# 配置 IPSec 隧道 - Cisco VPN 5000 集中器到 Checkpoint 4.1 防火墙

## 目录



## 简介

本文档演示如何使用预共享密钥形成IPsec隧道以加入两个专用网络。它将Cisco VPN 5000集中器(192.168.1.x)内的专用网络连接到Checkpoint 4.1防火墙(10.32.50.x)内的专用网络。 假设在您开始此配置之前，流量从VPN集中器内和检查点内流到Internet（在本文档中由172.18.124.x网络表示）。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco VPN 5000 集中器
- Cisco VPN 5000 集中器软件版本 5.2.19.0001

- 检查点 4.1 防火墙

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

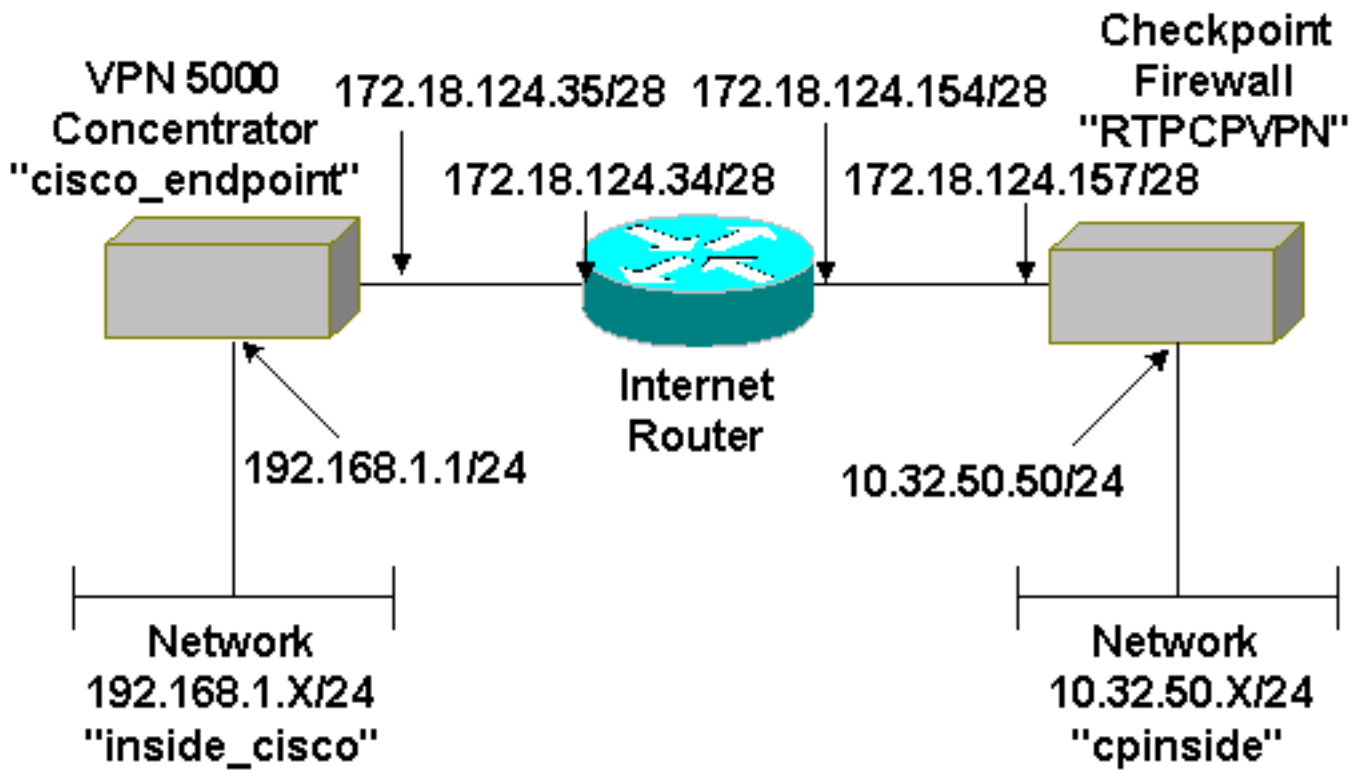
# 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意**：使用命令查找工具(仅限注册客户)可查找有关本文档中使用的命令的详细信息。

## 网络图

本文档使用以下网络设置：




## 配置

本文档使用以下配置。

**Cisco VPN 5000 集中器**

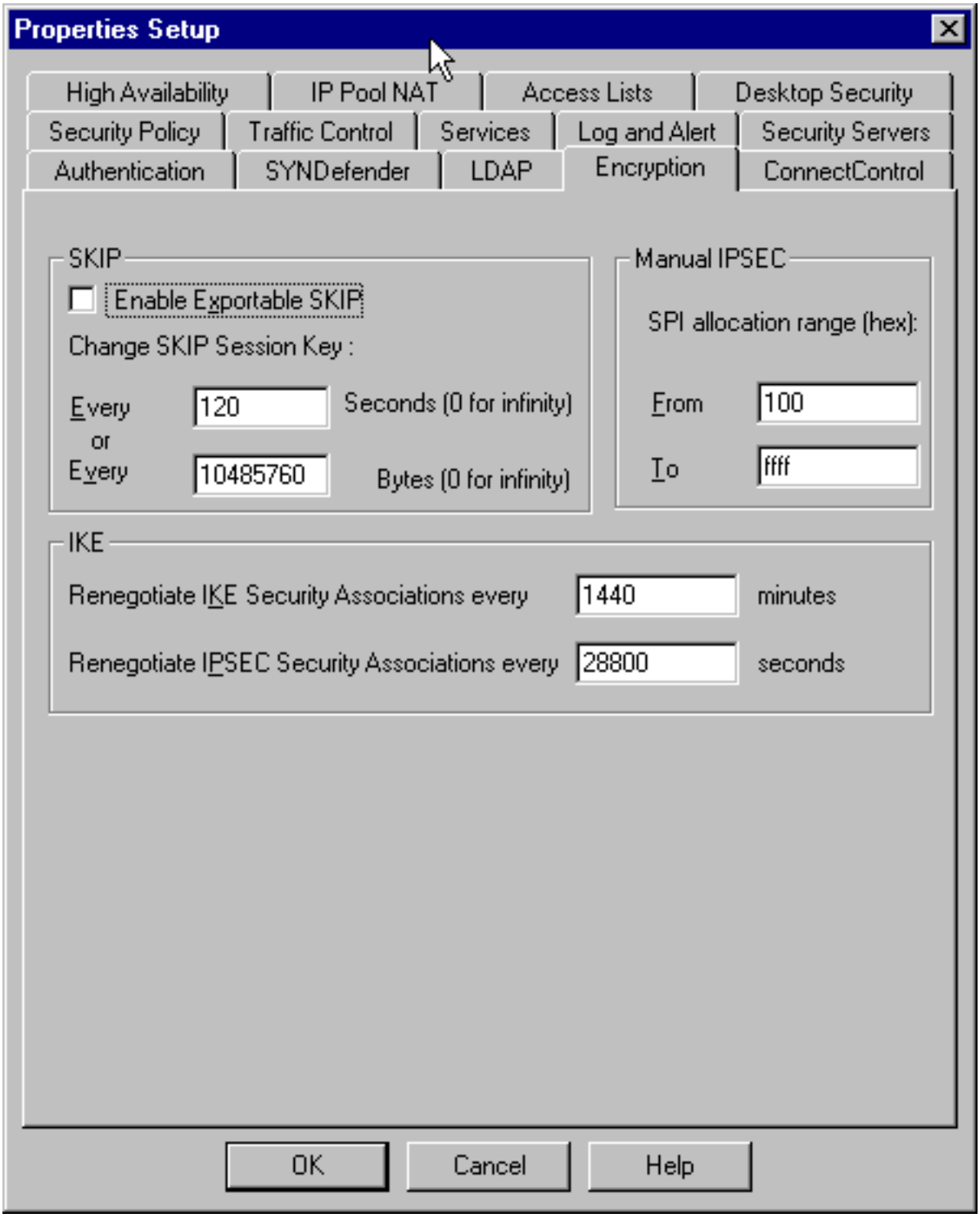
```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1
```

```
[ 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.
```

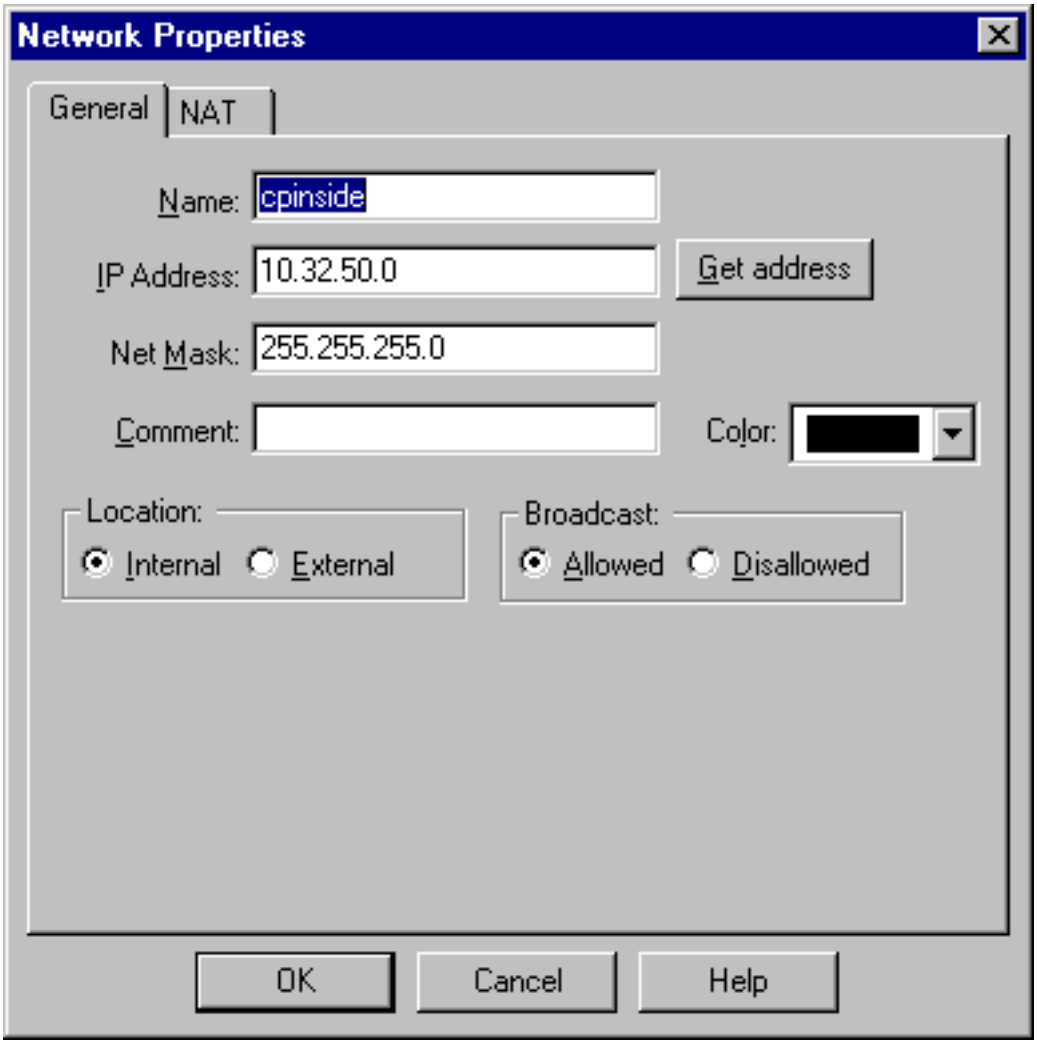
## 检查点 4.1 防火墙

完成以下步骤，以配置检查点 4.1 防火墙。

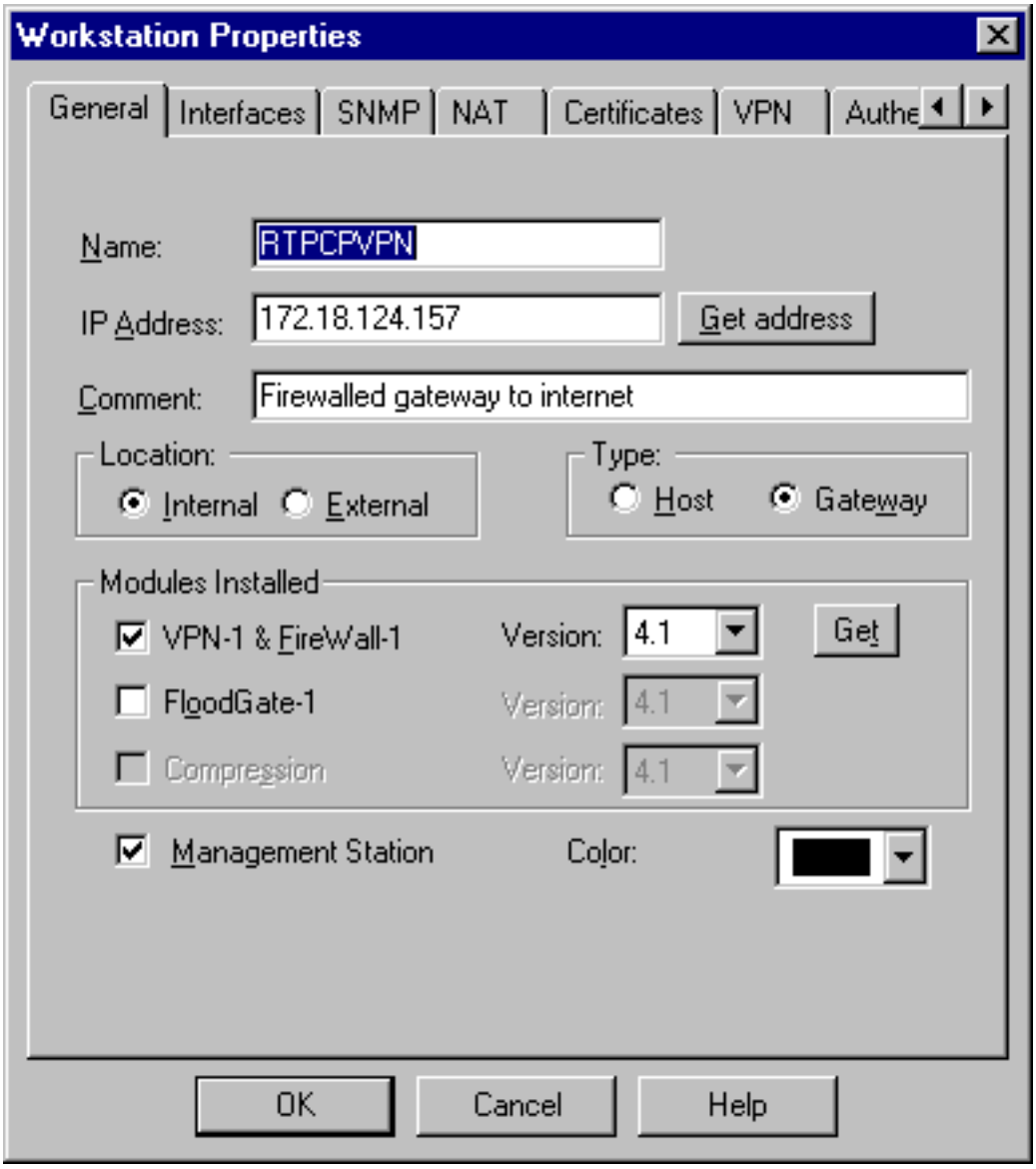
1. 选择**Properties > Encryption** ，将Checkpoint IPsec生存期设置为与**KeyLifeSecs = 28800** VPN集中器命令一致。**注意：**将检查点互联网密钥交换(IKE)生存期保留为默认值。



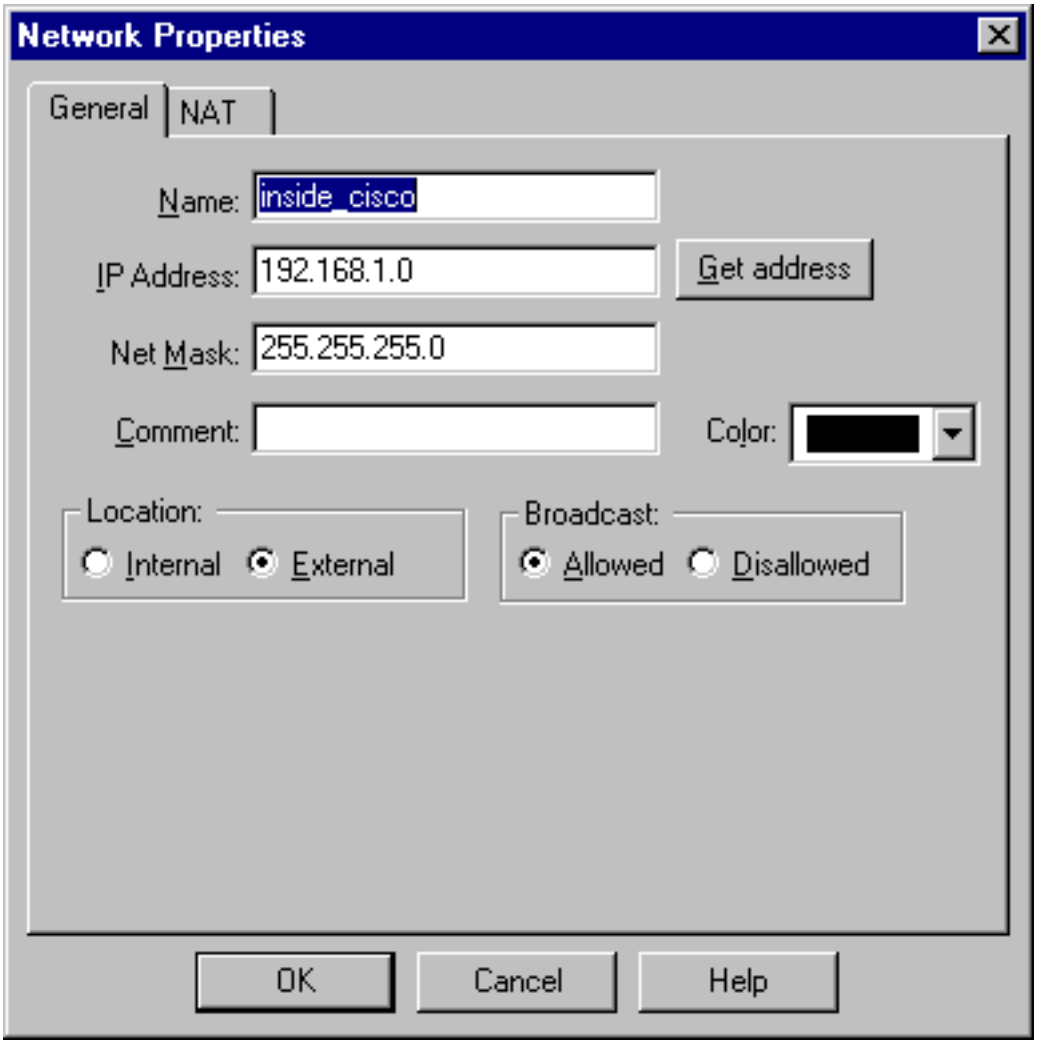

2. "选择Manage > Network objects > New (或 Edit) > Network，配置Checkpoint后的内部 (""cpinside"") 网络的对象。"这应与Peer = "**10.32.50.0/24" VPN集中器**命令一致。



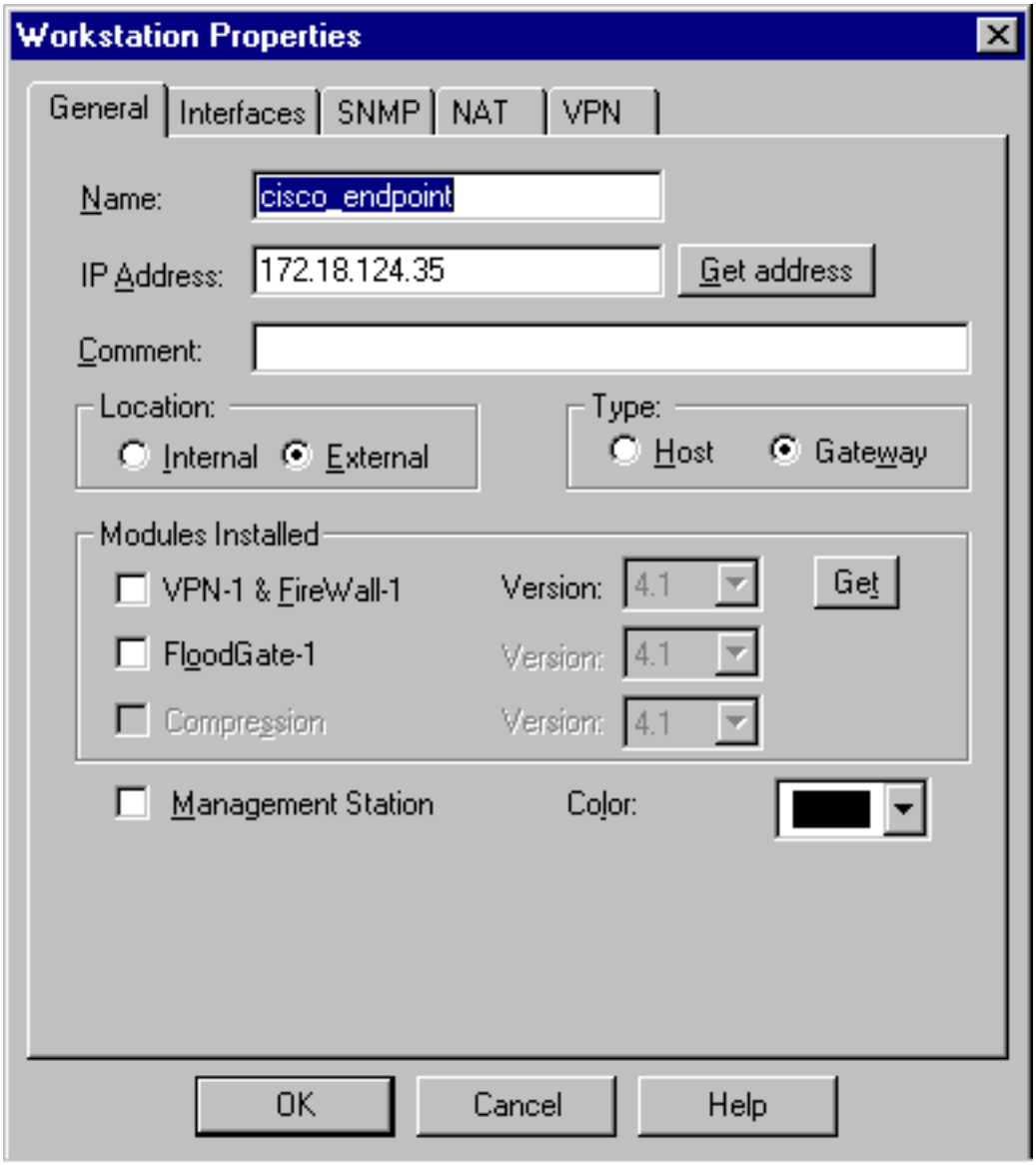

3. 选择**Manage > Network objects > Edit**以编辑VPN集中器在Partner = <ip>命令中指向的网关(“RTPCPVPN” Checkpoint)终**端的对**象。在“Location”下选择 **Internal。**选择**Gateway** 以进行类型。在“**Modules Installed（已安装模块）”**下选中**VPN-1** & FireWall-1和管理站。



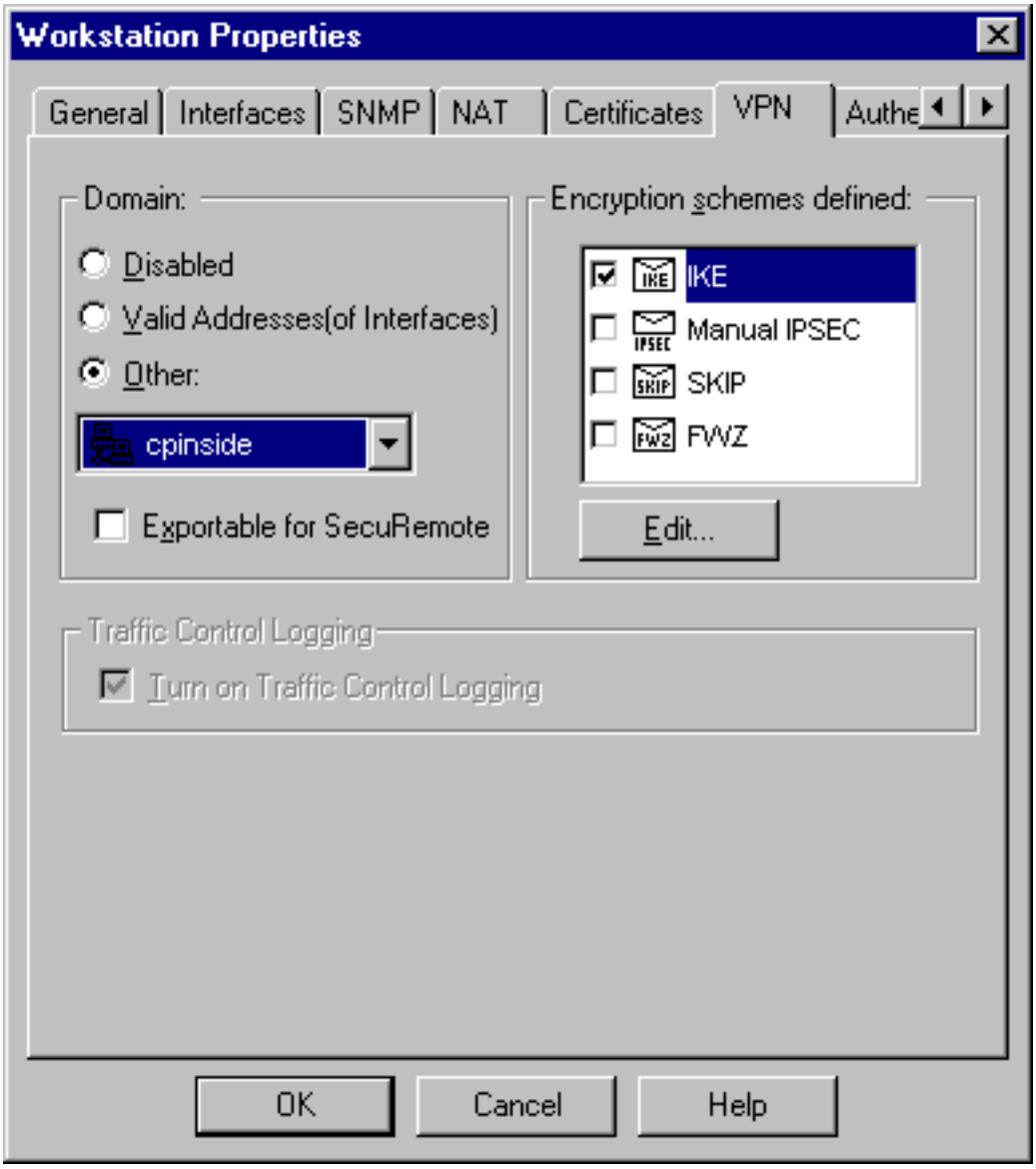

4. 选择 **Manage > Network objects > New (or Edit) > Network** 以配置 VPN 集中器后部的外部 ("inside_cisco") 网络的对象。这应与LocalAccess = **<192.168.1.0/24>VPN集中器**命令一致。



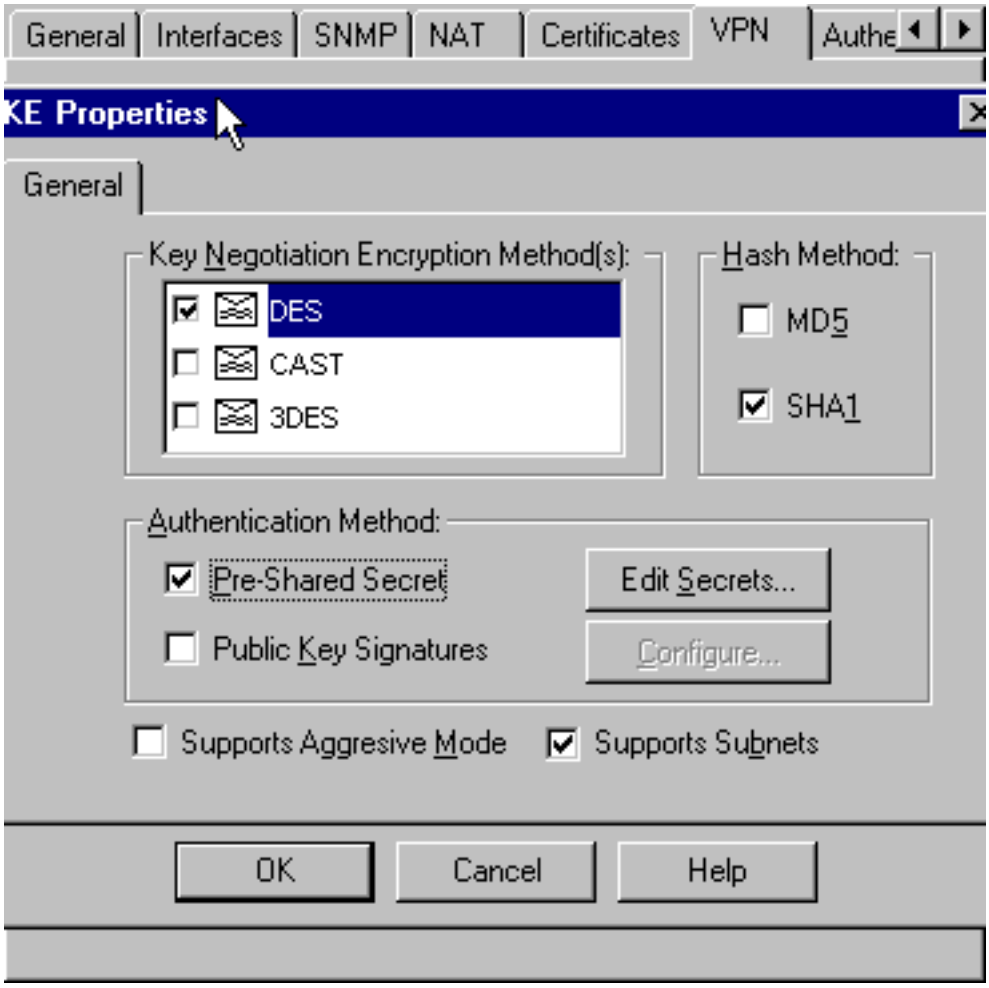

5. 选择 **Manage > Network objects > New > Workstation，为外部 ("cisco_endpoint") VPN 集中器网关添加对象。**这是与检查点连接的VPN集中器的“外部”接口(在本文档中，172.18.124.35是IP地址= <ip>命**令中的**IP地址)。在“Location”下选择 **External。**选择 **Gateway** 以进行类型。**注意：**请勿检查VPN-1/FireWall-1。




6. 选择 **Manage > Network objects > Edit 以编辑 Checkpoint 网关端点（称为 “RTPCPVPN”）VPN 选项卡。**在域下，请选择**其他然后从下拉列表中选择Checkpoint网络(称 “cpinside”)。**在被定义的加密机制下，精选的**IKE**，然后点击**编辑**。

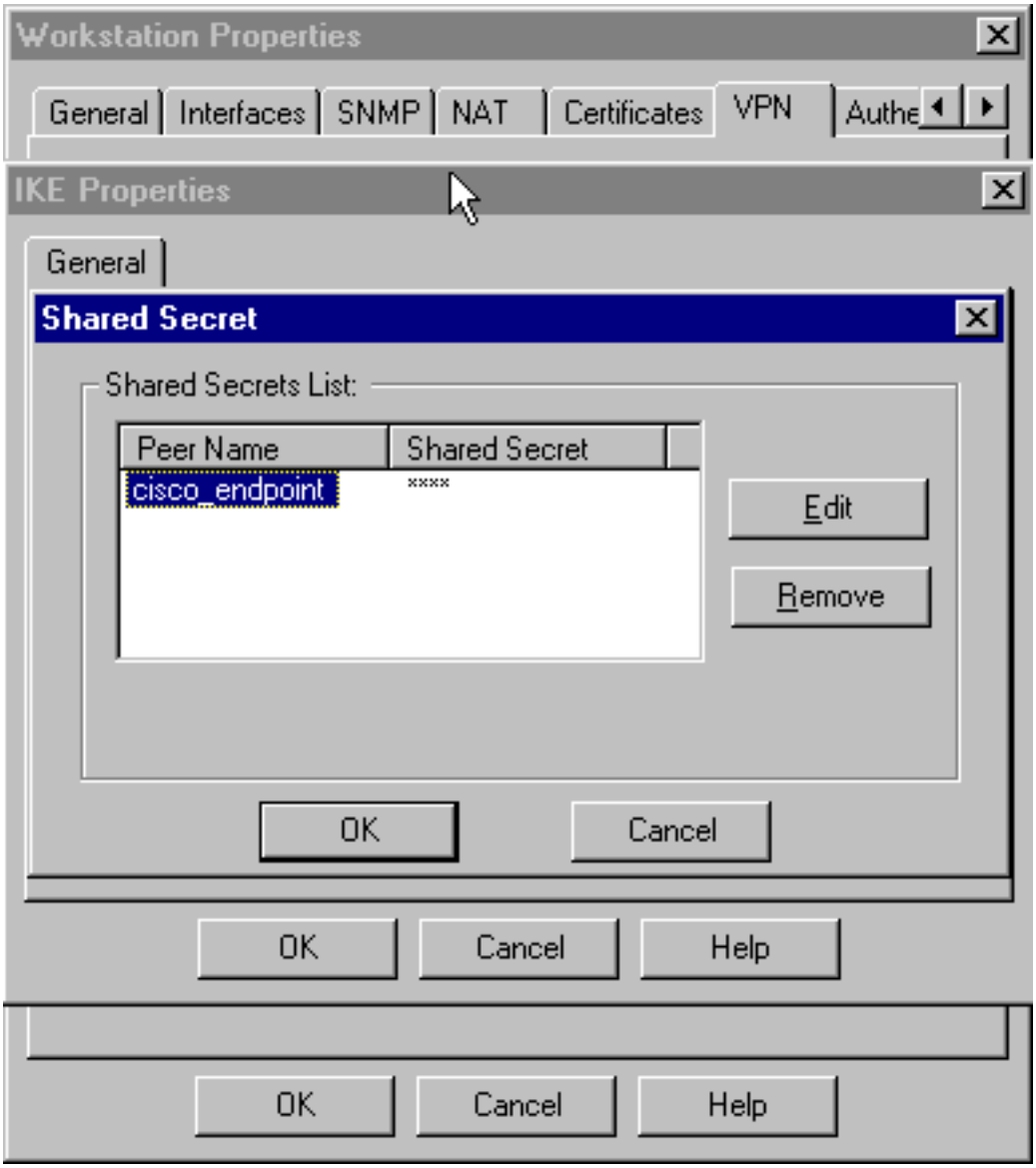



7. 将IKE属性更**改为**DES加**密和SHA1**散列以**与SHA_DES_G2 VPN集中器**命令一致。**注意**：“G2”是指Diffie-Hellman组1或2。在测试中，发现检查点接受“G2”或“G1”。更改这些设置：取消选定积极模式。选中 **Supports Subnets**。在“Authentication Method”下，选中 **Pre-**

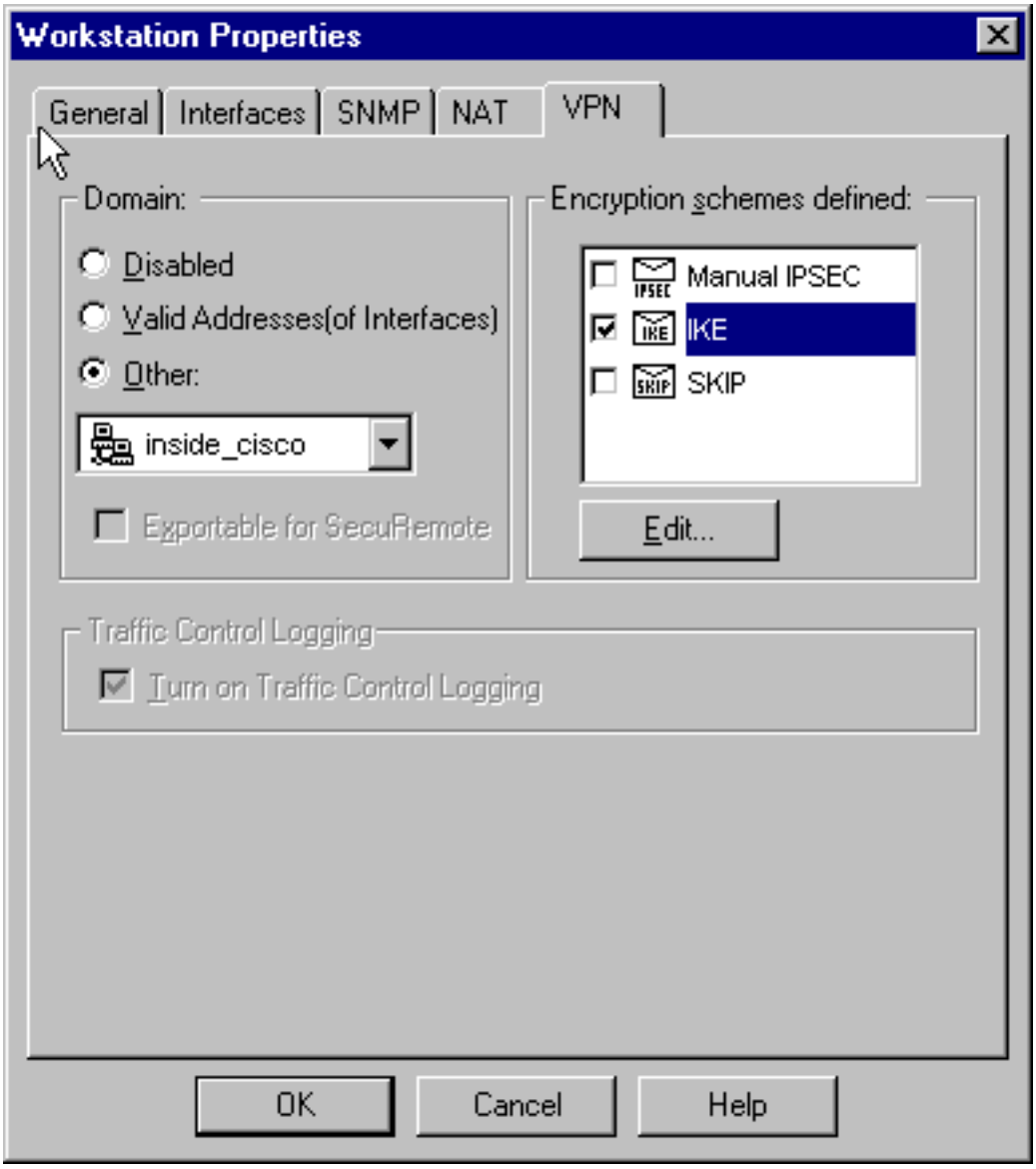



**Shared Secret。**

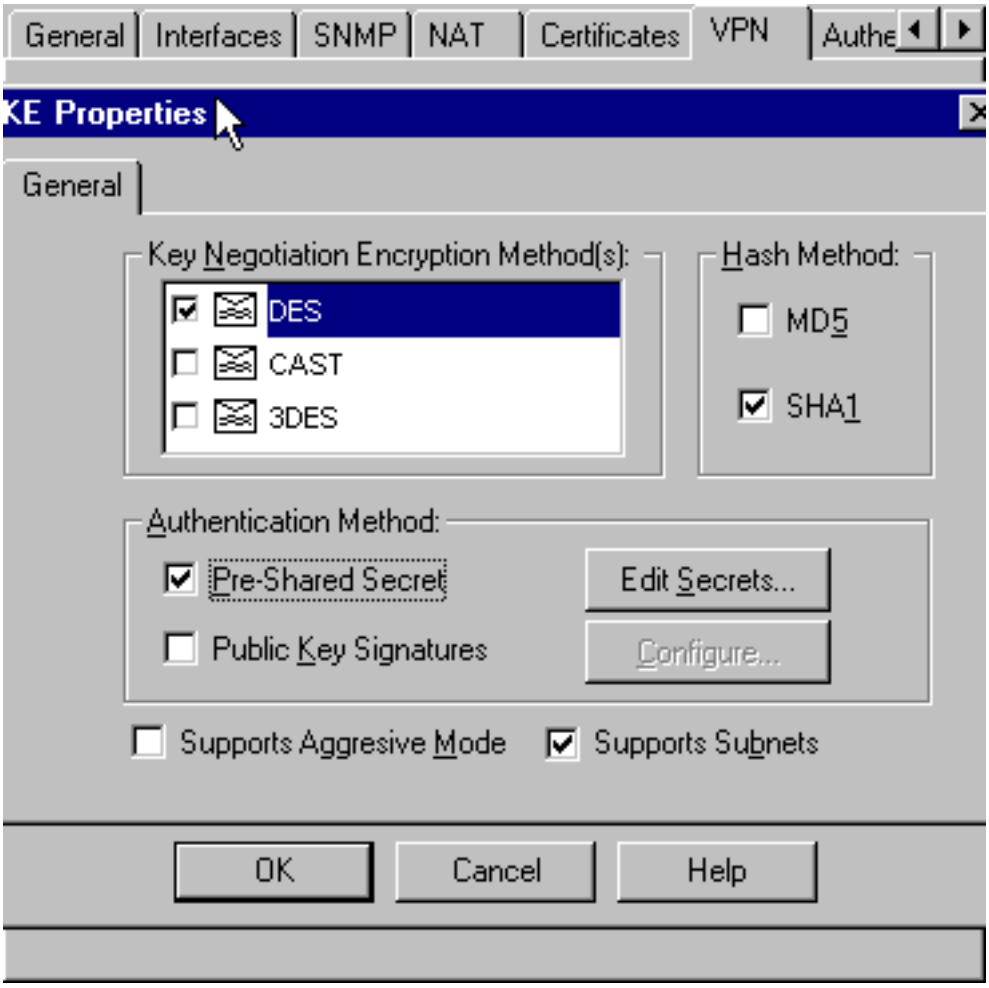
8. 单击**Edit Secrets**，将预共享密钥设置为与**SharedKey = <key>** VPN集中器命令一致。




9. 选择 **Manage > Network objects > Edit 以编辑“cisco_endpoint”VPN 选项卡。**在域下，选择**其他**，然后选择VPN集中器网络的内部（称为“inside_cisco”）。 在被定义的加密机制下，精选的**IKE**，然后点击**编辑**。

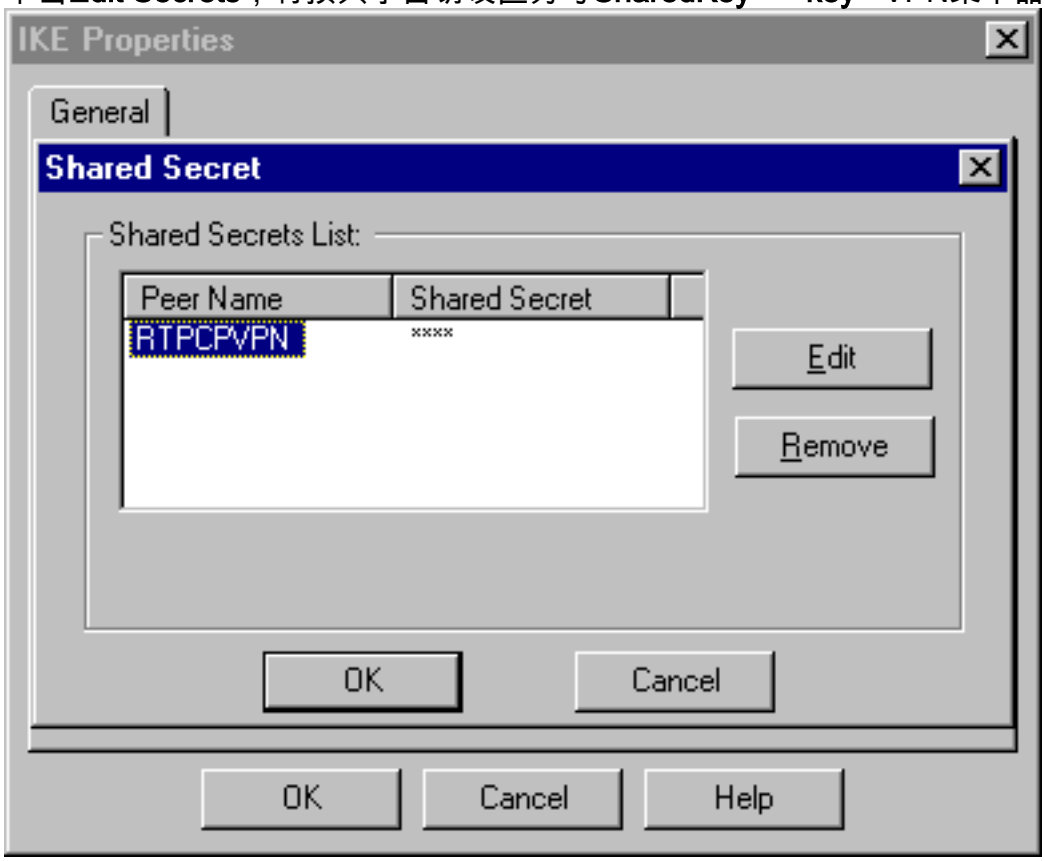



10. 将IKE属性更**改为**DES加**密和SHA1**散列以**与SHA_DES_G2 VPN集中器**命令一致。**注意**：“G2”是指Diffie-Hellman组1或2。在测试中，发现检查点接受“G2”或“G1”。更改这些设置：取消选定积极模式。选中 **Supports Subnets**。在“Authentication Method”下，选中 **Pre-**



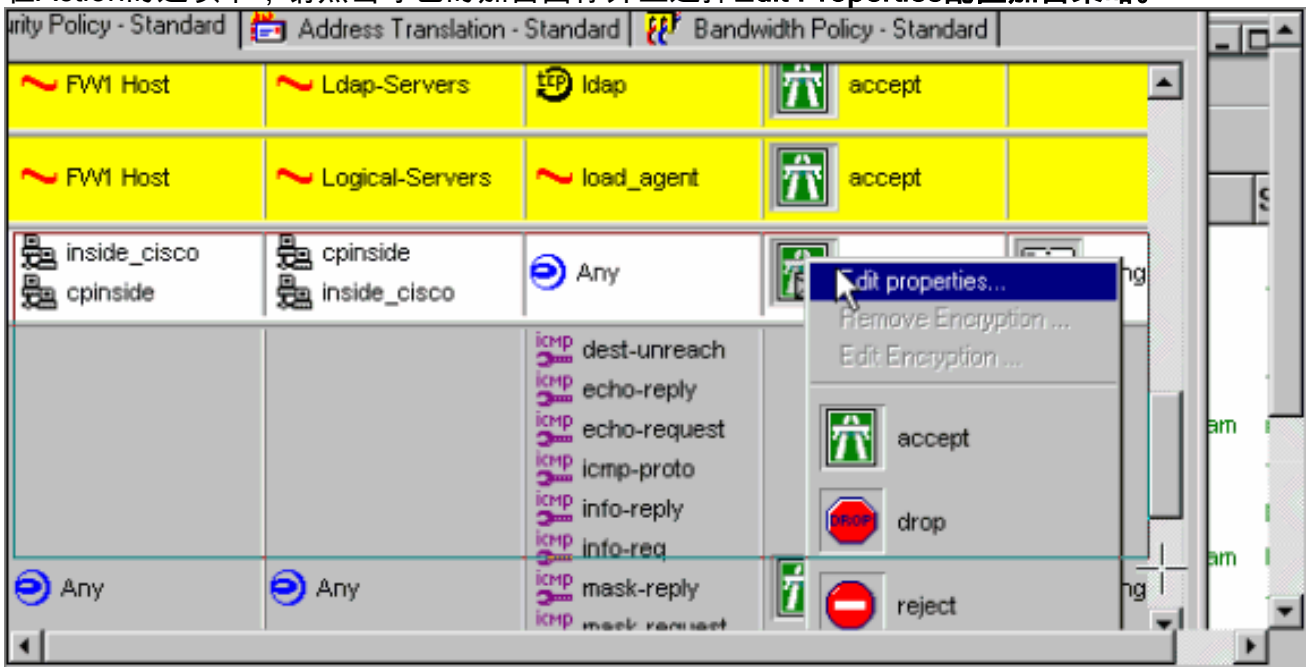

**Shared Secret。**

11. 单击**Edit Secrets**，将预共享密钥设置为与**SharedKey = <key>** VPN集中器命令一致。

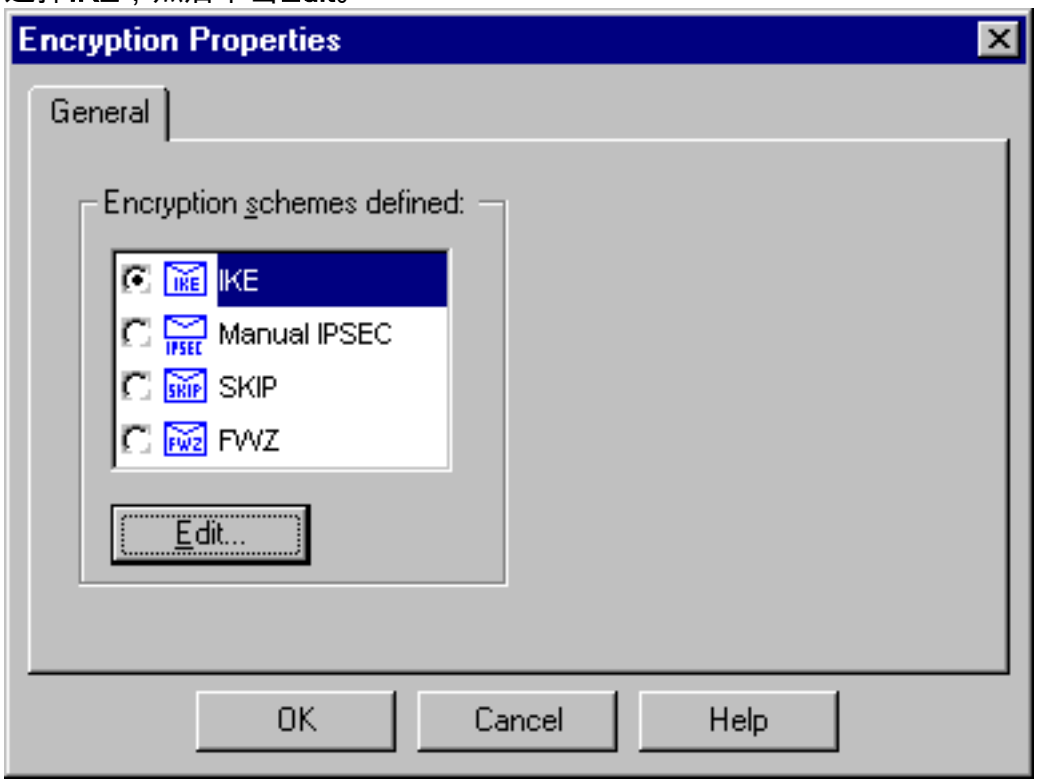



12. 在策略编辑器窗口，插入源和目的为“inside_cisco”和“cpinside”(双向)这一规则。 设置 **Service=Any、Action=Encrypt** 和 **Track=Long。**


13. 在Action的选项下，请点击绿色的加密图标并且选择**Edit Properties配置加密策略。**

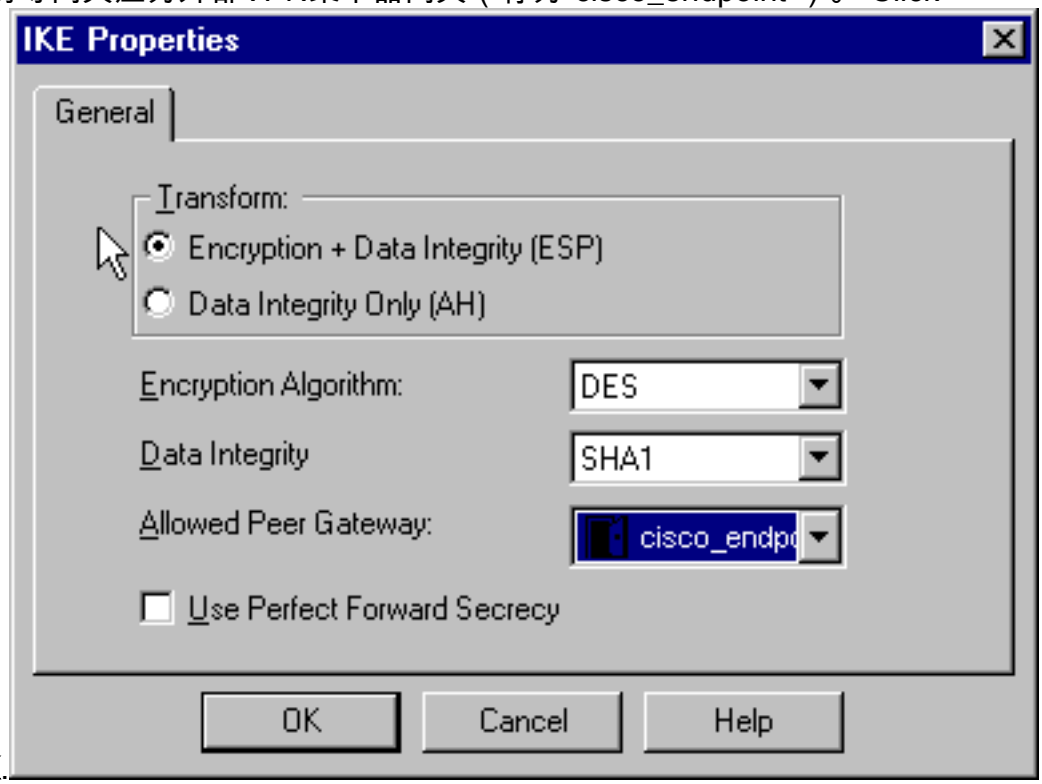



14. 选择**IKE**，然后单击**Edit**。




15. 在“IKE属性”窗口中，更改这些属性以与**Transform = esp(sha，des)VPN集中**器命令一致。下

面请变换，选择**加密+数据完整性(ESP)**。 加密算法应为**DES**，数据完整性应为**SHA1**，允许的对等网关应为外部VPN集中器网关（称为“cisco_endpoint”）。 Click OK.




16. 配置 Checkpoint 之后，在 Checkpoint 菜单上选择 **Policy > Install，使所做的更改生效。**

# 验证

当前没有可用于此配置的验证过程。

# 故障排除

## VPN 5000 集中器故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

**注意：在**使用debug命令之前，请参阅有关Debug命**令的**重要信息。

- **vpn trace dump all** — 显示有关所有匹配VPN连接的信息，包括有关时间、VPN编号、对等体的实际IP地址、已运行脚本以及发生错误的软件代码的例程和行号的信息。
- **show system log buffer** — 显示内部日志缓冲区的内容。
- **show vpn statistics** — 显示用户、合作伙伴的此信息以及两者的总信息。(对于模块化型号，显示器包括每个模块插槽的部分。请参阅“调试输出示例”部分。)(Current Active) — 当前活动连接。Negot — 当前协商连接。High Water — 自上次重新启动以来并发活动连接的最大数量。Running Total — 自上次重新启动以来成功连接的总数。Tunnel OK — 没有错误的隧道数。Tunnel Starts — 隧道启动数。Tunnel Error — 有错误的隧道数。
- **show vpn statistics verbose** — 显示ISAKMP协商统计信息和更多活动连接统计信息。

## 网络汇总

当多个相邻网络内部在检查点的时加密域配置，设备也许自动地总结他们关于关注数据流的情况。如果 VPN 集中器未配置为匹配，则隧道可能会出现故障。例如，如果 10.0.0.0/24 和 10.0.1.0/24 的内部网络已配置为包含在隧道中，则它们可能将汇总到 10.0.0.0/23。

## Checkpoint 4.1 防火墙Debug

这是Microsoft Windows NT安装。由于跟踪在“策略编辑器”（如步骤12所示）中设置为“长”，因此，在日志查看器中，被拒绝的流量应显示为红色。可通过以下方式获得更详细的调试：

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

并且在另一个窗口：

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

发出以下命令以清除检查点上的安全关联(SA):

```
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
```

在出现“Are you sure?”提示时，回答 **yes**提示。

## 调试输出示例

```
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
```

# 相关信息

- Cisco VPN 5000 系列集中器终止销售公告
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems