Configuring an IPSec Tunnel Between a Cisco Router and a Checkpoint NG

Document ID: 23784

Contents

Introduction

This document demonstrates how to form an IPSec tunnel with pre−shared keys to join two private networks:

- The 172.16.15.x private network inside the router.
- The 192.168.10.x private network inside the Checkpoint™ Next Generation (NG).

Prerequisites

Requirements

The procedures outlined in this document are based on these assumptions.

- The Checkpoint™ NG basic policy is set up.
- All access, Network Address Translation (NAT), and routing setups are configured.
- Traffic from inside the router and inside the Checkpoint™ NG to the Internet flows.

Components Used

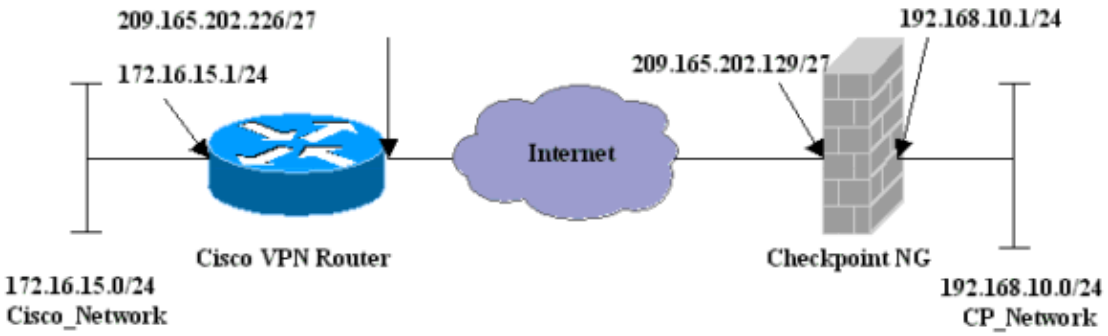
The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup:



Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Configure the Cisco 1751 VPN Router

Cisco VPN 1751 Router

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100

!--- Internet Key Exchange (IKE) configuration.

crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
  lifetime 1800

!--- IPSec configuration.

crypto isakmp key aptrules address 209.165.202.129
!
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
!
crypto map aptmap 1 ipsec-isakmp
  set peer 209.165.202.129
  set transform-set aptset
  match address 110
!
interface Ethernet0/0
  ip address 209.165.202.226 255.255.255.224
```

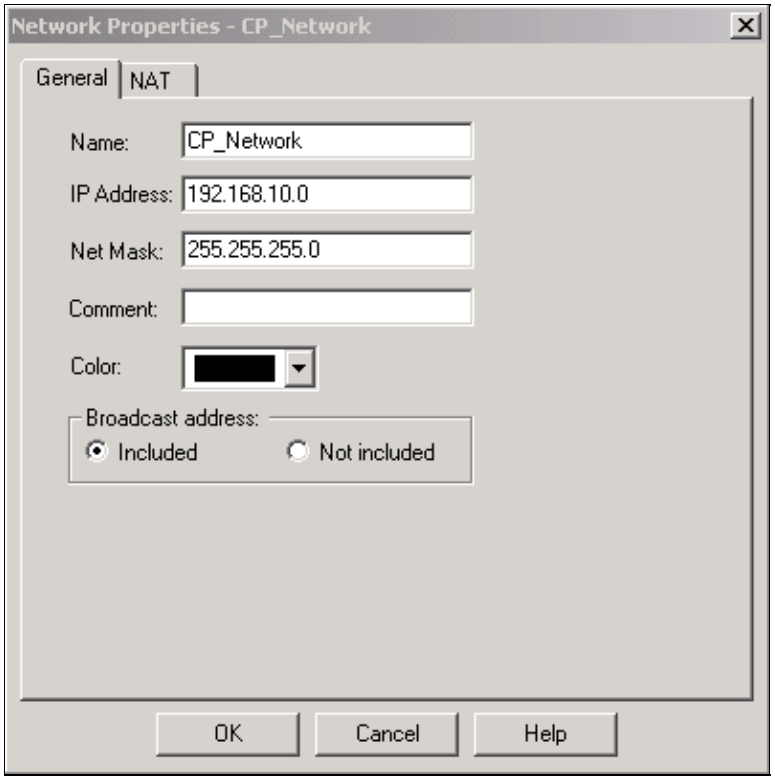
```
  ip nat outside
  half-duplex
  crypto map aptmap
!
interface FastEthernet0/0
  ip address 172.16.15.1 255.255.255.0
  ip nat inside
  speed auto

!--- NAT configuration.

ip nat inside source route-map nonat interface Ethernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.225
no ip http server
ip pim bidir-enable

!--- Encryption match address access list.

access-list 110 permit ip 172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255

!--- NAT access list.

access-list 120 deny ip 172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10
  match ip address 120
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password cisco
 login
end
```

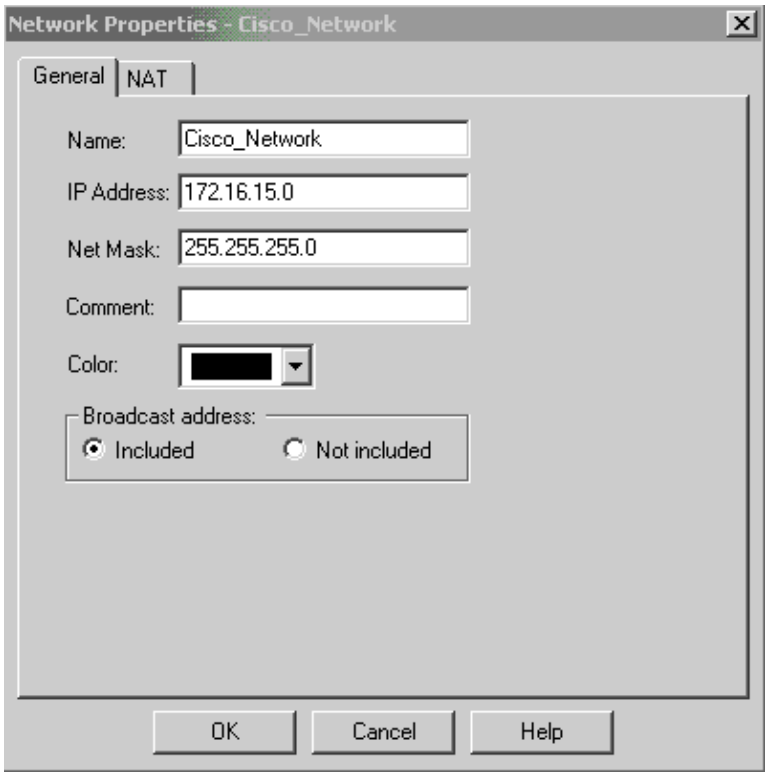
Configure the Checkpoint NG

The Checkpoint™ NG is an object−oriented configuration. Network objects and rules are defined to make up the policy that pertains to the VPN configuration to be set up. This policy is then installed using the Checkpoint™ NG Policy Editor to complete the Checkpoint™ NG side of the VPN configuration.

1. Create Cisco network subnet and Checkpoint™ NG network subnet as network objects. This is what is encrypted. To create the objects, select **Manage > Network Objects**, then select **New > Network**. Enter the appropriate network information, then click **OK**.

   These examples show a set up of objects called CP_Network and Cisco_Network.

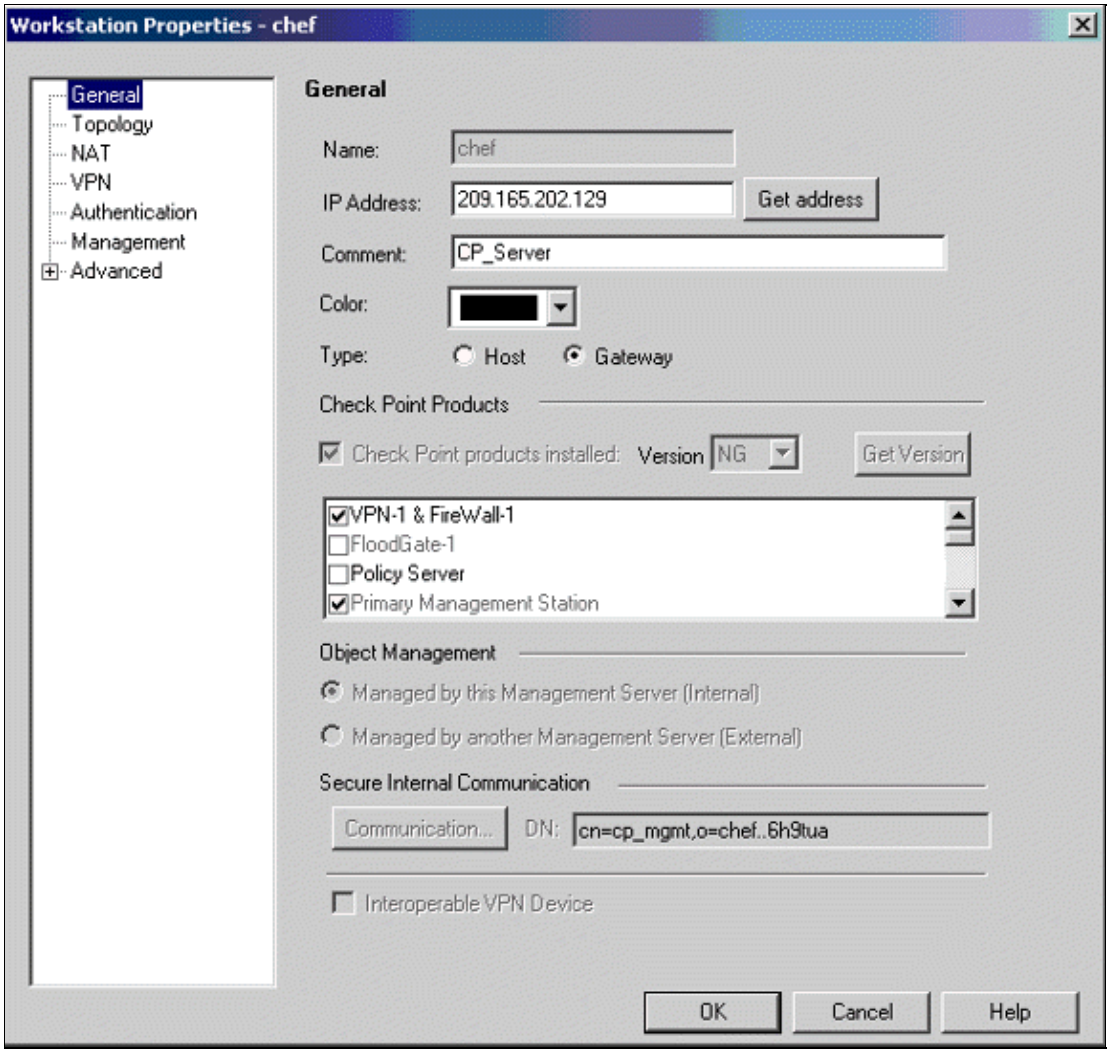


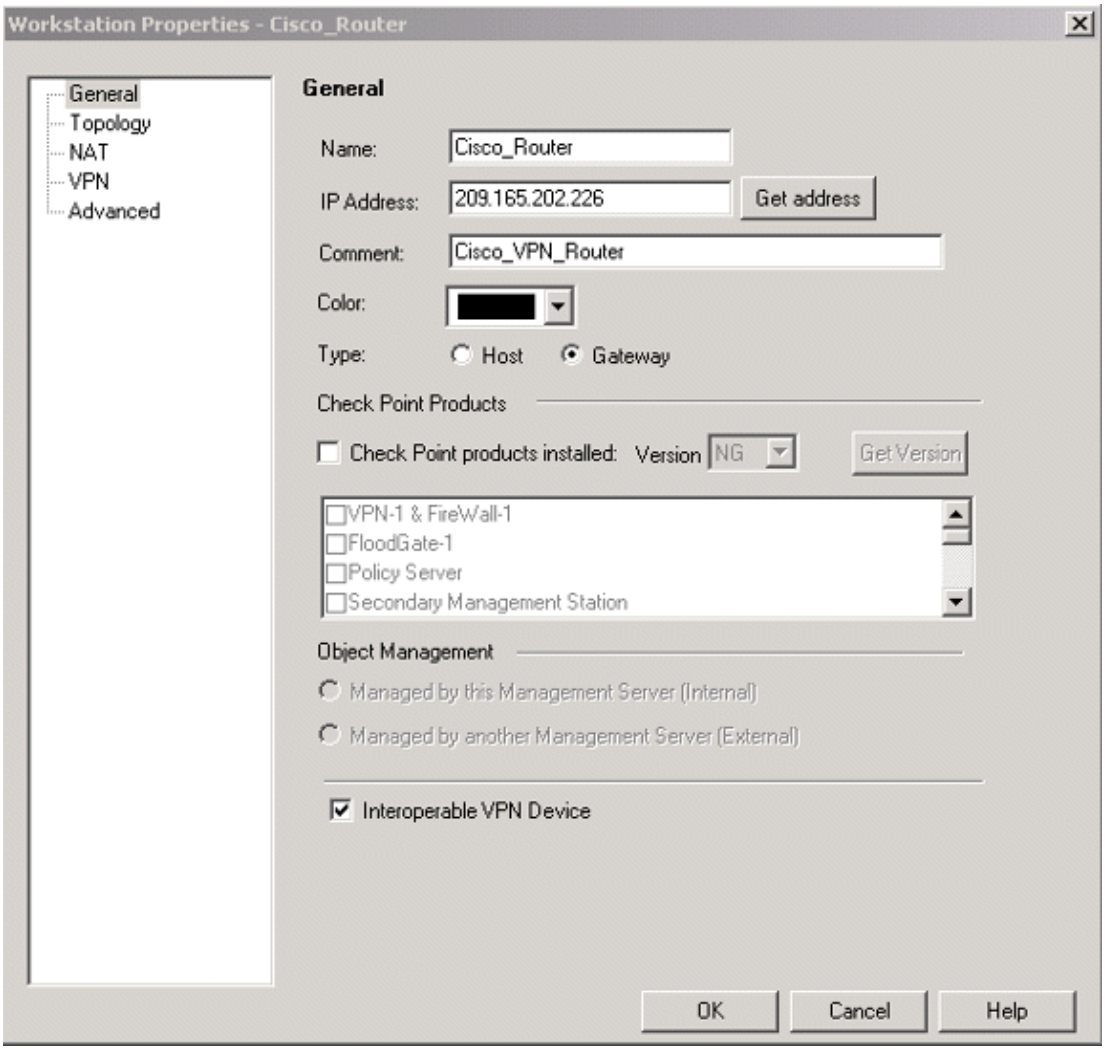


2. Create the Cisco_Router and Checkpoint_NG objects as workstation objects. These are the VPN devices. To create the objects, select **Manage > Network Objects**, then select **New > Workstation**.

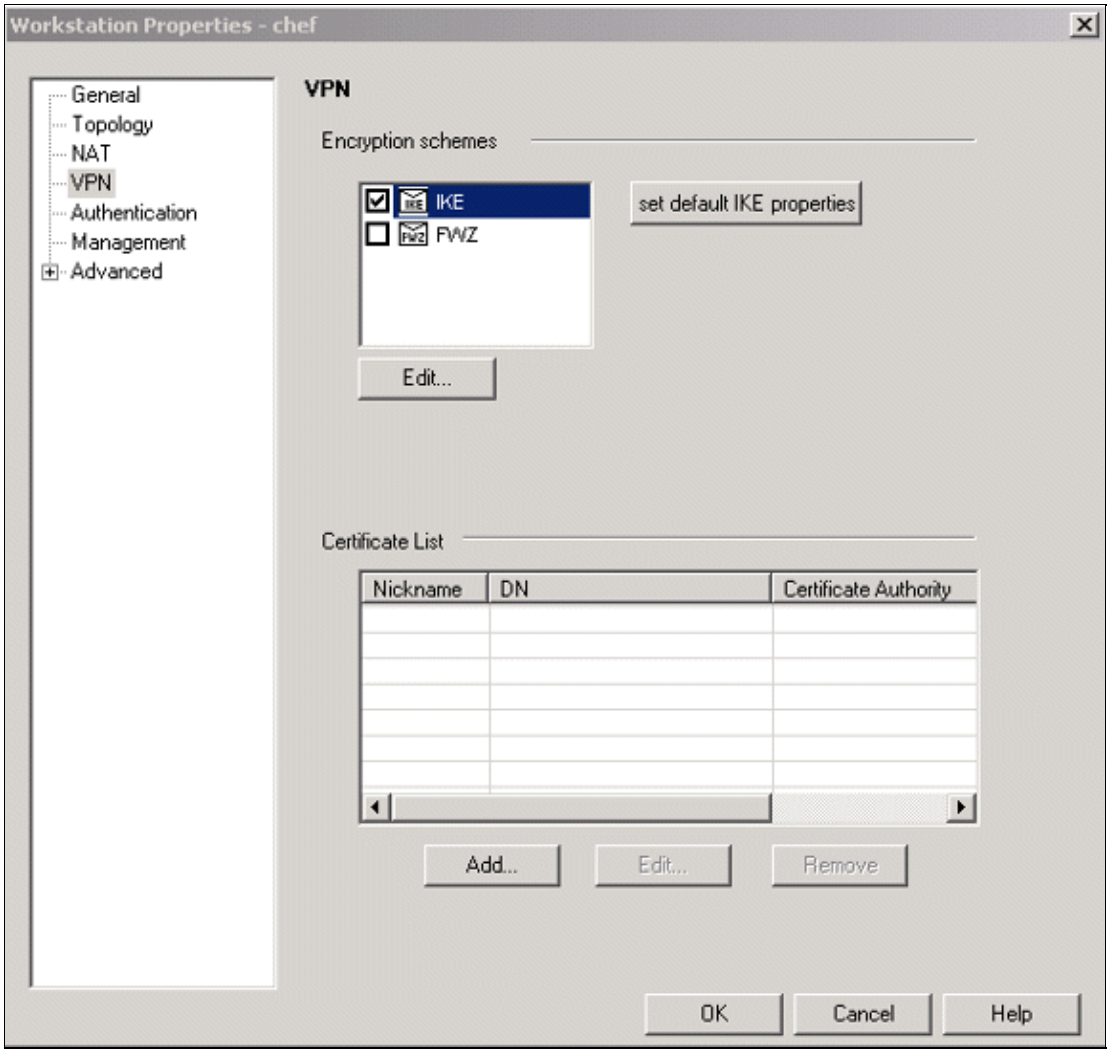
   Note that you can use the Checkpoint™ NG workstation object created during initial Checkpoint™ NG setup. Select the options to set the workstation as **Gateway** and **Interoperable VPN Device**.

   These examples show a set up of objects called chef and Cisco_Router.

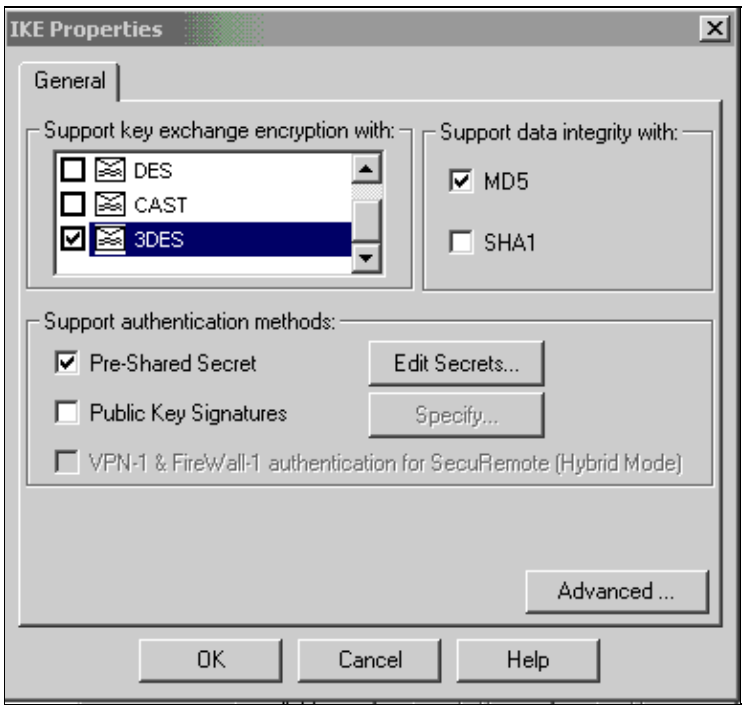

Workstation Properties - chef
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
chef
IP Address:
209.165.202.129
Get address
Comment:
CP_Server
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=chef..6h9tua
Interoperable VPN Device
OK
Cancel
Help



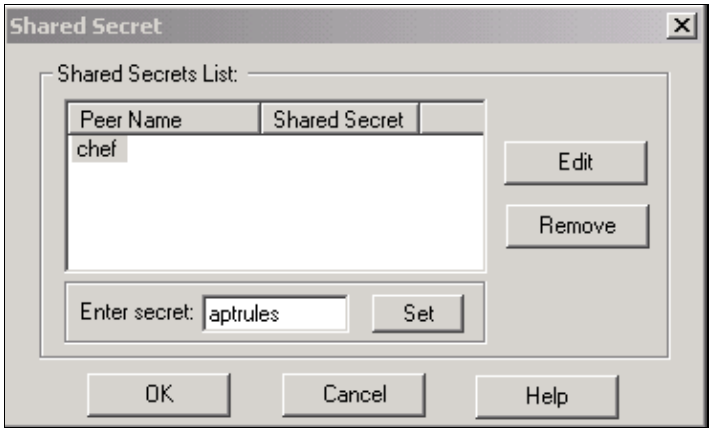
3. Configure the IKE on the VPN tab, then click **Edit**.



4. Configure the key exchange policy, and click **Edit Secrets**.

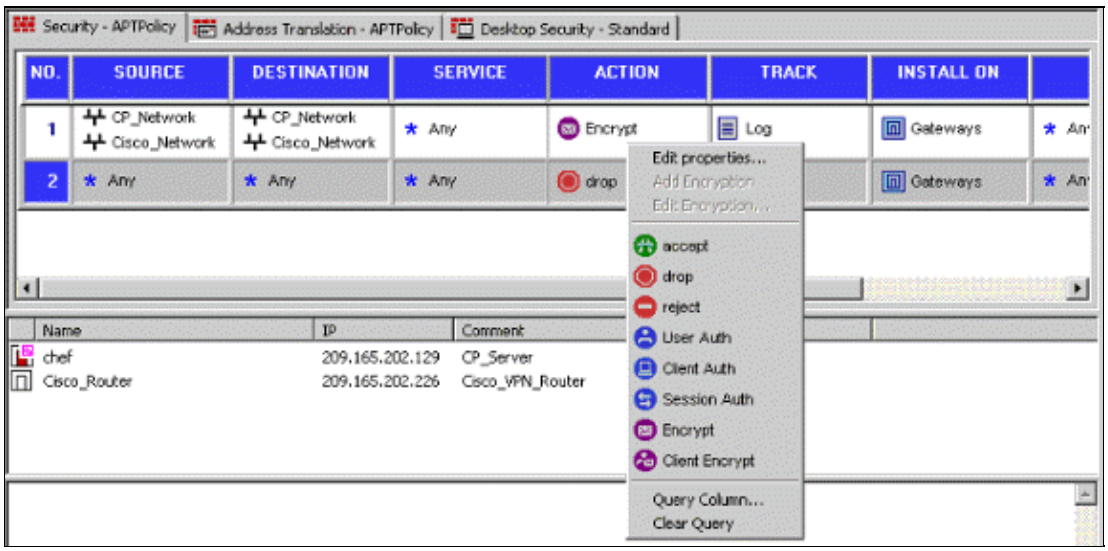


5. Set the pre−shared keys to be used, then click **OK** several times until the configuration windows disappear.

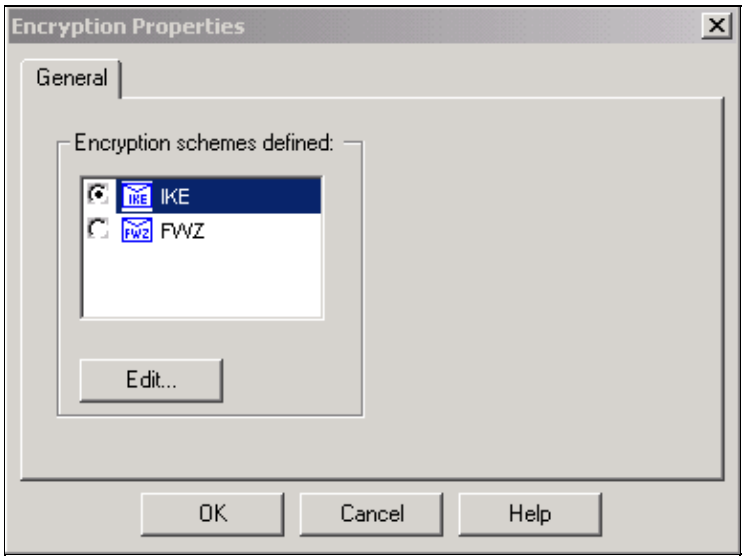


6. Select **Rules > Add Rules > Top** to configure the encryption rules for the policy.

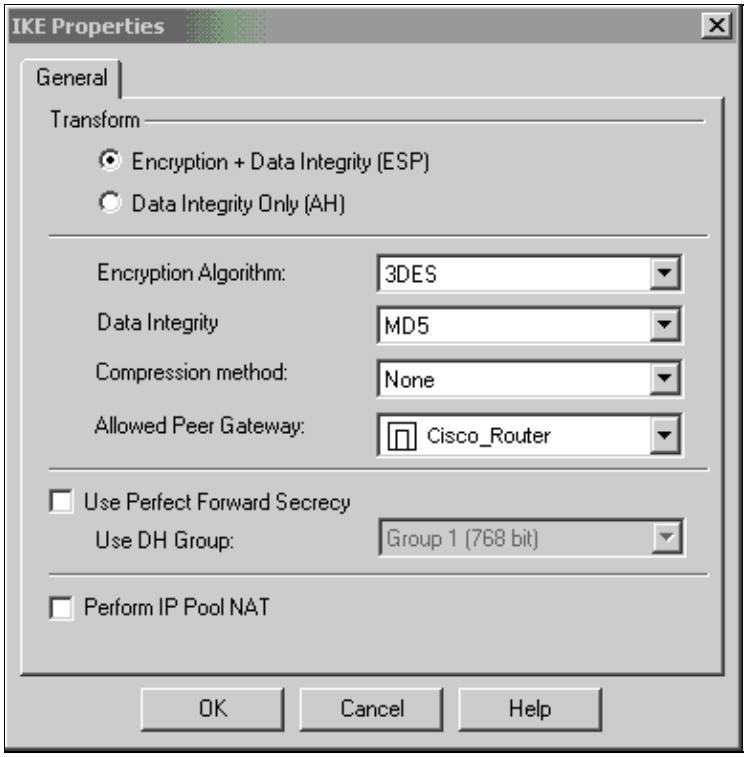
   The rule on the top is the first rule performed before any other rule that may bypass encryption. Configure the Source and Destination to include the CP_Network and the Cisco_Network, as shown here. Once you have added the Encrypt Action section of the rule, right−click **Action** and select **Edit Properties**.



7. With IKE selected and highlighted, click **Edit**.



8. Confirm the IKE configuration.



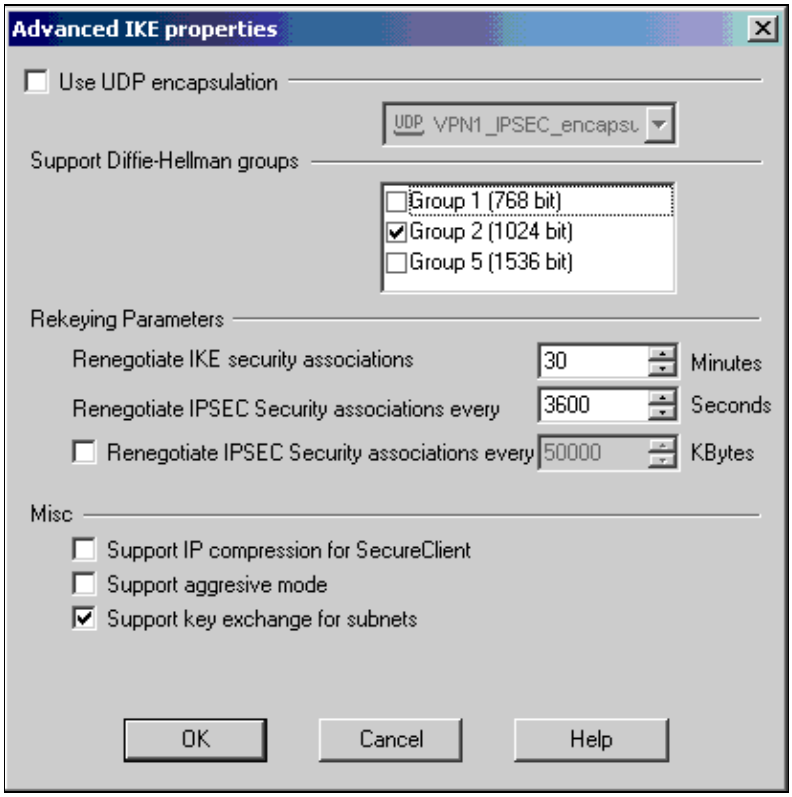
9. One of the main issues with running VPN between Cisco devices and other IPSec devices is the Key Exchange Renegotiation. Ensure that the setting for the IKE exchange on the Cisco router is exactly the same as that configured on the Checkpoint™ NG.

   Note: The actual value of this parameter is dependent on your particular corporate security policy.

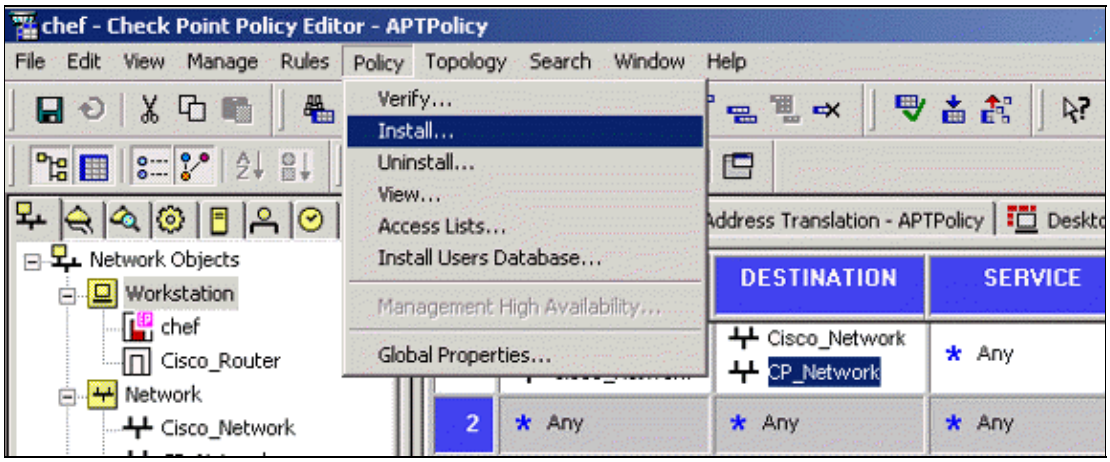
   In this example, the IKE configuration on the router has been set to 30 minutes with the **lifetime 1800** command. The same value has to be set on the Checkpoint™ NG.

   To set this value on the Checkpoint™ NG, select **Manage Network Object**, then select the Checkpoint™ NG object and click **Edit**. Then select **VPN**, and edit the IKE. Select **Advance** and configure the Rekeying Parameters. After you configure the key exchange for the Checkpoint™ NG network object, perform the same configuration of the Key Exchange Renegotiation for the Cisco_Router network object.

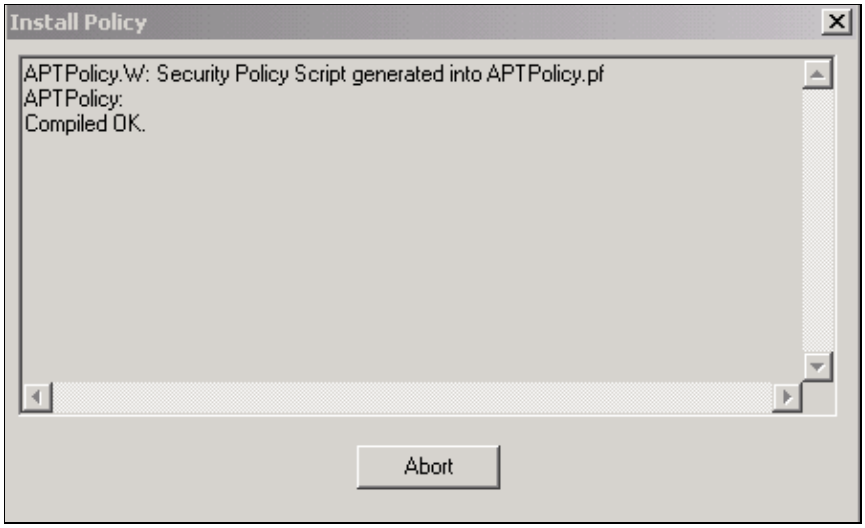
   Note: Ensure that you have the correct Diffie−Hellman group selected to match that configured on the router.



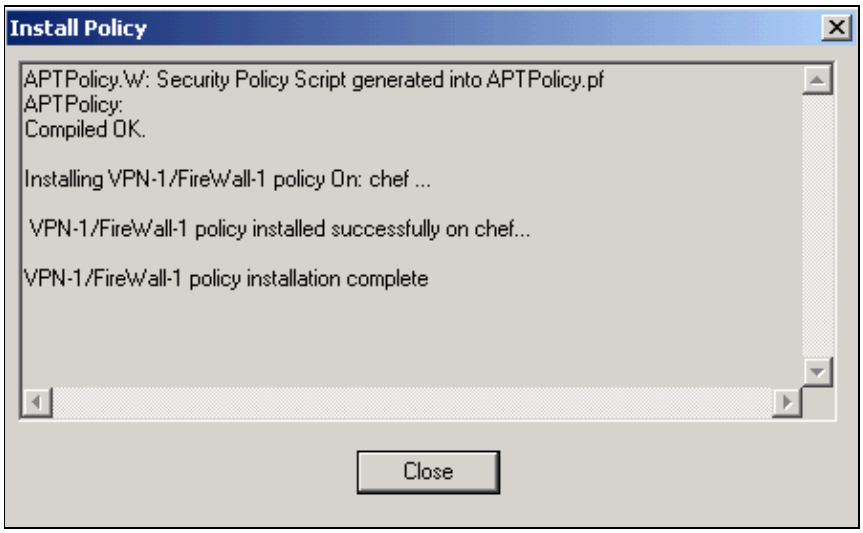
10. The policy configuration is complete. Save the policy and select **Policy > Install** to enable it.



The installation window displays progress notes as the policy is compiled.



When the installation window indicates that the policy installation is complete, click **Close** to finish the procedure.



Verify

This section provides information you can use to confirm your configuration is working properly.

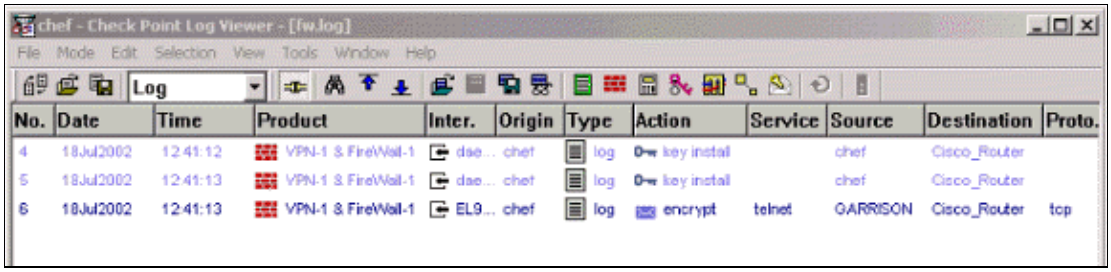
Verify the Cisco Router

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

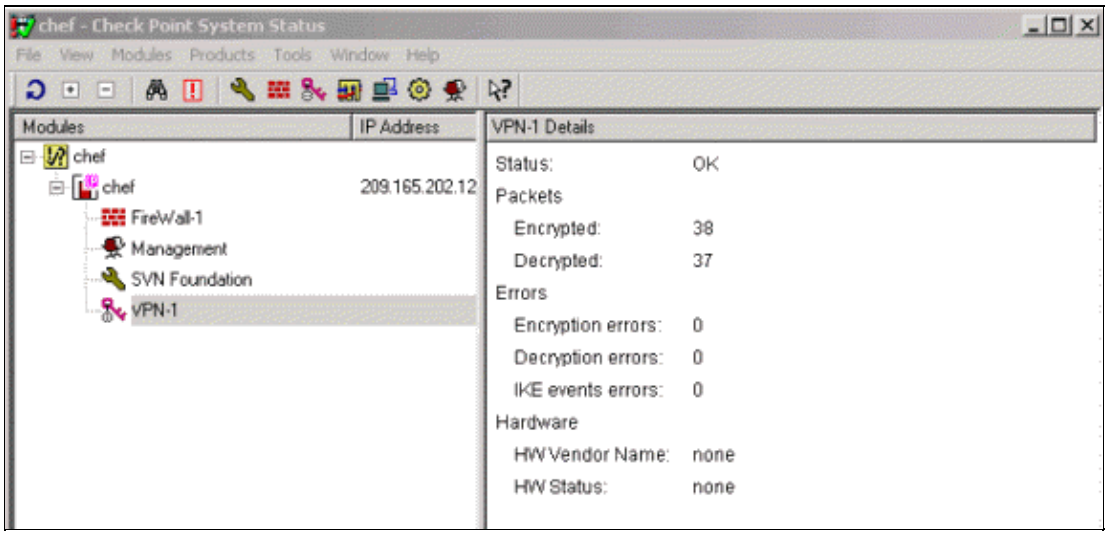
- **show crypto isakmp sa** Displays all current IKE security associations (SAs) at a peer.
- **show crypto ipsec sa** Displays the settings used by current SAs.

Verify Checkpoint NG

To view the logs, select **Window > Log Viewer**.



To view the system status, select **Window > System Status**.



Troubleshoot

Cisco Router

This section provides information you can use to troubleshoot your configuration.

For additional troubleshooting information, please refer to IP Security Troubleshooting − Understanding and Using debug Commands.

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

- **debug crypto engine** Displays debug messages about crypto engines, which perform encryption and decryption.
- **debug crypto isakmp** Displays messages about IKE events.
- **debug crypto ipsec** Displays IPSec events.
- **clear crypto isakmp** Clears all active IKE connections.
- **clear crypto sa** Clears all IPSec SAs.

Successful debug Log Output

```
18:05:32: ISAKMP (0:0): received packet from
   209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
```

```
   but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
   against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
   message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
   with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
```

```
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE
   New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   QM_IDLE
18:05:33: ISAKMP (0:1): processing HASH payload.
   message ID = −1335371103
18:05:33: ISAKMP (0:1): processing SA payload.
   message ID = −1335371103
18:05:33: ISAKMP (0:1): Checking IPSec proposal 1
18:05:33: ISAKMP: transform 1, ESP_3DES
18:05:33: ISAKMP: attributes in transform:
18:05:33: ISAKMP: SA life type in seconds
18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10
18:05:33: ISAKMP: authenticator is HMAC−MD5
18:05:33: ISAKMP: encaps is 1
18:05:33: ISAKMP (0:1): atts are acceptable.
18:05:33: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp−3des esp−md5−hmac ,
   lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
18:05:33: ISAKMP (0:1): processing NONCE payload.
   message ID = −1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = −1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = −1335371103
18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec
18:05:33: ISAKMP (0:1): Node −1335371103,
   Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA
from 209.165.202.226 to 209.165.202.129 for prot 3
18:05:33: ISAKMP: received ke message (2/1)
18:05:33: ISAKMP (0:1): sending packet to
   209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Node −1335371103,
   Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
18:05:33: ISAKMP (0:1): received packet
   from 209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Creating IPSec SAs
18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226
   (proxy 192.168.10.0 to 172.16.15.0)
18:05:33: has spi 0x800022D3 and conn_id 200 and flags 4
18:05:33: lifetime of 3600 seconds
18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129
   (proxy 172.16.15.0 to 192.168.10.0 )
18:05:33: has spi −2006413528 and conn_id 201 and flags C
18:05:33: lifetime of 3600 seconds
18:05:33: ISAKMP (0:1): deleting node −1335371103 error
   FALSE reason "quick mode done (await()"
18:05:33: ISAKMP (0:1): Node −1335371103, Input = IKE_MESG_FROM_PEER,
   IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(initialize_sas): ,
```

```
(key eng. msg.) INBOUND local= 209.165.202.226,
   remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
   lifedur= 3600s and 0kb,
spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0,
   flags= 0x4
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 209.165.202.226,
   remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
   lifedur= 3600s and 0kb,



spi= 0x88688F28(2288553768), conn_id= 201, keysize= 0,
   flags= 0xC
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.226, sa_prot= 50,
sa_spi= 0x800022D3(2147492563),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.129, sa_prot= 50,
sa_spi= 0x88688F28(2288553768),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201
18:05:34: ISAKMP (0:1): received packet
   from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
   of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
   node marked dead -1335371103
18:05:34: ISAKMP (0:1): received packet
   from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
   of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
   node marked dead -1335371103

sv1-6#show crypto isakmp sa
dst src state conn-id slot
209.165.202.226 209.165.202.129 QM_IDLE 1 0

sv1-6#show crypto ipsec sa
interface: Ethernet0/0
Crypto map tag: aptmap, local addr. 209.165.202.226
local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 209.165.202.129
PERMIT, flags={origin_is_acl,}
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 209.165.202.226, remote crypto endpt.: 209.165.202.129
path mtu 1500, media mtu 1500
current outbound spi: 88688F28
inbound esp sas:
spi: 0x800022D3(2147492563)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
```

```
slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3559)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x88688F28(2288553768)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3550)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:

sv1-6#show crypto engine conn act
ID Interface IP-                Address State Algorithm  Encrypt  Decrypt
1 Ethernet0/0 209.165.202.226    set HMAC_MD5+3DES_56_C      0        0
200 Ethernet0/0 209.165.202.226  set HMAC_MD5+3DES_56_C      0        24
201 Ethernet0/0 209.165.202.226  set HMAC_MD5+3DES_56_C      21       0
```

Related Information

- **IPSec Support Page**
- **Technical Support − Cisco Systems**

Updated: Jan 14, 2008 Document ID: 23784