Configuring an IPsec Tunnel − Cisco Router to Checkpoint Firewall 4.1

Document ID: 5463

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configure
Network Diagram
Configurations
Verify
Troubleshoot
Troubleshooting Commands
Network Summarization
Checkpoint
Sample debug Output
Related Information

Introduction

This document demonstrates how to form an IPsec tunnel with pre−shared keys to join two private networks: the 192.168.1.x private network inside the Cisco router and the 10.32.50.x private network inside the Checkpoint Firewall.

Prerequisites

Requirements

This sample configuration assumes that traffic from inside the router and inside the Checkpoint to the Internet (represented here by the 172.18.124.x networks) flows before you start the configuration.

Components Used

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

- Cisco 3600 router
- Cisco IOS® Software (C3640−JO3S56I−M), Release 12.1(5)T, RELEASE SOFTWARE (fc1)
- Checkpoint Firewall 4.1

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.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

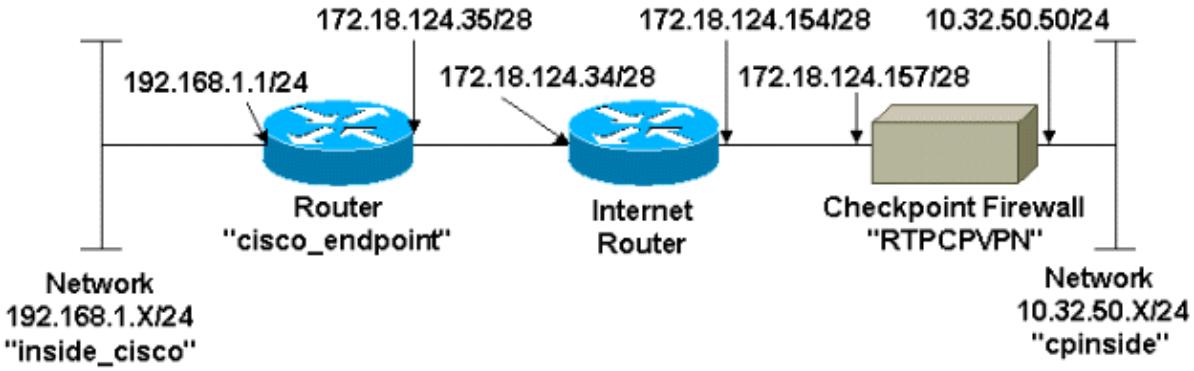
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations.

- Router Configuration
- Checkpoint Firewall Configuration

Router Configuration

Cisco 3600 Router Configuration

```
Current configuration : 1608 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
```

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

crypto isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!

!--- IPsec configuration

crypto ipsec transform-set rtpset esp-des esp-sha-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
!
controller T1 1/0
!
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.255.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask 255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Checkpoint Firewall Configuration

Complete these steps to configure the Checkpoint Firewall.

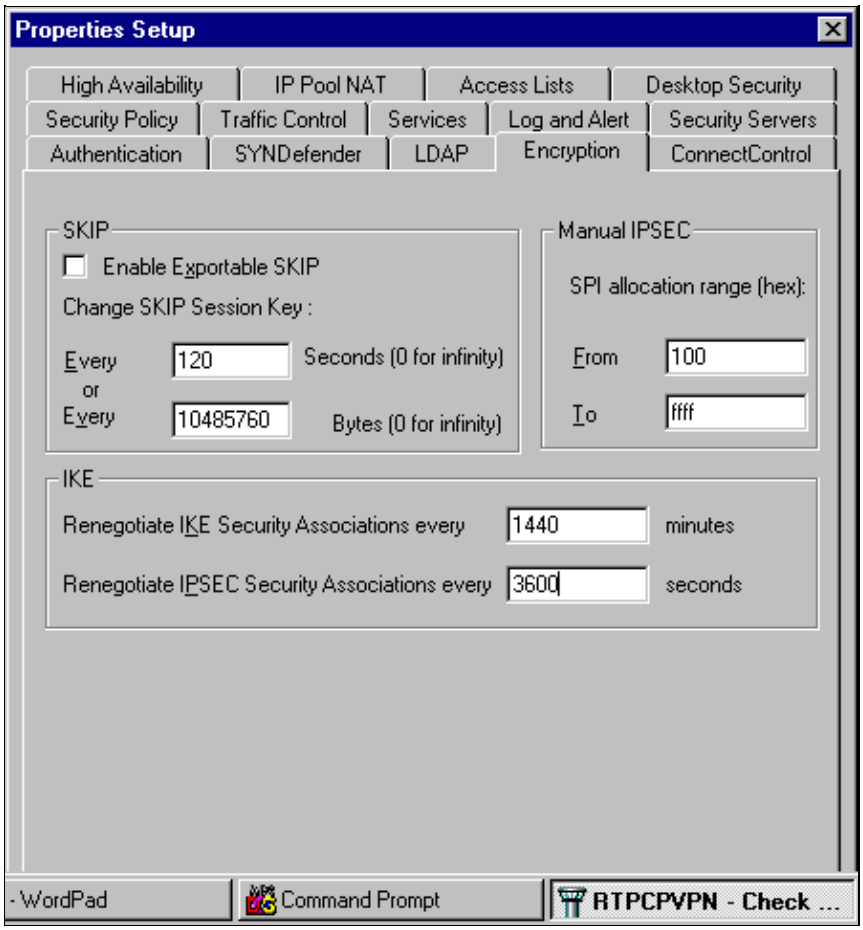
1. Since the IKE and IPsec default lifetimes differ between vendors, select **Properties > Encryption** to set the Checkpoint lifetimes to agree with the Cisco defaults.

   The Cisco default IKE lifetime is 86400 seconds (= 1440 minutes), and it can be modified by these commands:

   - **crypto isakmp policy #**
   - **lifetime #**

   The configurable Cisco IKE lifetime is from 60−86400 seconds. The Cisco default IPsec lifetime is 3600 seconds, and it can be modified by the **crypto ipsec security−association lifetime seconds #** command.

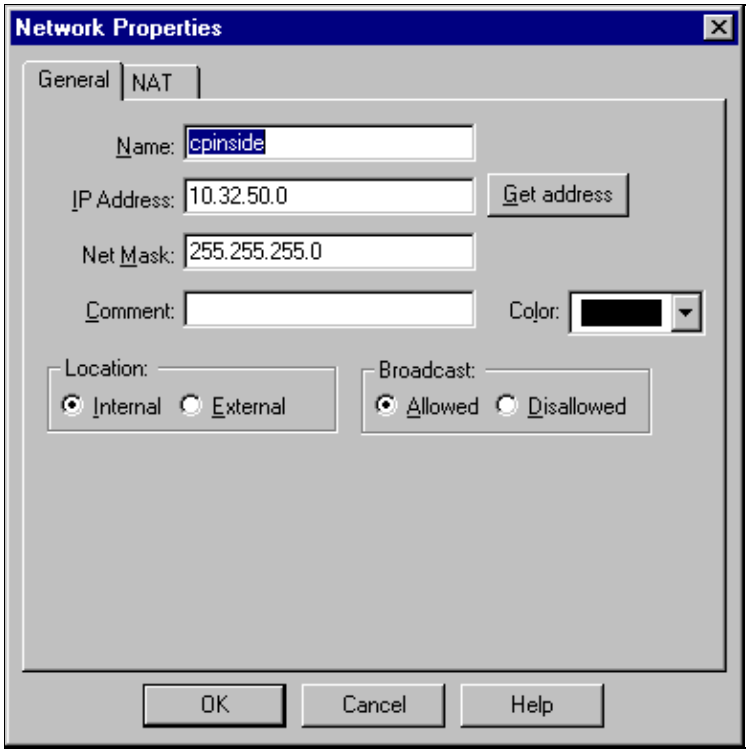
   The configurable Cisco IPsec lifetime is from 120−86400 seconds.



2. Select **Manage > Network objects > New (or Edit) > Network** to configure the object for the internal network (called "cpinside") behind the Checkpoint.

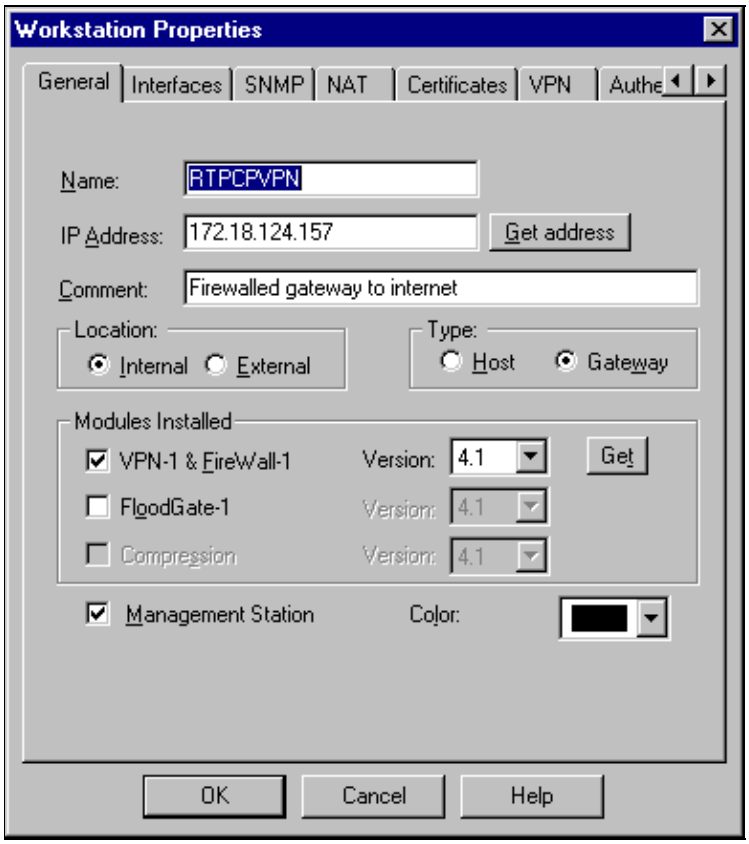
   This should agree with the destination (second) network in the Cisco **access−list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255** command.

   Select **Internal** under Location.



3. Select **Manage > Network objects > Edit** to edit the object for the RTPCPVPN Checkpoint (gateway) endpoint that the Cisco router points to in the **set peer 172.18.124.157** command.

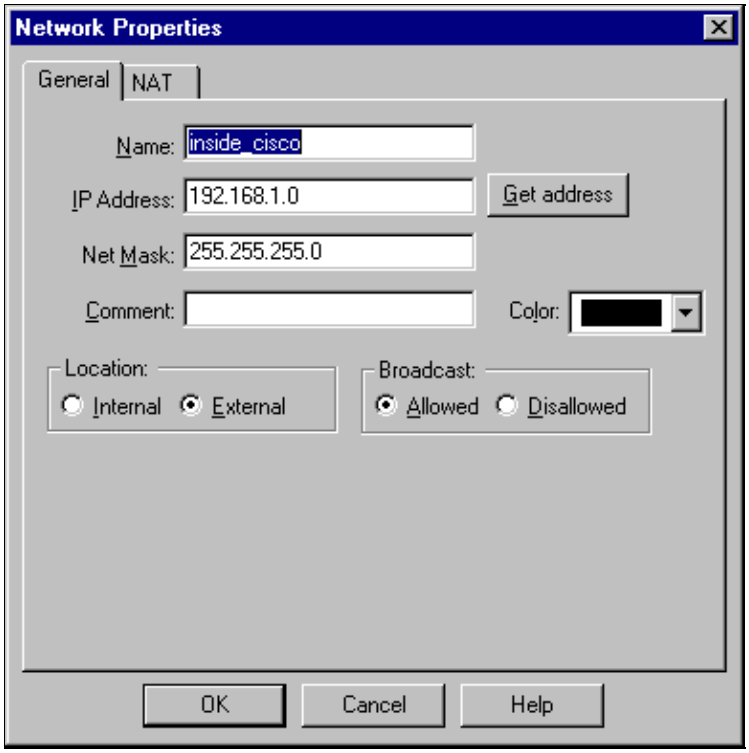
   Select **Internal** under Location. For Type, select **Gateway**. Under Modules Installed, select the **VPN−1 & FireWall−1** check box, and also select the **Management Station** check box:



4. Select **Manage > Network objects > New > Network** to configure the object for the external network (called "inside_cisco") behind the Cisco router.

This should agree with the source (first) network in the Cisco **access−list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255** command.

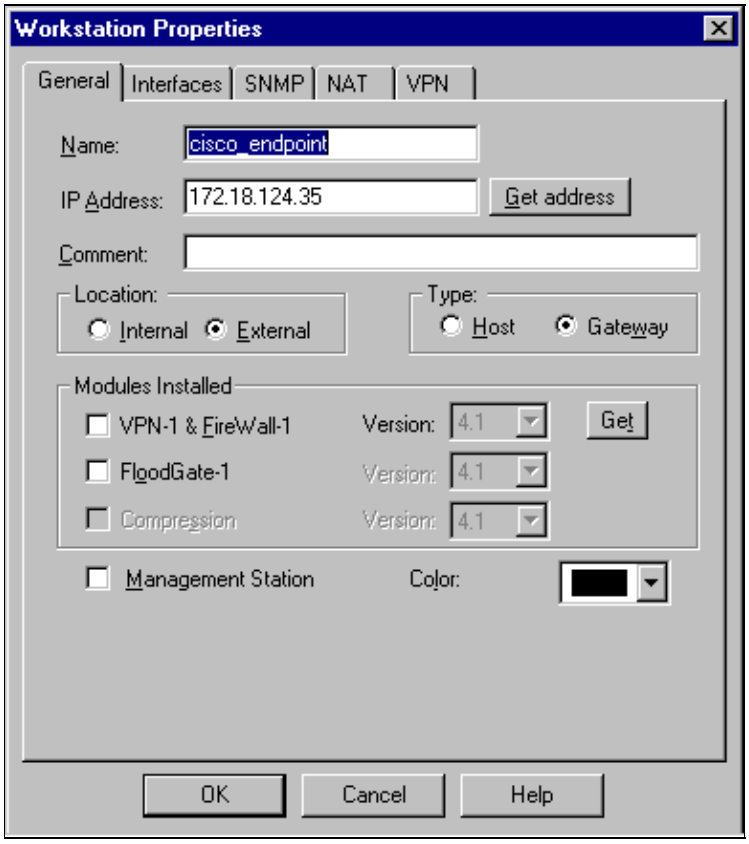
Select **External** under Location.



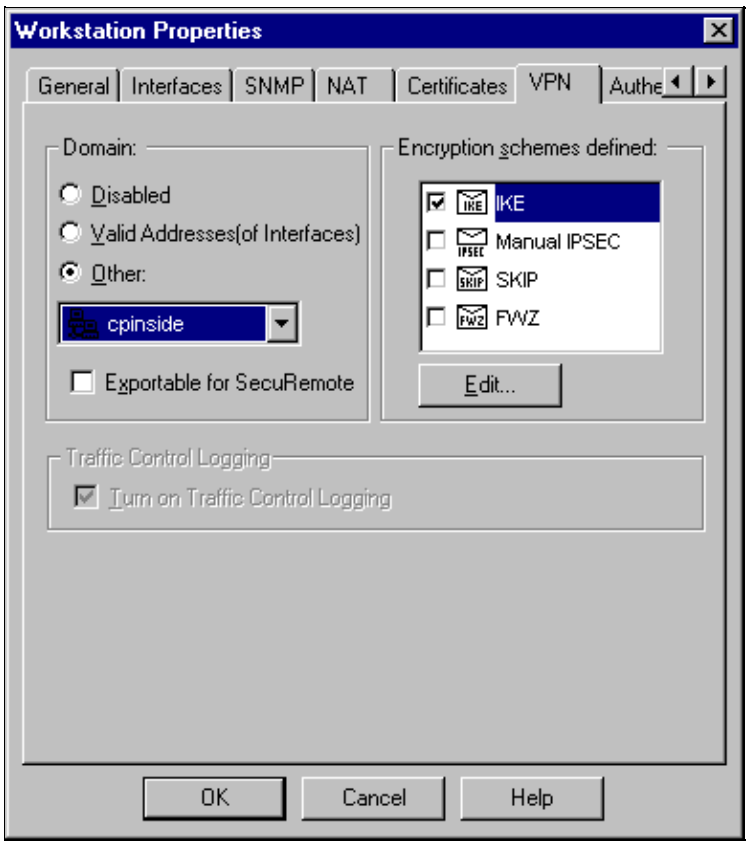
5. Select **Manage > Network objects > New > Workstation** to add an object for the external Cisco router gateway (called "cisco_endpoint"). This is the Cisco interface to which the **crypto map** *name* command is applied.

   Select **External** under Location. For Type, select **Gateway**.

   Note: Do not select the VPN−1/FireWall−1 check box.



6. Select **Manage > Network objects > Edit** to edit the Checkpoint gateway endpoint (called "RTPCPVPN") VPN tab. Under Domain, select **Other** and then select the inside of the Checkpoint network (called "cpinside") from the drop−down list. Under Encryption schemes defined, select **IKE**, and then click **Edit**.



7. Change the IKE properties for DES encryption to agree with these commands:

- **crypto isakmp policy #**
- **encryption des**

Note: DES encryption is the default so it is not visible in the Cisco configuration.

8. Change the IKE properties to SHA1 hashing to agree with these commands:

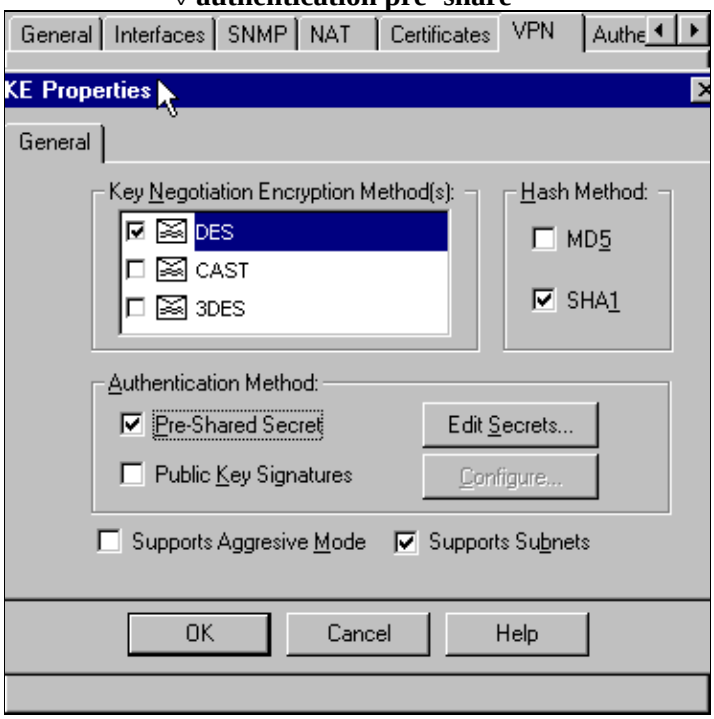
   - **crypto isakmp policy #**
   - **hash sha**

   Note: The SHA hashing algorithm is the default so it is not visible in the Cisco configuration.

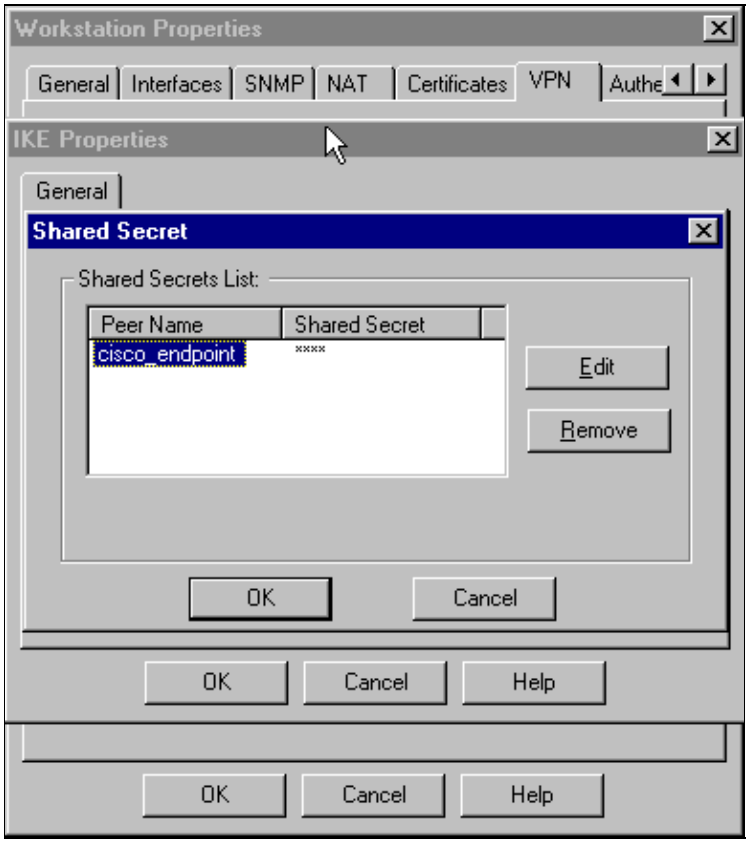
   Change these settings:

   - De−select **Aggressive Mode**.
   - Check **Supports Subnets**.
   - Check **Pre−Shared Secret** under Authentication Method. This agrees with these commands:

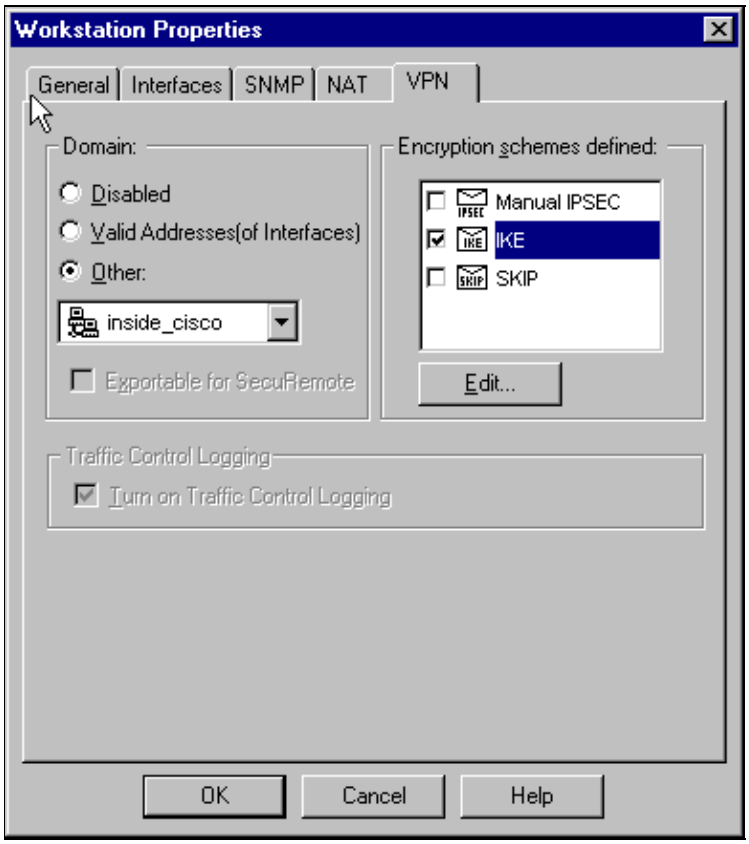
     - **crypto isakmp policy #**
     - **authentication pre−share**



9. Click **Edit Secrets** to set the pre−shared key to agree with the Cisco **crypto isakmp key** *key* **address** *address* command:



10. Select **Manage > Network objects > Edit** to edit the "cisco_endpoint" VPN tab. Under Domain, select **Other**, and then select the inside of the Cisco network (called "inside_cisco"). Under Encryption schemes defined, select **IKE**, and then click **Edit**.



11. Change the IKE properties DES encryption to agree with these commands:

    - **crypto isakmp policy #**

- **encryption des**

Note: DES encryption is the default so it is not visible in the Cisco configuration.

12. Change the IKE properties to SHA1 hashing to agree with these commands:

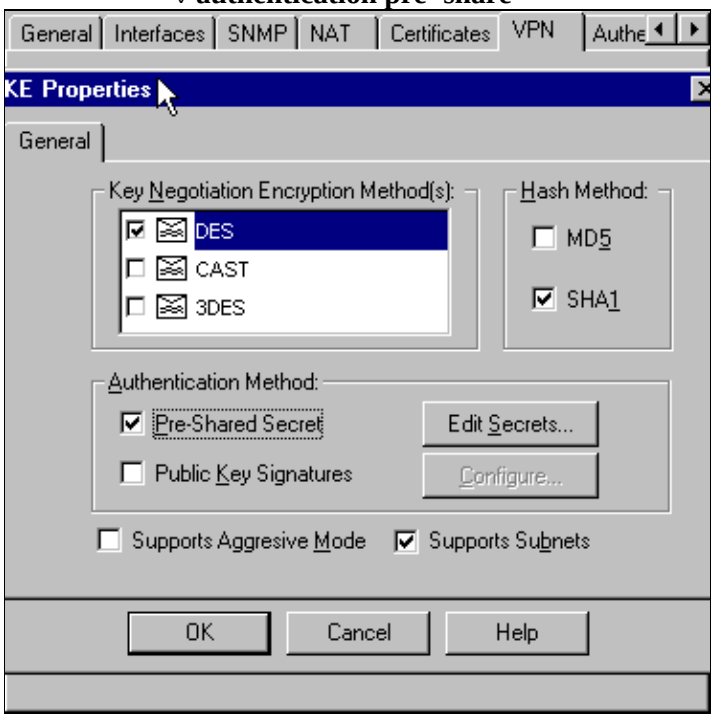
    - **crypto isakmp policy #**
    - **hash sha**

    Note: The SHA hashing algorithm is the default so it is not visible in the Cisco configuration.

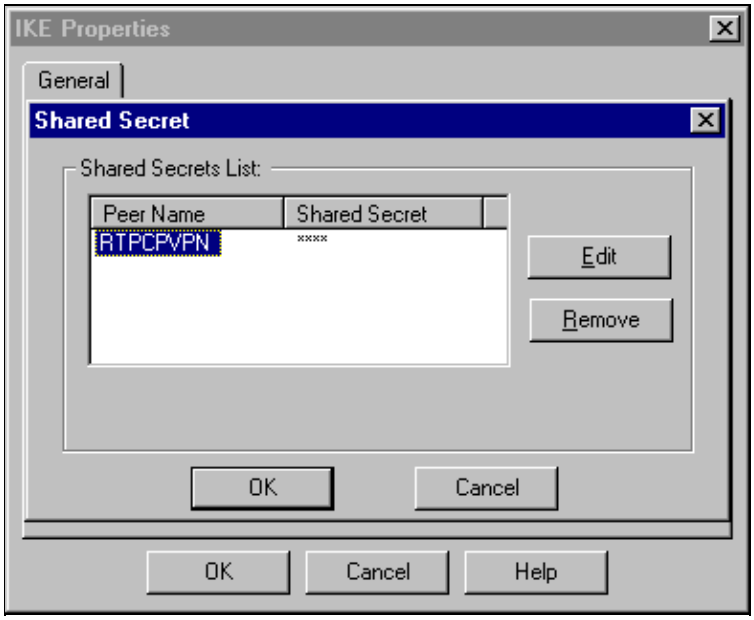
    Change these settings:

    - De−select **Aggressive Mode**.
    - Check **Supports Subnets**.
    - Check **Pre−Shared Secret** under Authentication Method. This agrees with these commands:

        - **crypto isakmp policy #**
        - **authentication pre−share**



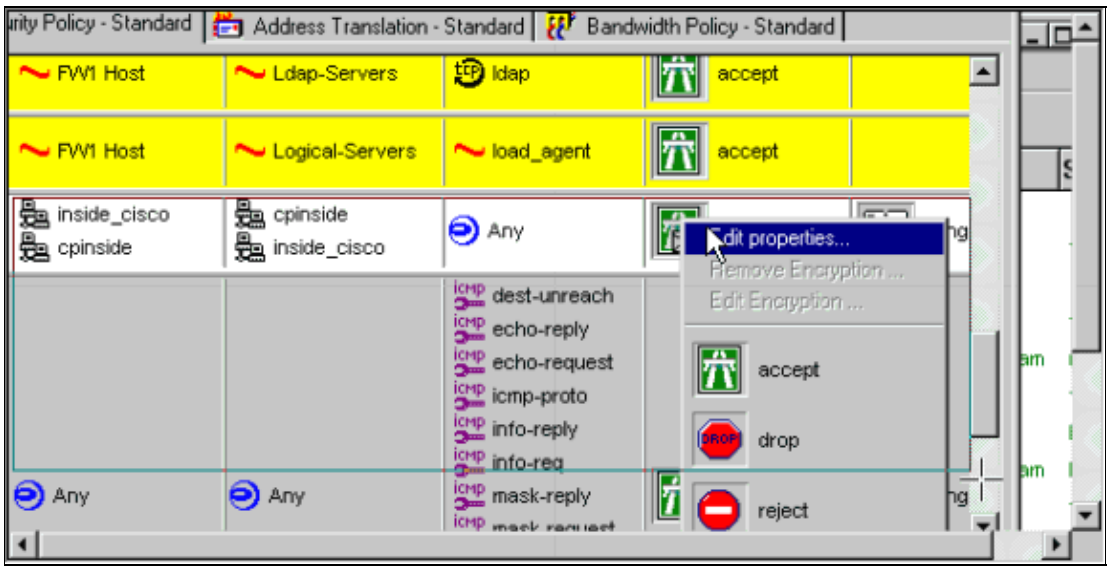
13. Click **Edit Secrets** to set the pre−shared key to agree with the **crypto isakmp key** *key* **address** *address* Cisco command.



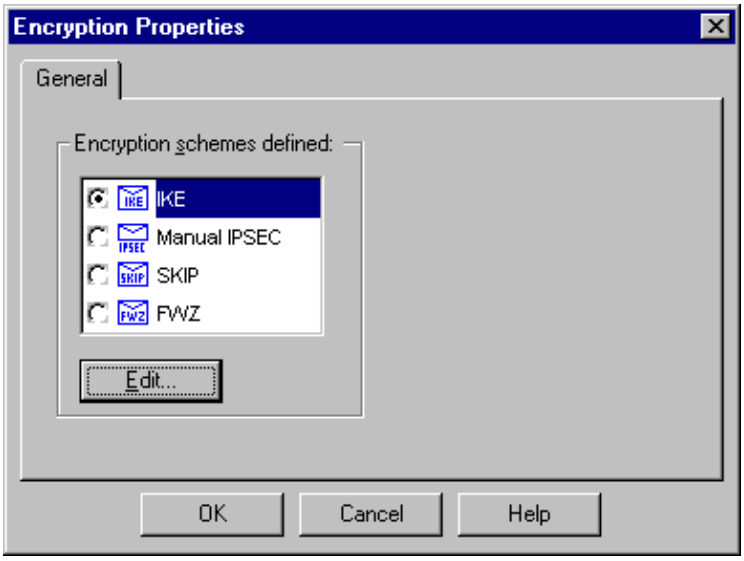
14. In the Policy Editor window, insert a rule with both Source and Destination as "inside_cisco" and "cpinside" (bidirectional). Set **Service=Any**, **Action=Encrypt**, and **Track=Long**.



15. Click the green **Encrypt** icon and select **Edit properties** to configure encryption policies under the Action heading.

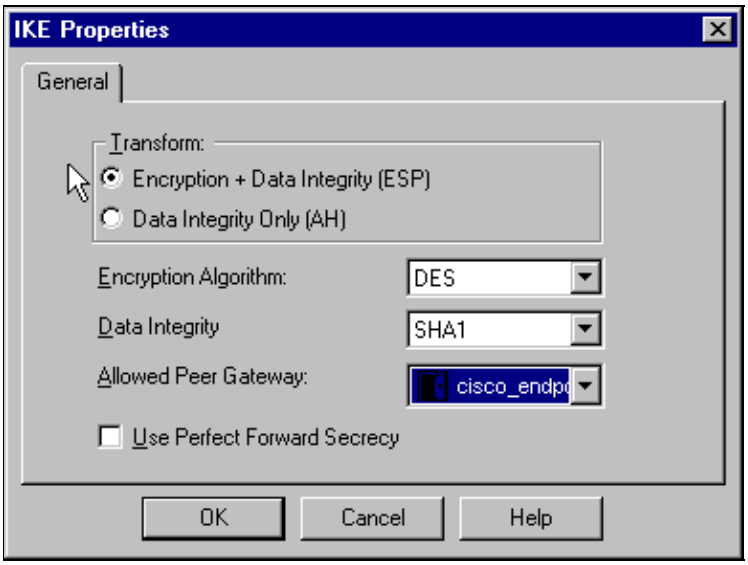


16. Select **IKE**, and then click **Edit**.



17. On the IKE Properties window, change these properties to agree with the Cisco IPsec transforms in the **crypto ipsec transform−set rtpset esp−des esp−sha−hmac** command:

    Under Transform, select **Encryption + Data Integrity (ESP)**. The Encryption Algorithm should be **DES**, Data Integrity should be **SHA1**, and the Allowed Peer Gateway should be the external router gateway (called "cisco_endpoint"). Click **OK**.



18. After you configure the Checkpoint, select **Policy > Install** on the Checkpoint menu to have the changes take effect.

Verify

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

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

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

Troubleshoot

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

Troubleshooting Commands

Note: Refer to Important Information on Debug Commands before you use **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.

Network Summarization

When multiple adjacent inside networks are configured in the encryption domain on the Checkpoint, the device might automatically summarize them with regard to interesting traffic. If the router is not configured to match, the tunnel is likely to fail. For example, if the inside networks of 10.0.0.0 /24 and 10.0.1.0 /24 are configured to be included in the tunnel, they might be summarized to 10.0.0.0 /23.

Checkpoint

Because the Tracking was set for Long in the Policy Editor window, denied traffic should appear in red in the Log Viewer. More verbose debug can be obtained with:

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

and in another window:

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

Note: This was a Microsoft Windows NT installation.

Issue these commands to clear SAs on the 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
```

Answer **yes** at the Are you sure? prompt.

Sample debug Output

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
```

```
cisco_endpoint#
20:54:06: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP:      encryption DES-CBC
20:54:06: ISAKMP:      hash SHA
20:54:06: ISAKMP:      default group 1
20:54:06: ISAKMP:      auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
   using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
20:54:06: ISAKMP (1): Total payload length: 12
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPSec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP:   attributes in transform:
20:54:06: ISAKMP:      encaps is 1
20:54:06: ISAKMP:      SA life type in seconds
20:54:06: ISAKMP:      SA life duration (basic) of 3600
20:54:06: ISAKMP:      SA life type in kilobytes
20:54:06: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
20:54:06: ISAKMP:      authenticator is HMAC-SHA
20:54:06: validate proposal 0
```

```
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
20:54:06: ISAKMP (0:1): Creating IPSec SAs
20:54:06:         inbound SA from 172.18.124.157 to 172.18.124.35
        (proxy 10.32.50.0 to 192.168.1.0)
20:54:06:         has spi 0xA29984CA and conn_id 2000 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06:         outbound SA from 172.18.124.35   to 172.18.124.157
   (proxy 192.168.1.0 to 10.32.50.0)
20:54:06:         has spi 404516441 and conn_id 2001 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.35, sa_prot= 50,
    sa_spi= 0xA29984CA(2727969994),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.157, sa_prot= 50,
    sa_spi= 0x181C6E59(404516441),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa

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

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

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

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

     inbound ah sas:

     inbound pcp sas:

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

     outbound ah sas:

     outbound pcp sas:


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

cisco_endpoint#exit
```

Related Information

- **IPsec Negotiation/IKE Protocols**
- **Configuring IPsec Network Security**
- **Configuring Internet Key Exchange Security Protocol**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Oct 13, 2008 Document ID: 5463