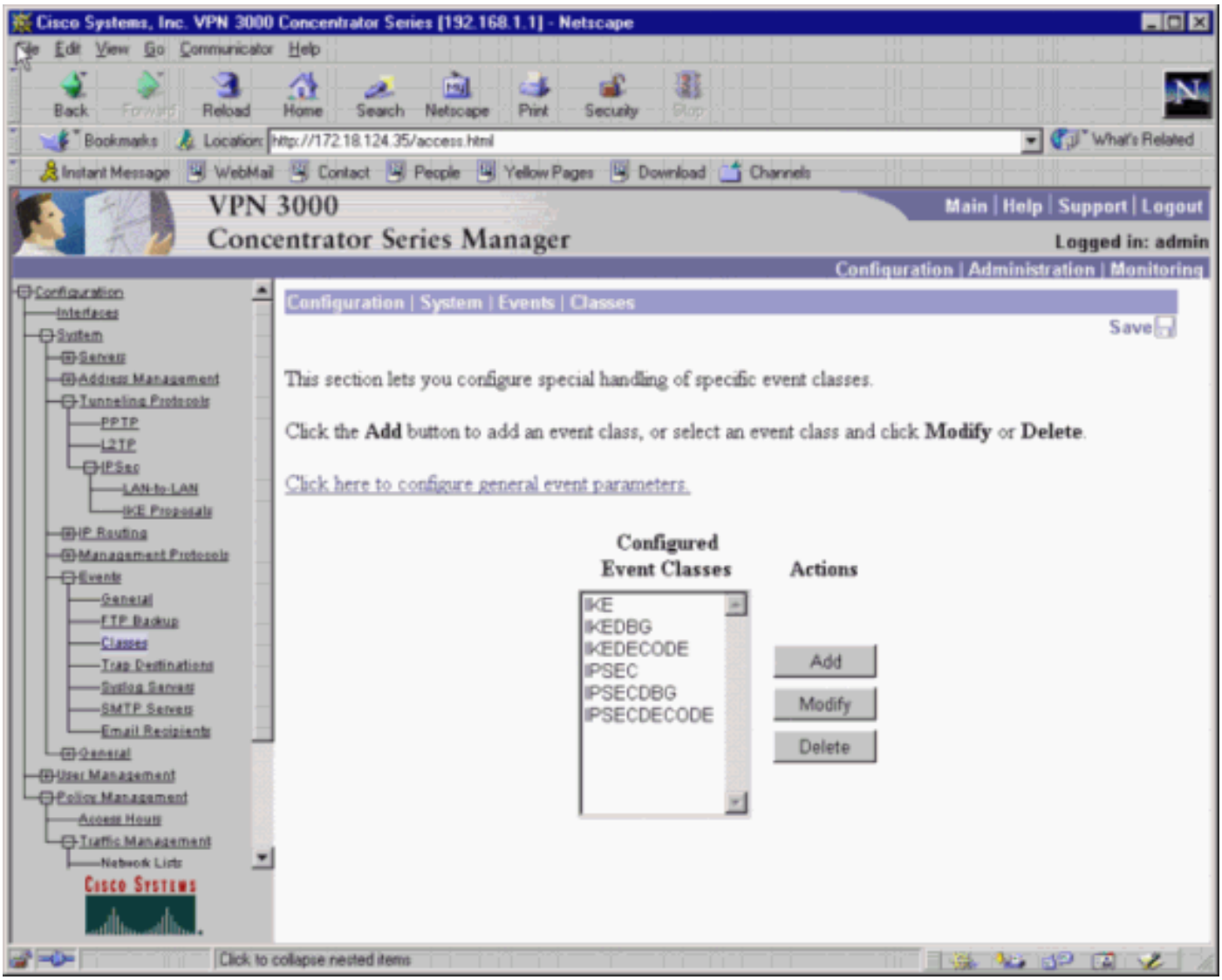
Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

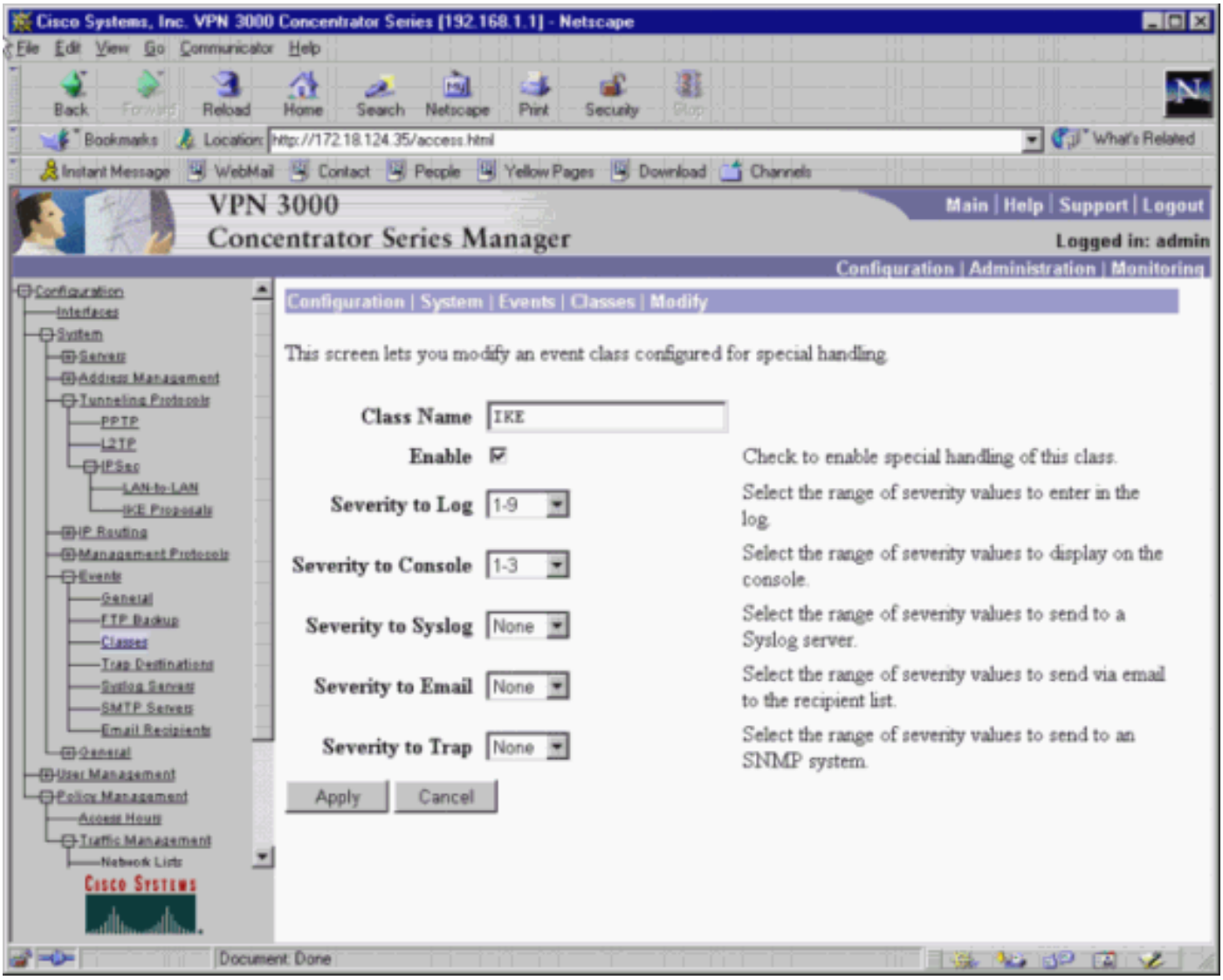
Netwerksamenvatting

Wanneer meerdere aangrenzende interne netwerken zijn geconfigureerd in het encryptiedomein op het Selectieteken, kan het apparaat deze automatisch samenvatten met betrekking tot interessant verkeer. Als de VPN Concentrator niet is geconfigureerd om aan elkaar te koppelen, zal de tunnel waarschijnlijk falen. Als bijvoorbeeld de binnennetwerken van 10.0.0.0/24 en 10.0.1.0/24 zodanig zijn geconfigureerd dat ze in de tunnel worden opgenomen, kunnen ze worden samengevat tot 10.0.0.0/23.

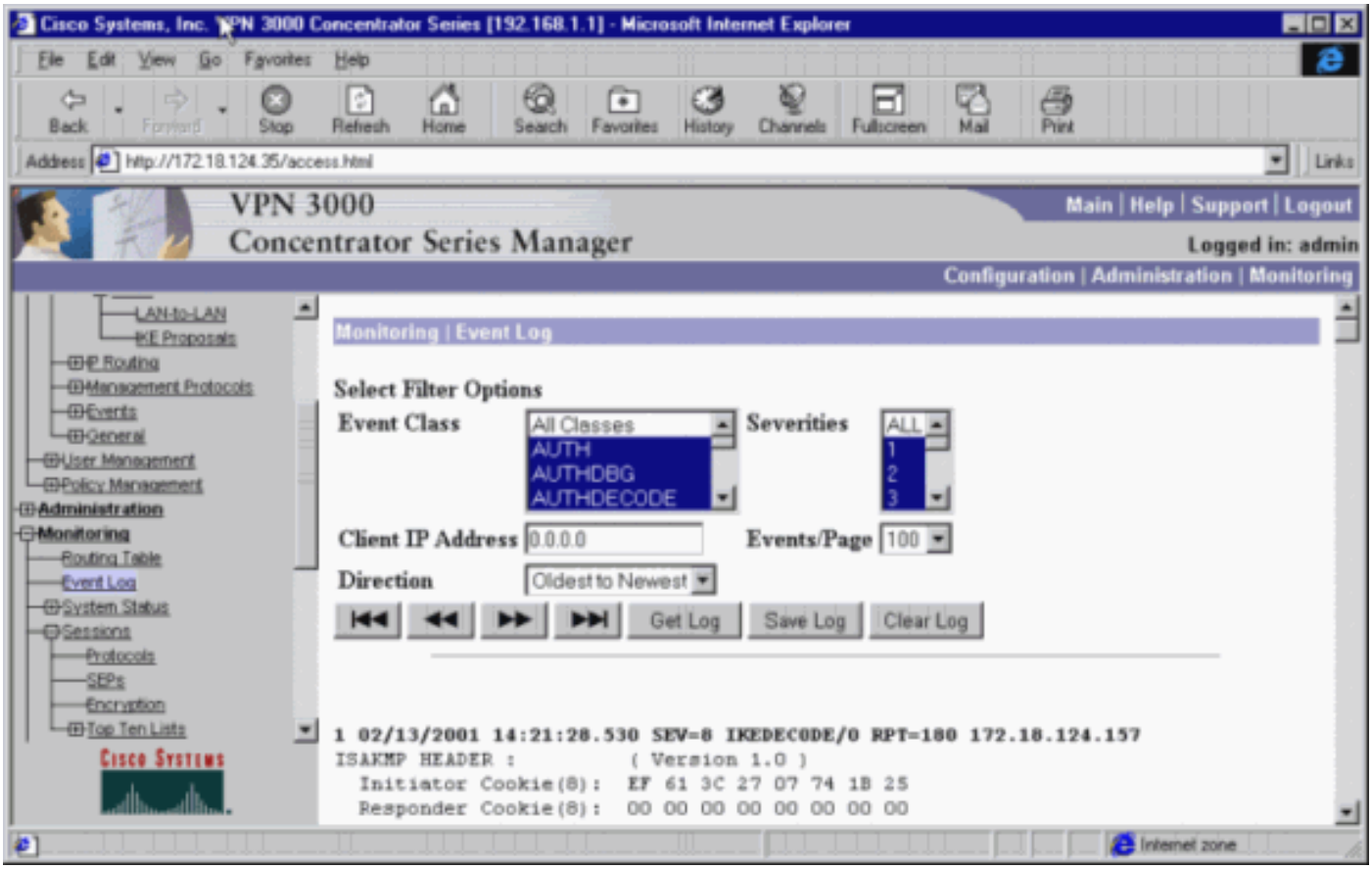
VPN 3000 Concentrator-debug

Mogelijke VPN-concentratordebugs zijn IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE. Dit is ingesteld in **Configuration > System > Events > Classes**.

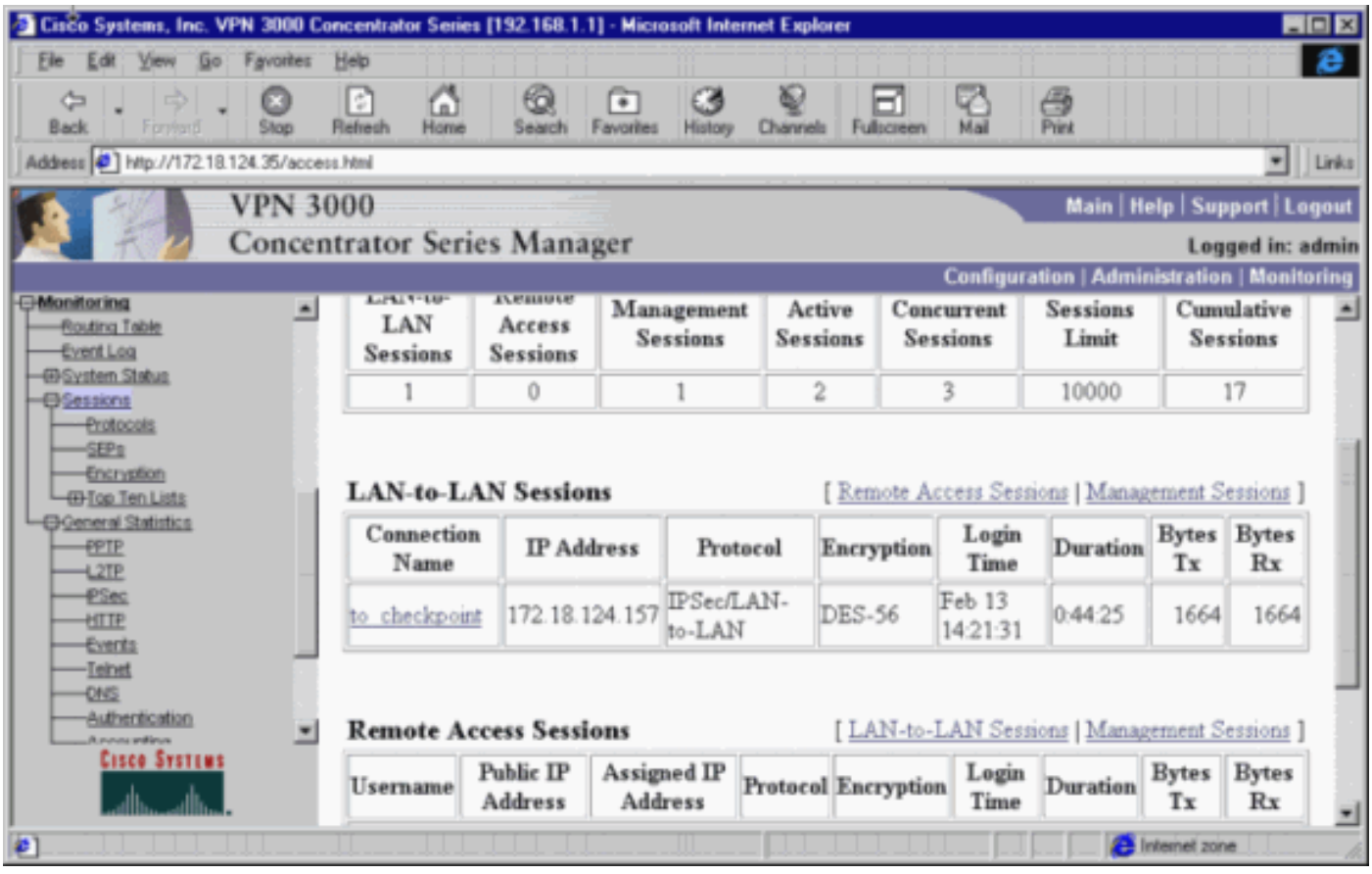




U kunt uiteinden in **bewaking > Event log > Get Log bekijken**.



Selecteer **Monitoring > Sessies** om het LAN-to-LAN tunnelverkeer te bewaken.



Selecteer **Administratie > Sessies beheren > LAN-to-LAN sessies > Handelingen - Uitloggen** om de tunnel te verwijderen.

Checkpoint 4.1 Firewall debug

Opmerking: dit was een Microsoft Windows NT-installatie. Omdat de tracering voor lang is ingesteld in het venster Policy Editor, moet het ontkende verkeer in het logvenster rood verschijnen. U kunt meer breedband debug gebruiken bij:

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

en in een ander venster:

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

Geef deze opdrachten uit om de SA's te wissen op het checkpoint:

```
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
```

Antwoord **ja** op de `Zijn jullie zeker?` .

Voorbeeld van output van foutopsporing

Cisco VPN 3000 Concentrator

```
1 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=180 172.18.124.157
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  00 00 00 00 00 00 00 00
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       164

7 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=406 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 164

9 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=407 172.18.124.157
processing SA payload

10 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=181 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       92

13 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=182 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       2
  Length        :       80
```

```
16 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=183 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       36

18 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=184 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  Auth Method   :       Preshared Key (1)
  DH Group      :       Oakley Group 2 (2)
  Life Time     :       86400 seconds

23 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=185 172.18.124.157
Transform # 2 Decode for Proposal # 1:
  Transform #   :       2
  Transform ID  :       IKE (1)
  Length        :       36

25 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=186 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 2:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  Auth Method   :       Preshared Key (1)
  DH Group      :       Oakley Group 1 (1)
  Life Time     :       86400 seconds

30 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=408 172.18.124.157
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

35 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=409 172.18.124.157
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

38 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=410 172.18.124.157
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

41 02/13/2001 14:21:28.530 SEV=7 IKEDBG/0 RPT=411 172.18.124.157
Oakley proposal is acceptable

42 02/13/2001 14:21:28.530 SEV=9 IKEDBG/1 RPT=107 172.18.124.157
processing vid payload

43 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=412 172.18.124.157
processing IKE SA

44 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=413 172.18.124.157
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
```

```
    Cfg'd: Oakley Group 1

49 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=414 172.18.124.157
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

52 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=415 172.18.124.157
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

55 02/13/2001 14:21:28.530 SEV=7 IKEDBG/28 RPT=3 172.18.124.157
IKE SA Proposal # 1, Transform # 2 acceptable
Matches global IKE entry # 1

56 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=416 172.18.124.157
constructing ISA_SA for isakmp

57 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=417 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1)  ... total length : 84

58 02/13/2001 14:21:28.630 SEV=8 IKEDECODE/0 RPT=187 172.18.124.157
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       KE (4)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       152

64 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=418 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

66 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=419 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

68 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=420 172.18.124.157
processing ke payload

69 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=421 172.18.124.157
processing ISA_KE

70 02/13/2001 14:21:28.630 SEV=9 IKEDBG/1 RPT=108 172.18.124.157
processing nonce payload

71 02/13/2001 14:21:28.650 SEV=9 IKEDBG/0 RPT=422 172.18.124.157
constructing ke payload

72 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=109 172.18.124.157
constructing nonce payload

73 02/13/2001 14:21:28.650 SEV=9 IKEDBG/38 RPT=7 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti
es: 20000001)

75 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=110 172.18.124.157
constructing vid payload
```

```
76 02/13/2001 14:21:28.650 SEV=9 IKE/0 RPT=26 172.18.124.157
Generating keys for Responder...

77 02/13/2001 14:21:28.650 SEV=8 IKEDBG/0 RPT=423 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4)  ... total length : 192

78 02/13/2001 14:21:28.770 SEV=8 IKEDECODE/0 RPT=188 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68

84 02/13/2001 14:21:28.770 SEV=8 IKEDBG/0 RPT=424 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

86 02/13/2001 14:21:28.770 SEV=9 IKEDBG/1 RPT=111 172.18.124.157
Processing ID

87 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=425 172.18.124.157
processing hash

88 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=426 172.18.124.157
computing hash

89 02/13/2001 14:21:28.770 SEV=9 IKEDBG/23 RPT=7 172.18.124.157
Starting group lookup for peer 172.18.124.157

90 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=427 172.18.124.157
Found Phase 1 Group (172.18.124.157)

91 02/13/2001 14:21:28.870 SEV=7 IKEDBG/14 RPT=7 172.18.124.157
Authentication configured for Internal

92 02/13/2001 14:21:28.870 SEV=9 IKEDBG/1 RPT=112 172.18.124.157
constructing ID

93 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=428
construct hash payload

94 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=429 172.18.124.157
computing hash


95 02/13/2001 14:21:28.870 SEV=8 IKEDBG/0 RPT=430 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5)  ... total length : 64

96 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=431 172.18.124.157
Starting phase 1 rekey timer

97 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=189 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
```

```
  Message ID    :       7755aa11
  Length        :       164

104 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=432 172.18.124.157
RECEIVED Message (msgid=7755aa11) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 160

107 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=433 172.18.124.157
processing hash

108 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=434 172.18.124.157
processing SA payload

109 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=190 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       52

112 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=191 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       DA 16 3F E3
  Length        :       40

116 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=192 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
  Length        :       28

118 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=193 172.18.124.157
Phase 2 SA Attribute Decode for Transform # 1:
  Life Time     :       28800 seconds
  HMAC Algorithm:       SHA (2)
  Encapsulation :       Tunnel (1)

121 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=113 172.18.124.157
processing nonce payload

122 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=114 172.18.124.157
Processing ID

123 02/13/2001 14:21:29.030 SEV=5 IKE/35 RPT=14 172.18.124.157
Received remote IP Proxy Subnet data in ID Payload:
 Address 10.32.50.0, Mask 255.255.255.0, Protocol 0, Port 0

125 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=115 172.18.124.157
Processing ID

126 02/13/2001 14:21:29.030 SEV=5 IKE/34 RPT=14 172.18.124.157
Received local IP Proxy Subnet data in ID Payload:
 Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0

128 02/13/2001 14:21:29.030 SEV=5 IKE/66 RPT=4 172.18.124.157
IKE Remote Peer configured for SA: L2L: to_checkpoint

129 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=435 172.18.124.157
processing IPSEC SA

130 02/13/2001 14:21:29.030 SEV=7 IKEDBG/27 RPT=1 172.18.124.157
```

```
IPSec SA Proposal # 1, Transform # 1 acceptable

131 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=436 172.18.124.157
IKE: requesting SPI!

132 02/13/2001 14:21:29.030 SEV=8 IKEDBG/6 RPT=6
IKE got SPI from key engine: SPI = 0x4d6e483f

133 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=437 172.18.124.157
oakley constucting quick mode

134 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=438 172.18.124.157
constructing blank hash

135 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=439 172.18.124.157
constructing ISA_SA for ipsec

136 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=116 172.18.124.157
constructing ipsec nonce payload

137 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=117 172.18.124.157
constructing proxy ID

138 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=440 172.18.124.157
Transmitting Proxy Id:
  Remote subnet: 10.32.50.0  Mask 255.255.255.0 Protocol 0  Port 0
  Local subnet:  192.168.1.0  mask 255.255.255.0 Protocol 0  Port 0

141 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=441 172.18.124.157
constructing qm hash

142 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=442 172.18.124.157
SENDING Message (msgid=7755aa11) with payloads :
HDR + HASH (8)  ... total length : 156

144 02/13/2001 14:21:29.270 SEV=8 IKEDECODE/0 RPT=194 172.18.124.157
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

151 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=443 172.18.124.157
RECEIVED Message (msgid=7755aa11) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 52

153 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=444 172.18.124.157
processing hash

154 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=445 172.18.124.157
loading all IPSEC SAs

155 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=118 172.18.124.157
Generating Quick Mode Key!

156 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=119 172.18.124.157
Generating Quick Mode Key!

157 02/13/2001 14:21:29.270 SEV=7 IKEDBG/0 RPT=446 172.18.124.157
Loading subnet:
  Dst: 192.168.1.0  mask: 255.255.255.0
```

```
  Src: 10.32.50.0  mask: 255.255.255.0

159 02/13/2001 14:21:29.270 SEV=4 IKE/49 RPT=6 172.18.124.157
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x4d6e483f, Outbound SPI = 0xda163fe3

161 02/13/2001 14:21:29.270 SEV=8 IKEDBG/7 RPT=6
IKE got a KEY_ADD msg for SA: SPI = 0xda163fe3

162 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=447
pitcher: rcv KEY_UPDATE, spi 0x4d6e483f

163 02/13/2001 14:21:29.670 SEV=8 IKEDECODE/0 RPT=195 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

170 02/13/2001 14:21:29.670 SEV=6 IKE/0 RPT=27 172.18.124.157
Duplicate Phase 2 packet detected!

171 02/13/2001 14:21:29.760 SEV=8 IKEDECODE/0 RPT=196 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

178 02/13/2001 14:21:29.760 SEV=6 IKE/0 RPT=28 172.18.124.157
Duplicate Phase 2 packet detected!

179 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=448
pitcher: recv KEY_SA_ACTIVE spi 0x4d6e483f

180 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=449
KEY_SA_ACTIVE old rekey centry found with new spi 0x4d6e483f

181 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=5 172.18.124.157
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

182 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=450 172.18.124.157
IKE SA MM:f2ea8e68 rcv'd Terminate: state MM_ACTIVE_REKEY
flags 0x000000e6, refcnt 1, tuncnt 0

184 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=451 172.18.124.157
IKE SA MM:f2ea8e68 terminating:
flags 0x000000a6, refcnt 0, tuncnt 0

185 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=452
sending delete message

186 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=453 172.18.124.157
constructing blank hash

187 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=454
constructing delete payload
```

```
188 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=455 172.18.124.157
constructing qm hash

189 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=456 172.18.124.157
SENDING Message (msgid=87b7c1a4) with payloads :
HDR + HASH (8)  ... total length : 80

191 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=457 172.18.124.157
IKE SA MM:241840a1 rcv'd Terminate: state MM_REKEY_DONE
flags 0x00000082, refcnt 1, tuncnt 1

193 02/13/2001 14:21:29.880 SEV=6 IKE/0 RPT=29 172.18.124.157
Removing peer from peer table failed, no match!

194 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=458
sending delete message

195 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=459 172.18.124.157
constructing blank hash

196 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=460
constructing ipsec delete payload

197 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=461 172.18.124.157
constructing qm hash

198 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=462 172.18.124.157
SENDING Message (msgid=63f2abb8) with payloads :
HDR + HASH (8)  ... total length : 68

200 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=6 172.18.124.157
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

201 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=463 172.18.124.157
IKE SA MM:241840a1 terminating:
flags 0x00000082, refcnt 0, tuncnt 0

202 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=464
sending delete message

203 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=465 172.18.124.157
constructing blank hash

204 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=466
constructing delete payload

205 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=467 172.18.124.157
constructing qm hash

206 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=468 172.18.124.157
SENDING Message (msgid=d6a00071) with payloads :
HDR + HASH (8)  ... total length : 80

208 02/13/2001 14:21:29.880 SEV=4 AUTH/22 RPT=13
User 172.18.124.157 disconnected

209 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=469
pitcher: received key delete msg, spi 0x2962069b

210 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=470
pitcher: received key delete msg, spi 0xda163fe2

211 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=471
pitcher: received key delete msg, spi 0x4d6e483f
```

```
212 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=472
pitcher: received key delete msg, spi 0xda163fe3

213 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=473
pitcher: received a key acquire message!

214 02/13/2001 14:21:29.890 SEV=4 IKE/41 RPT=6 172.18.124.157
IKE Initiator: New Phase 1, Intf 2, IKE Peer 172.18.124.157
local Proxy Address 192.168.1.0, remote Proxy Address 10.32.50.0,
SA (L2L: to_checkpoint)

217 02/13/2001 14:21:29.890 SEV=9 IKEDBG/0 RPT=474 172.18.124.157
constructing ISA_SA for isakmp

218 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=475 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1)  ... total length : 84

219 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=197 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       84

225 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=476 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

227 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=477 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

229 02/13/2001 14:21:30.430 SEV=9 IKEDBG/0 RPT=478 172.18.124.157
processing SA payload

230 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=198 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       56

233 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=199 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       1
  Length        :       44

236 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=200 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       36

238 02/13/2001 14:21:30.440 SEV=8 IKEDECODE/0 RPT=201 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 1 (1)
```

```
  Auth Method   :       Preshared Key (1)
  Life Time     :       86400 seconds

243 02/13/2001 14:21:30.440 SEV=7 IKEDBG/0 RPT=479 172.18.124.157
Oakley proposal is acceptable

244 02/13/2001 14:21:30.440 SEV=9 IKEDBG/0 RPT=480 172.18.124.157
constructing ke payload

245 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=120 172.18.124.157
constructing nonce payload

246 02/13/2001 14:21:30.440 SEV=9 IKEDBG/38 RPT=8 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti
es: 20000001)

248 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=121 172.18.124.157
constructing vid payload

249 02/13/2001 14:21:30.440 SEV=8 IKEDBG/0 RPT=481 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4)  ... total length : 192

250 02/13/2001 14:21:30.540 SEV=8 IKEDECODE/0 RPT=202 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       KE (4)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       152

256 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=482 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

258 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=483 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

260 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=484 172.18.124.157
processing ke payload

261 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=485 172.18.124.157
processing ISA_KE

262 02/13/2001 14:21:30.540 SEV=9 IKEDBG/1 RPT=122 172.18.124.157
processing nonce payload

263 02/13/2001 14:21:30.560 SEV=9 IKE/0 RPT=30 172.18.124.157
Generating keys for Initiator...

264 02/13/2001 14:21:30.570 SEV=9 IKEDBG/1 RPT=123 172.18.124.157
constructing ID

265 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=486
construct hash payload

266 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=487 172.18.124.157
computing hash

267 02/13/2001 14:21:30.570 SEV=8 IKEDBG/0 RPT=488 172.18.124.157
SENDING Message (msgid=0) with payloads :
```

```
HDR + ID (5)  ... total length : 64

268 02/13/2001 14:21:30.740 SEV=8 IKEDECODE/0 RPT=203 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68

274 02/13/2001 14:21:30.740 SEV=8 IKEDBG/0 RPT=489 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

276 02/13/2001 14:21:30.740 SEV=9 IKEDBG/1 RPT=124 172.18.124.157
Processing ID

277 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=490 172.18.124.157
processing hash

278 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=491 172.18.124.157
computing hash

279 02/13/2001 14:21:30.740 SEV=9 IKEDBG/23 RPT=8 172.18.124.157
Starting group lookup for peer 172.18.124.157

280 02/13/2001 14:21:30.830 SEV=8 IKEDECODE/0 RPT=204 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68

286 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=31 172.18.124.157
Duplicate Phase 1 packet detected!

287 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=32
MM received unexpected event EV_RESEND_MSG in state MM_I_DONE

288 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=492 172.18.124.157
Found Phase 1 Group (172.18.124.157)

289 02/13/2001 14:21:30.840 SEV=7 IKEDBG/14 RPT=8 172.18.124.157
Authentication configured for Internal

290 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=493 172.18.124.157
Oakley begin quick mode

291 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=494 172.18.124.157
Starting phase 1 rekey timer

292 02/13/2001 14:21:30.840 SEV=4 AUTH/21 RPT=15
User 172.18.124.157 connected

293 02/13/2001 14:21:30.840 SEV=8 IKEDBG/6 RPT=7
IKE got SPI from key engine: SPI = 0x08201539

294 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=495 172.18.124.157
oakley constucting quick mode
```

```
295 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=496 172.18.124.157
constructing blank hash

296 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=497 172.18.124.157
constructing ISA_SA for ipsec

297 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=125 172.18.124.157
constructing ipsec nonce payload

298 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=126 172.18.124.157
constructing proxy ID

299 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=498 172.18.124.157
Transmitting Proxy Id:
  Local subnet:  192.168.1.0  mask 255.255.255.0 Protocol 0  Port 0
  Remote subnet: 10.32.50.0  Mask 255.255.255.0 Protocol 0  Port 0

302 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=499 172.18.124.157
constructing qm hash

303 02/13/2001 14:21:30.840 SEV=8 IKEDBG/0 RPT=500 172.18.124.157
SENDING Message (msgid=23bc1709) with payloads :
HDR + HASH (8)  ... total length : 184

305 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=205 172.18.124.157
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       23bc1709
  Length        :       164

312 02/13/2001 14:21:31.000 SEV=8 IKEDBG/0 RPT=501 172.18.124.157
RECEIVED Message (msgid=23bc1709) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 156

315 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=502 172.18.124.157
processing hash

316 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=503 172.18.124.157
processing SA payload

317 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=206 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       48

320 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=207 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       DA 16 3F E4
  Length        :       36

324 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=208 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
```

```
  Length        :       24

326 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=209 172.18.124.157
Phase 2 SA Attribute Decode for Transform # 1:
  Life Time     :       28800 seconds
  Encapsulation :       Tunnel (1)
  HMAC Algorithm:       SHA (2)

329 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=127 172.18.124.157
processing nonce payload

330 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=128 172.18.124.157
Processing ID

331 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=129 172.18.124.157
Processing ID

332 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=504 172.18.124.157
loading all IPSEC SAs

333 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=130 172.18.124.157
Generating Quick Mode Key!

334 02/13/2001 14:21:31.010 SEV=9 IKEDBG/1 RPT=131 172.18.124.157
Generating Quick Mode Key!

335 02/13/2001 14:21:31.010 SEV=7 IKEDBG/0 RPT=505 172.18.124.157
Loading subnet:
  Dst: 10.32.50.0  mask: 255.255.255.0
  Src: 192.168.1.0  mask: 255.255.255.0

337 02/13/2001 14:21:31.010 SEV=4 IKE/49 RPT=7 172.18.124.157
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Initiator, Inbound SPI = 0x08201539, Outbound SPI = 0xda163fe4

339 02/13/2001 14:21:31.010 SEV=9 IKEDBG/0 RPT=506 172.18.124.157
oakley constructing final quick mode

340 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=507 172.18.124.157
SENDING Message (msgid=23bc1709) with payloads :
HDR + HASH (8)  ... total length : 76

342 02/13/2001 14:21:31.010 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0xda163fe4

343 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=508
pitcher: rcv KEY_UPDATE, spi 0x8201539

344 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=509
pitcher: recv KEY_SA_ACTIVE spi 0x8201539

345 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=510
KEY_SA_ACTIVE no old rekey centry found with new spi 0x8201539, mess_id 0x0
```

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems