Configuring an IPsec Tunnel − Cisco VPN 5000 Concentrator to Checkpoint 4.1 Firewall

Document ID: 14105

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. Refer to the End−of−Sales Announcement for more information.

Contents

Introduction

This document demonstrates how to form an IPsec tunnel with pre−shared keys to join two private networks. It joins a private network inside the Cisco VPN 5000 Concentrator (192.168.1.x) to a private network inside the Checkpoint 4.1 Firewall (10.32.50.x). It is assumed that traffic from inside the VPN Concentrator and inside the Checkpoint to the Internet (represented in this document by the 172.18.124.x networks) flows before you start this configuration.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator software version 5.2.19.0001
- Checkpoint 4.1 Firewall

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.

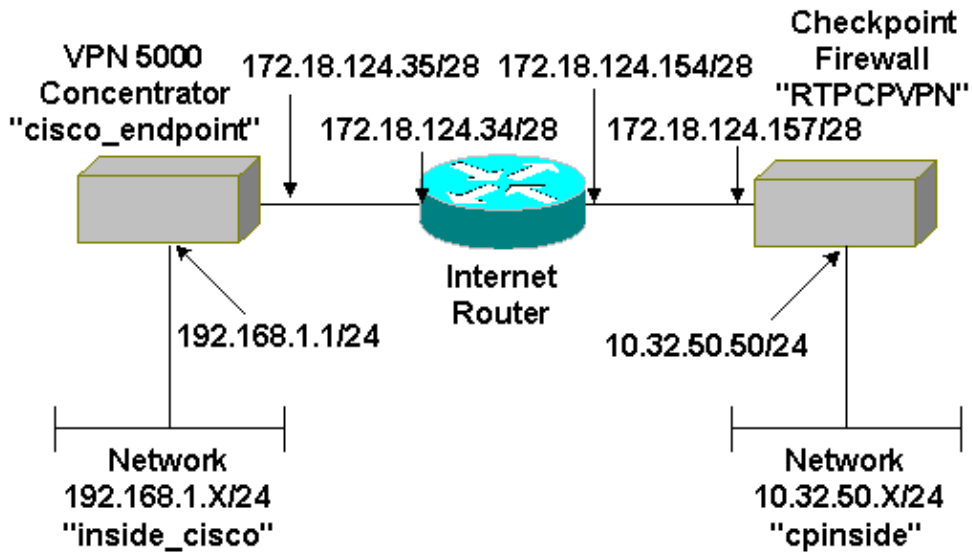
Configure

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 this configuration.

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
```

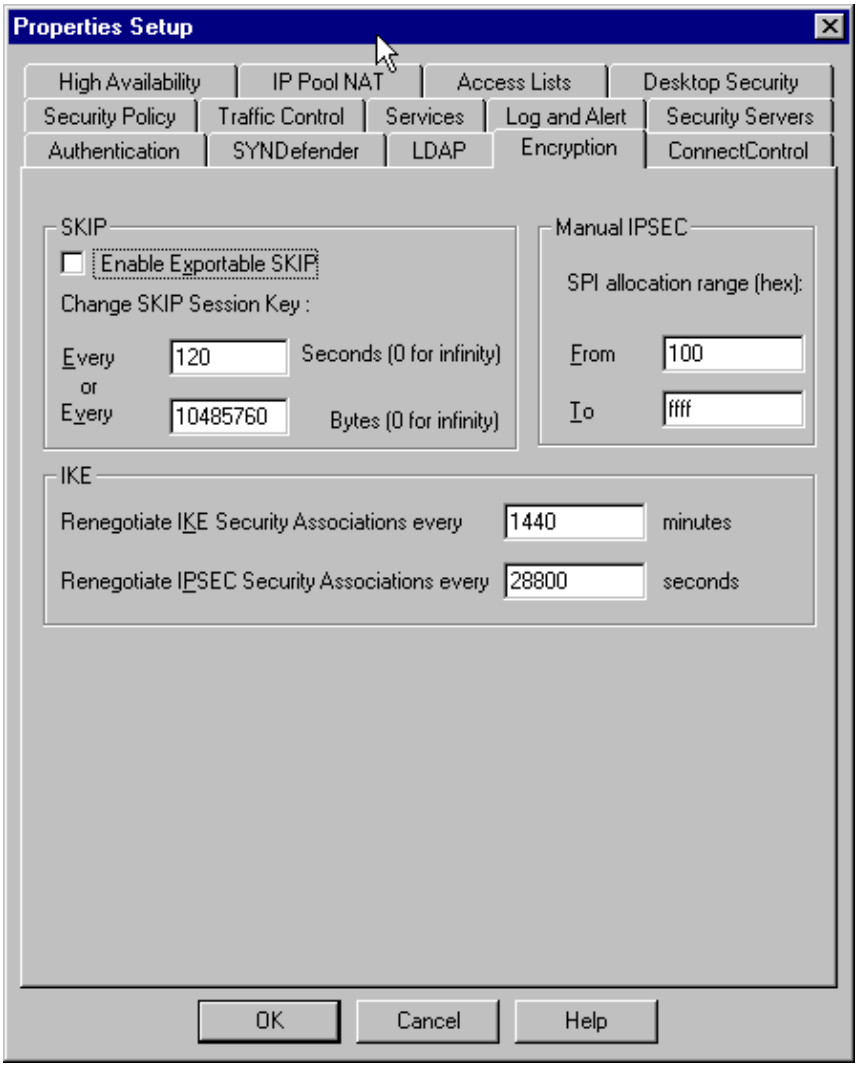
```
[ IKE Policy ]
Protection               = SHA_DES_G2

[ 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

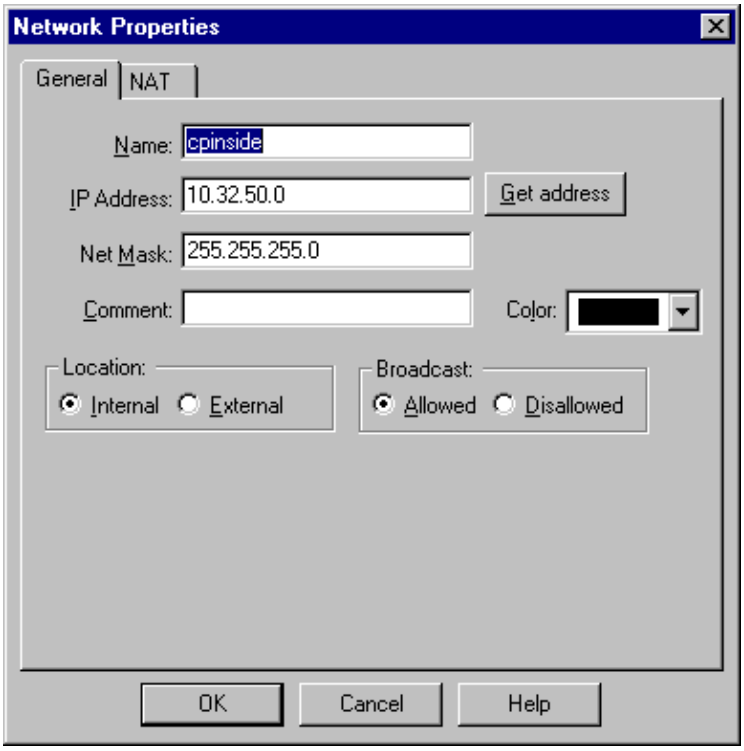
Complete these steps to configure the Checkpoint 4.1 Firewall.

1. Select **Properties** > **Encryption** to set the Checkpoint IPsec lifetimes to agree with the **KeyLifeSecs = 28800** VPN Concentrator command.

   Note: Leave the Checkpoint Internet Key Exchange (IKE) lifetimes at the default.

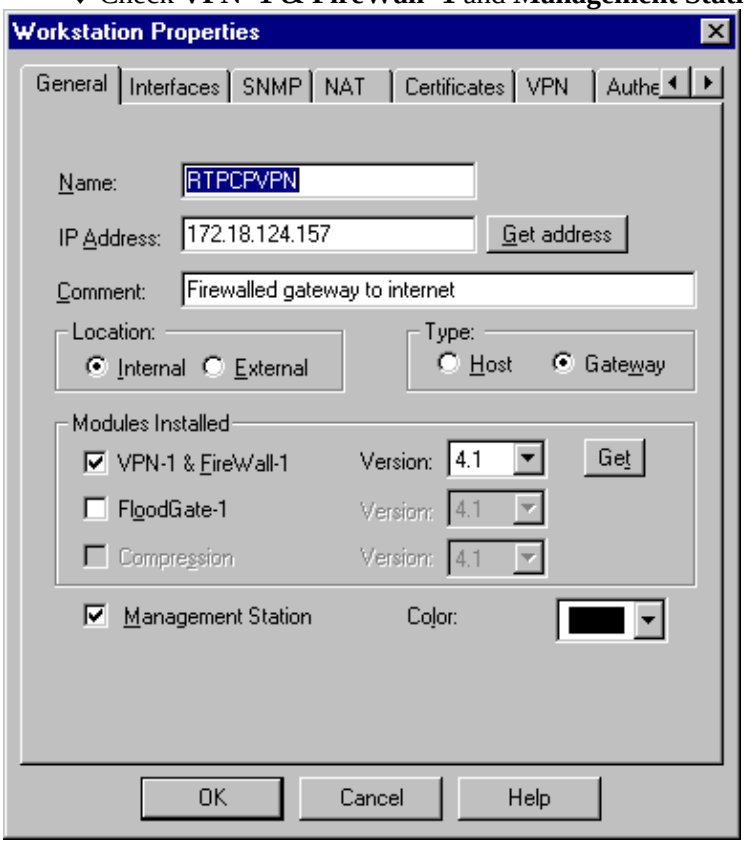


2. Select **Manage > Network objects > New (or Edit) > Network** to configure the object for the internal ("cpinside") network behind the Checkpoint. This should agree with the **Peer = "10.32.50.0/24"** VPN Concentrator command.



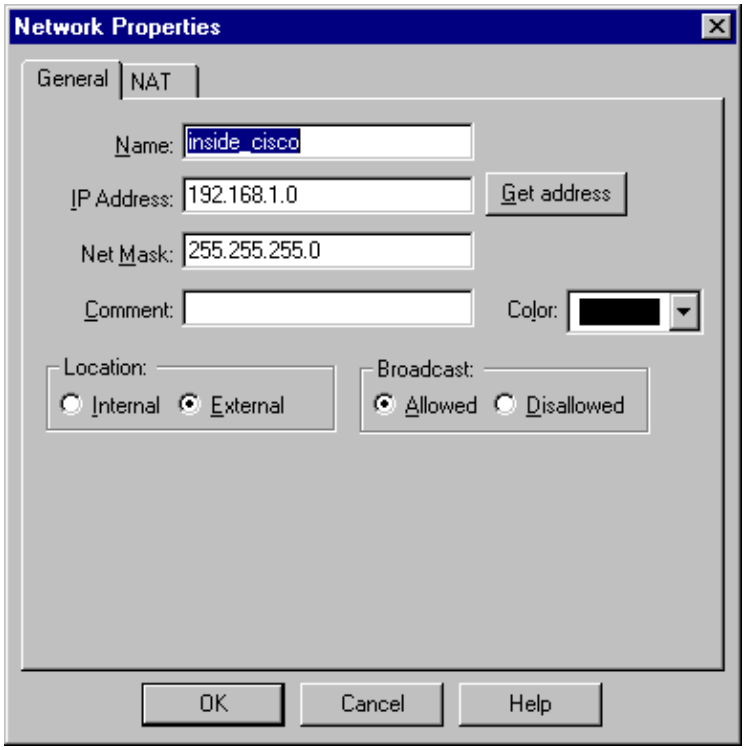
3. Select **Manage > Network objects > Edit** to edit the object for the gateway ("RTPCPVPN" Checkpoint) endpoint that the VPN Concentrator points to in the **Partner = <ip>** command.

   - Select **Internal** under Location.
   - Select **Gateway** for Type.
   - Check **VPN−1 & FireWall−1** and **Management Station** under Modules Installed.



4. Select **Manage > Network objects > New (or Edit) > Network** to configure the object for the external ("inside_cisco") network behind the VPN Concentrator.

This should agree with the **LocalAccess = <192.168.1.0/24>** VPN Concentrator command.

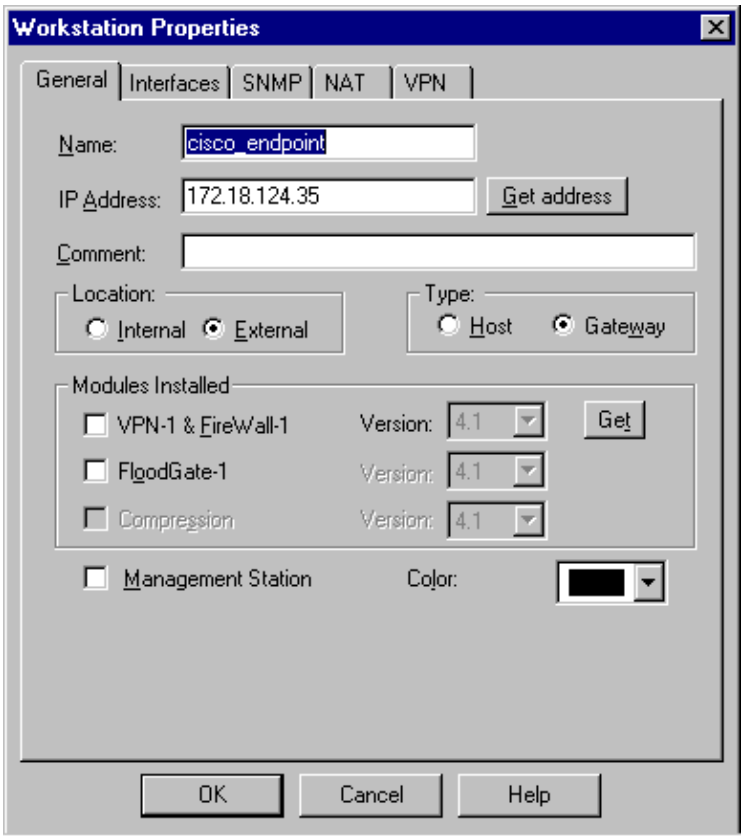


5. Select **Manage > Network objects > New > Workstation** to add an object for the external ("cisco_endpoint") VPN Concentrator gateway.

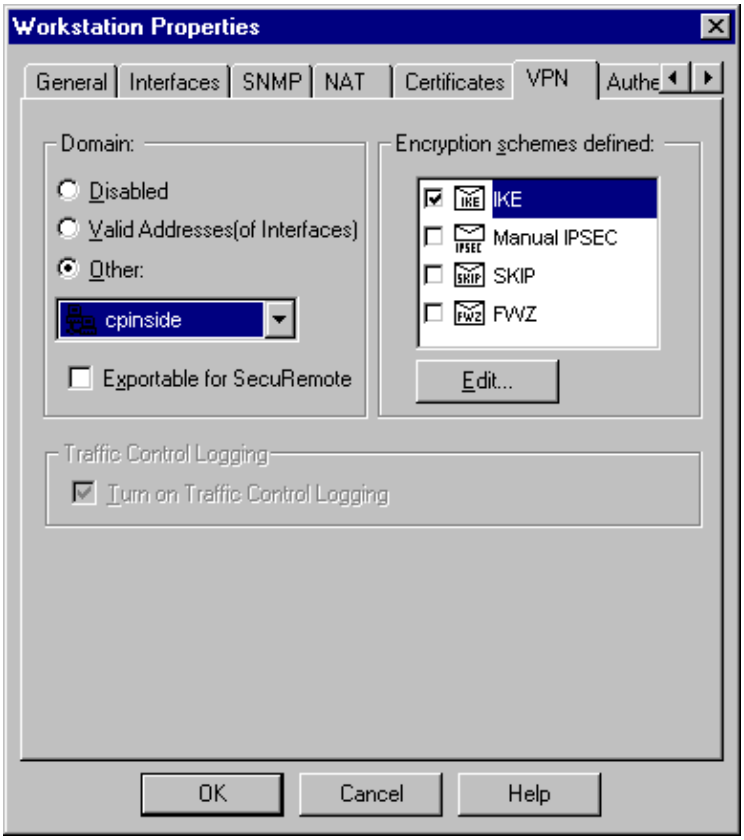
   This is the "outside" interface of the VPN Concentrator with connectivity to the Checkpoint (in this document, 172.18.124.35 is the IP address in the **IPAddress = <ip>** command).

   Select **External** under Location. Select **Gateway** for Type.

   Note: Do not check VPN−1/FireWall−1.



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**.

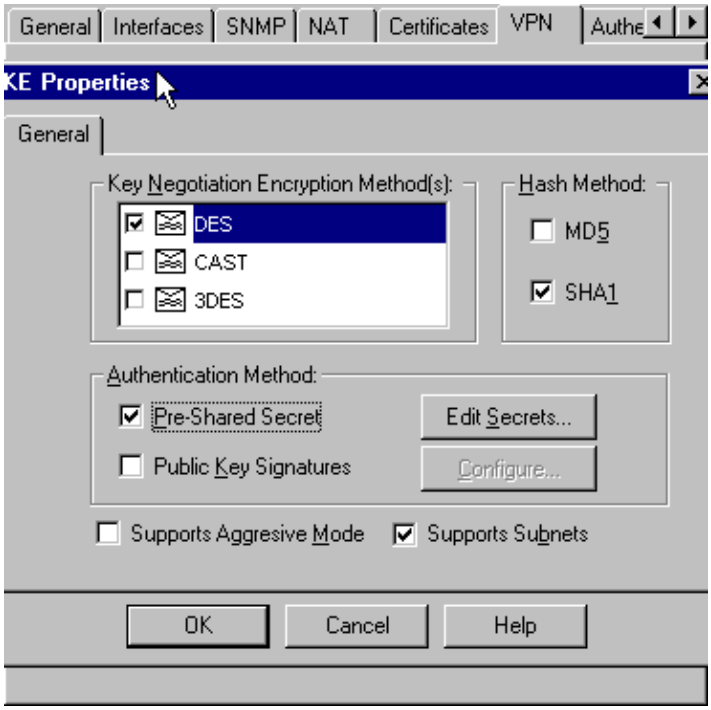


7. Change the IKE properties to **DES** encryption and **SHA1** hashing to agree with the **SHA_DES_G2** VPN Concentrator command.

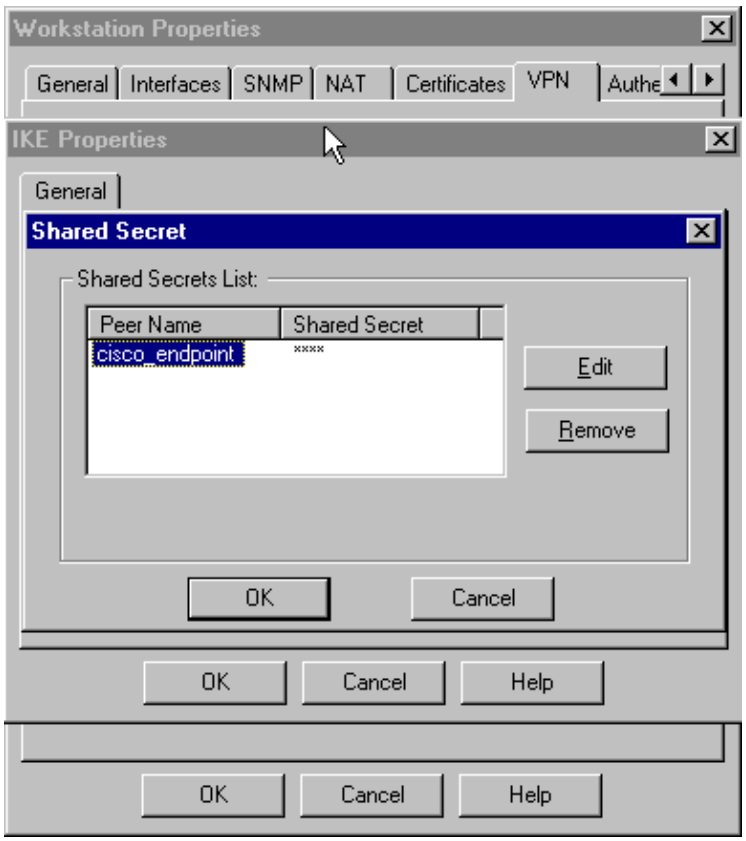
Note: The "G2" refers to Diffie−Hellman group 1 or 2. In testing, it was discovered that the Checkpoint accepts either "G2" or "G1."

Change these settings:

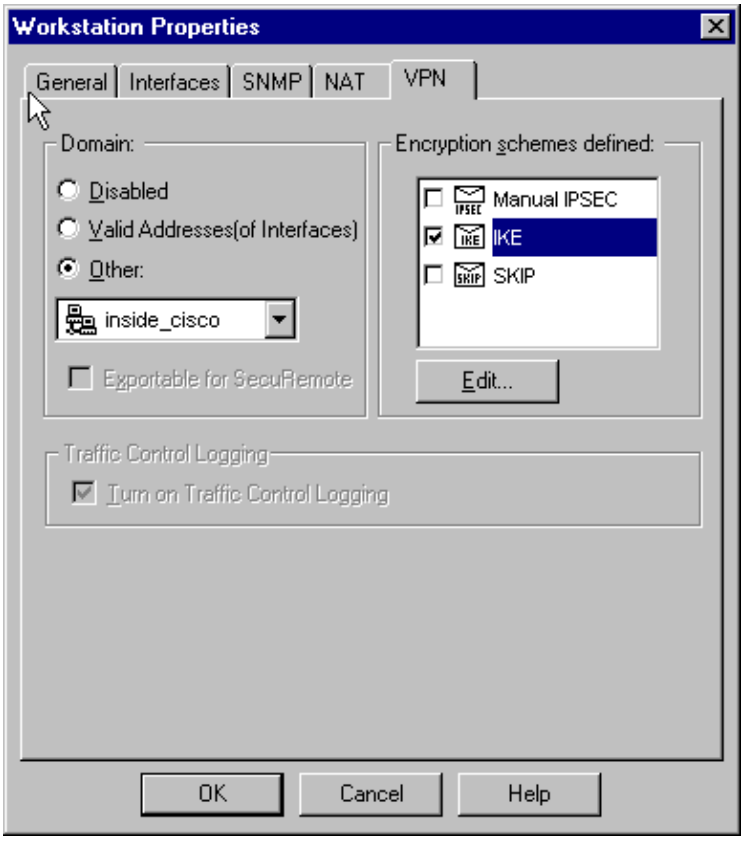
a. De−select **Aggressive Mode**.
b. Check **Supports Subnets**.
c. Check **Pre−Shared Secret** under Authentication Method.



8. Click **Edit Secrets** to set the pre−shared key to agree with the **SharedKey = <key>** VPN Concentrator command.



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

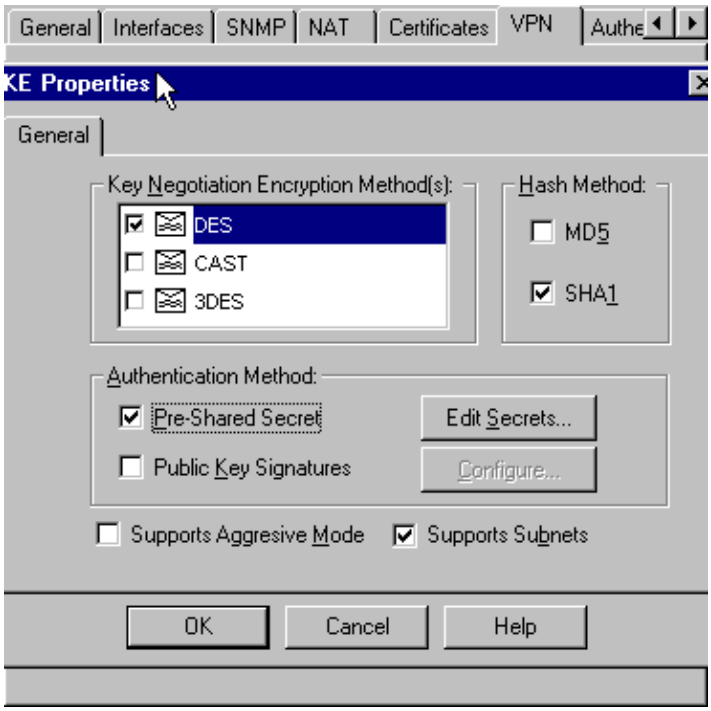


10. Change the IKE properties to **DES** encryption and **SHA1** hashing to agree with the **SHA_DES_G2** VPN Concentrator command.

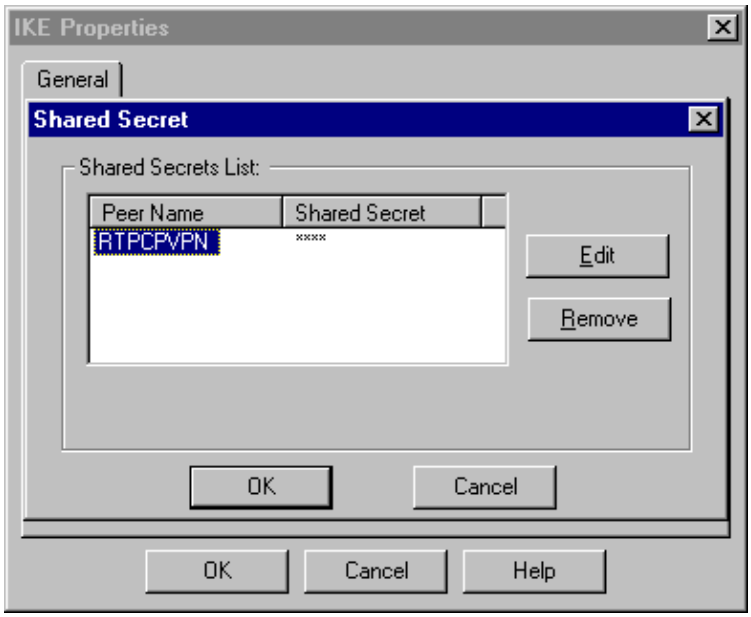
    Note: The "G2" refers to Diffie−Hellman group 1 or 2. In testing, it was found that the Checkpoint accepts either "G2" or "G1."

    Change these settings:

    a. De−select **Aggressive Mode**.
    b. Check **Supports Subnets**.
    c. Check **Pre−Shared Secret** under Authentication Method.

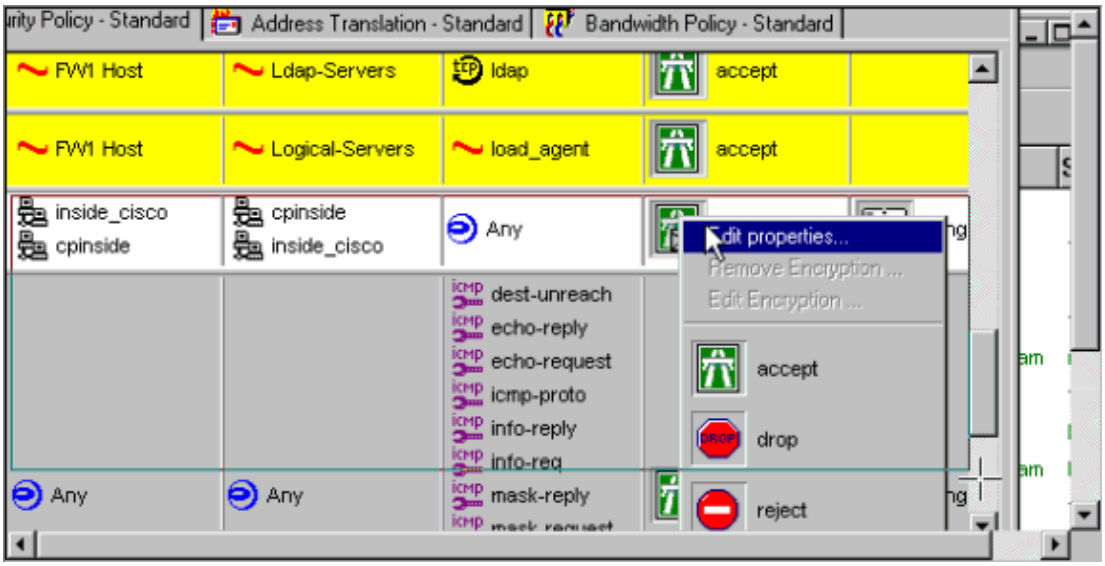


11. Click **Edit Secrets** to set the pre−shared key to agree with the **SharedKey = <key>** VPN Concentrator command.

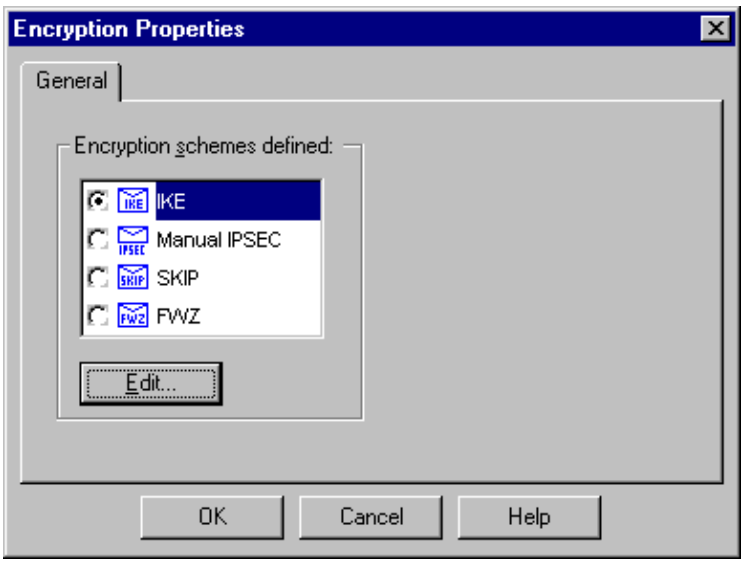


12. In the Policy Editor window, insert a rule with both Source and Destination as "inside_cisco" and "cpinside" (bidirectional). Set **Service=Any**, **Action=Encrypt**, and **Track=Long**.

13. Under the Action heading, click the green **Encrypt** icon and select **Edit properties** to configure encryption policies.

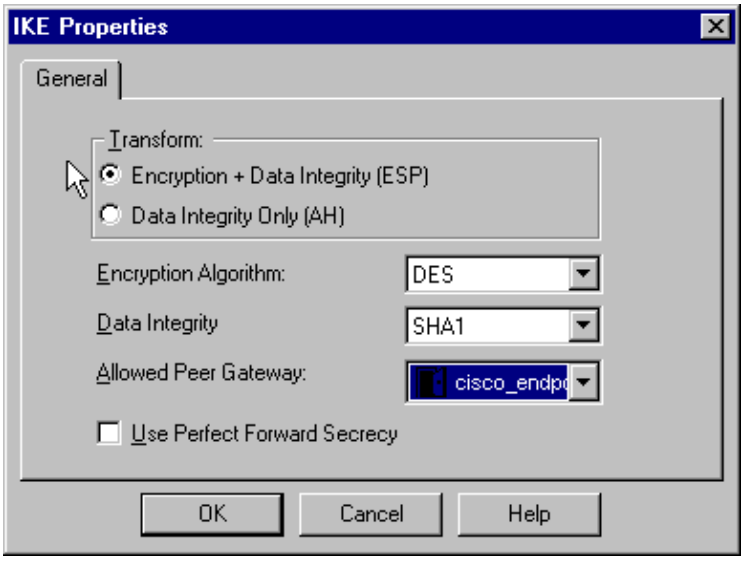


14. Select **IKE**, and click **Edit**.



15. On the IKE Properties window, change these properties to agree with the **Transform = esp(sha,des)** VPN Concentrator 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 VPN Concentrator gateway (called "cisco_endpoint"). Click **OK**.



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

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

VPN 5000 Concentrator Troubleshooting Commands

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

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

- **vpn trace dump all** Shows information about all matching VPN connections, including information about the time, the VPN number, the real IP address of the peer, which scripts have been run, and in the case of an error, the routine and line number of the software code where the error occurred.
- **show system log buffer** Shows the contents of the internal log buffer.
- **show vpn statistics** Shows this information for users, partners, and the total for both. (For modular models, the display includes a section for each module slot. Refer to the Sample Debug Output section.)
    - `Current Active` The current active connections.
    - `In Negot` The currently negotiating connections.
    - `High Water` The highest number of concurrent active connections since the last reboot.
    - `Running Total` The total number of successful connections since the last reboot.
    - `Tunnel OK` The number of tunnels for which there were no errors.
    - `Tunnel Starts` The number of tunnel starts.
    - `Tunnel Error` The number of tunnels with errors.
- **show vpn statistics verbose** Shows ISAKMP negotiation statistics, and many more active connection statistics.

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 VPN Concentrator 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 4.1 Firewall Debug

This was a Microsoft Windows NT installation. Because the tracking was set for `Long` in the Policy Editor window (as seen in Step 12), denied traffic should appear in red in the Log Viewer. More verbose debug can be obtained by:

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

and in another window:

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

Issue these commands to clear the Security Associations (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

```
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
```

Related Information

- **Cisco VPN 5000 Series Concentrators End−of−Sales Announcement**
- **IPsec Negotiation/IKE Protocols**
- **Technical Support & Documentation − Cisco Systems**

Updated: May 02, 2008 Document ID: 14105