配置IPSec隧道-对检查点4.1防火墙的Cisco VPN 5000集中器

目录

简介

本文展示如何形成有预先共享密钥的一个IPSec隧道加入两私有网络。它加入一私有网络在Cisco VPN 5000集中器(192.168.1.x)里面对一私有网络在检查点4.1防火墙(10.32.50.x)里面。假设，从VPN集中器和里面里边的流量对互联网的Checkpoint (代表在本文通过172.18.124.x网络)流，在您开始此配置前。

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。

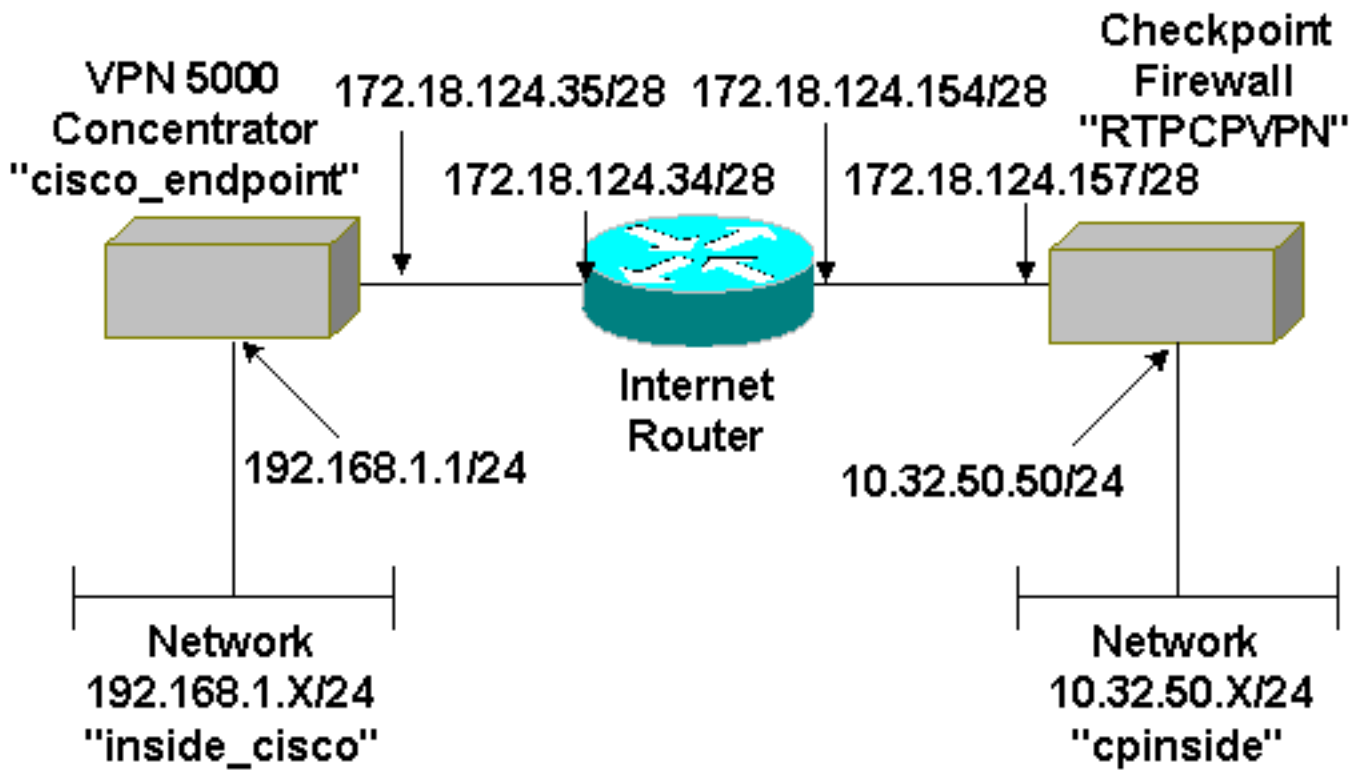
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

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。

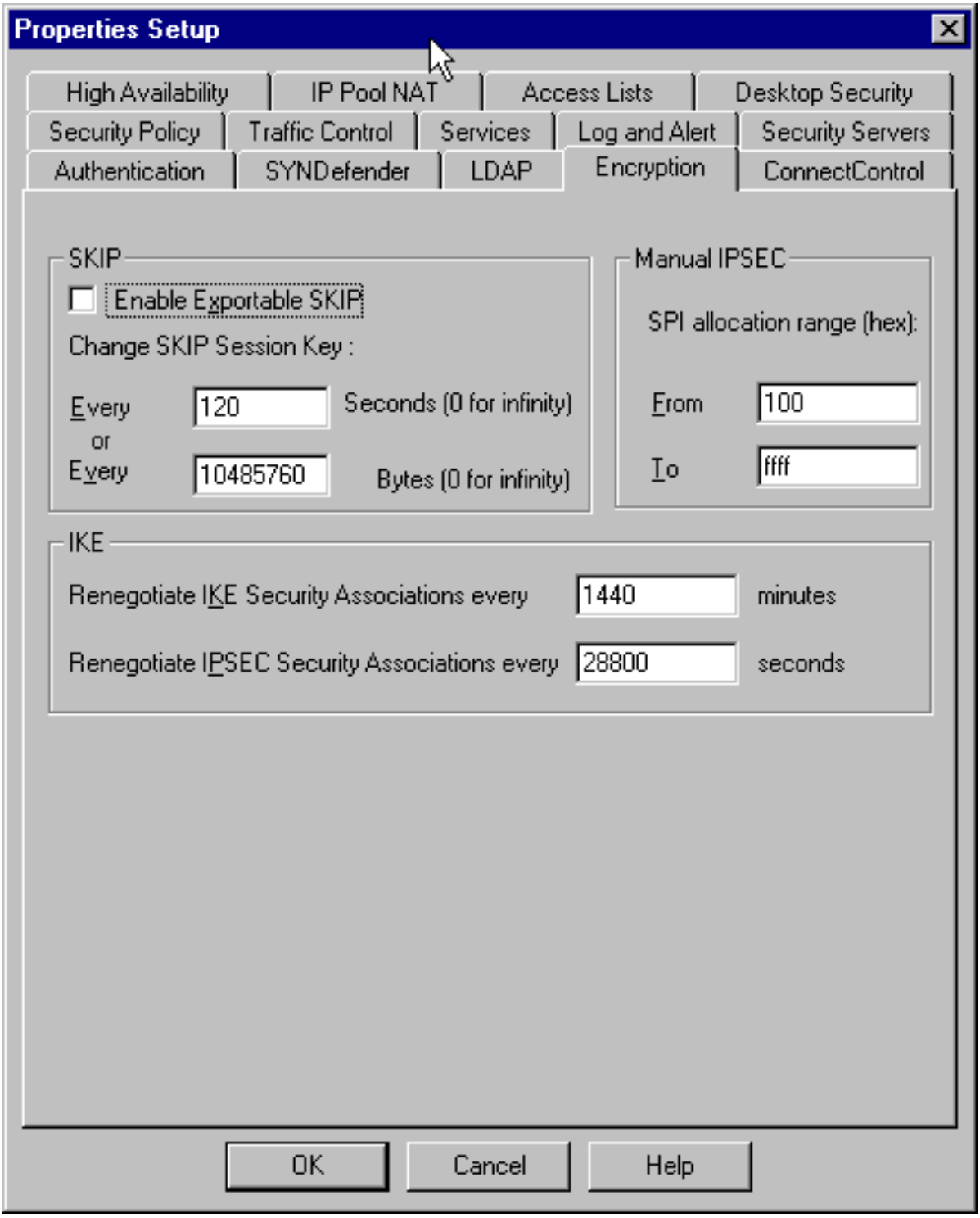
Cisco VPN 5000 集中器
[IP Ethernet 0:0] Mode = Routed SubnetMask = 255.255.255.0 IPAddress = 192.168.1.1

```
[ 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.
```

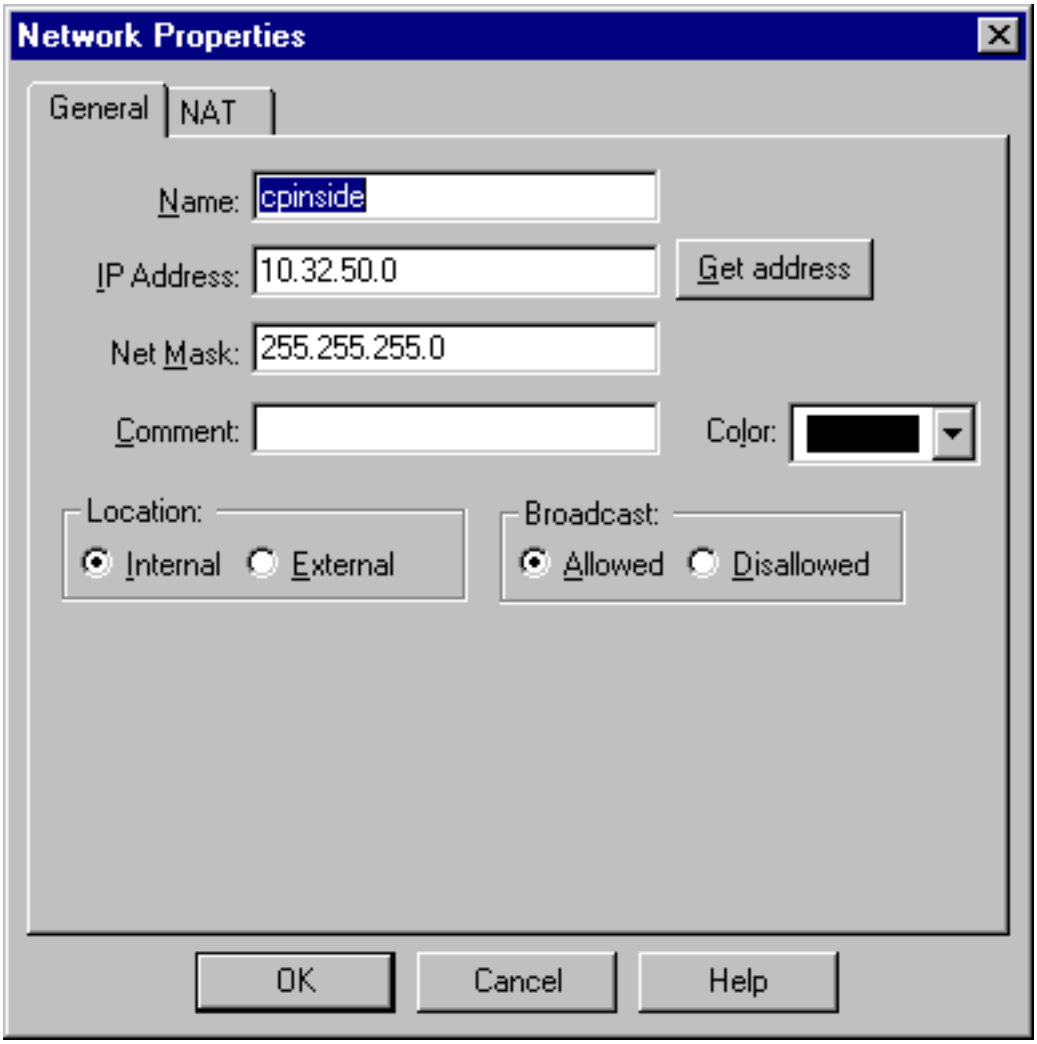
检查点 4.1 防火墙

完成以下步骤，以配置检查点 4.1 防火墙。

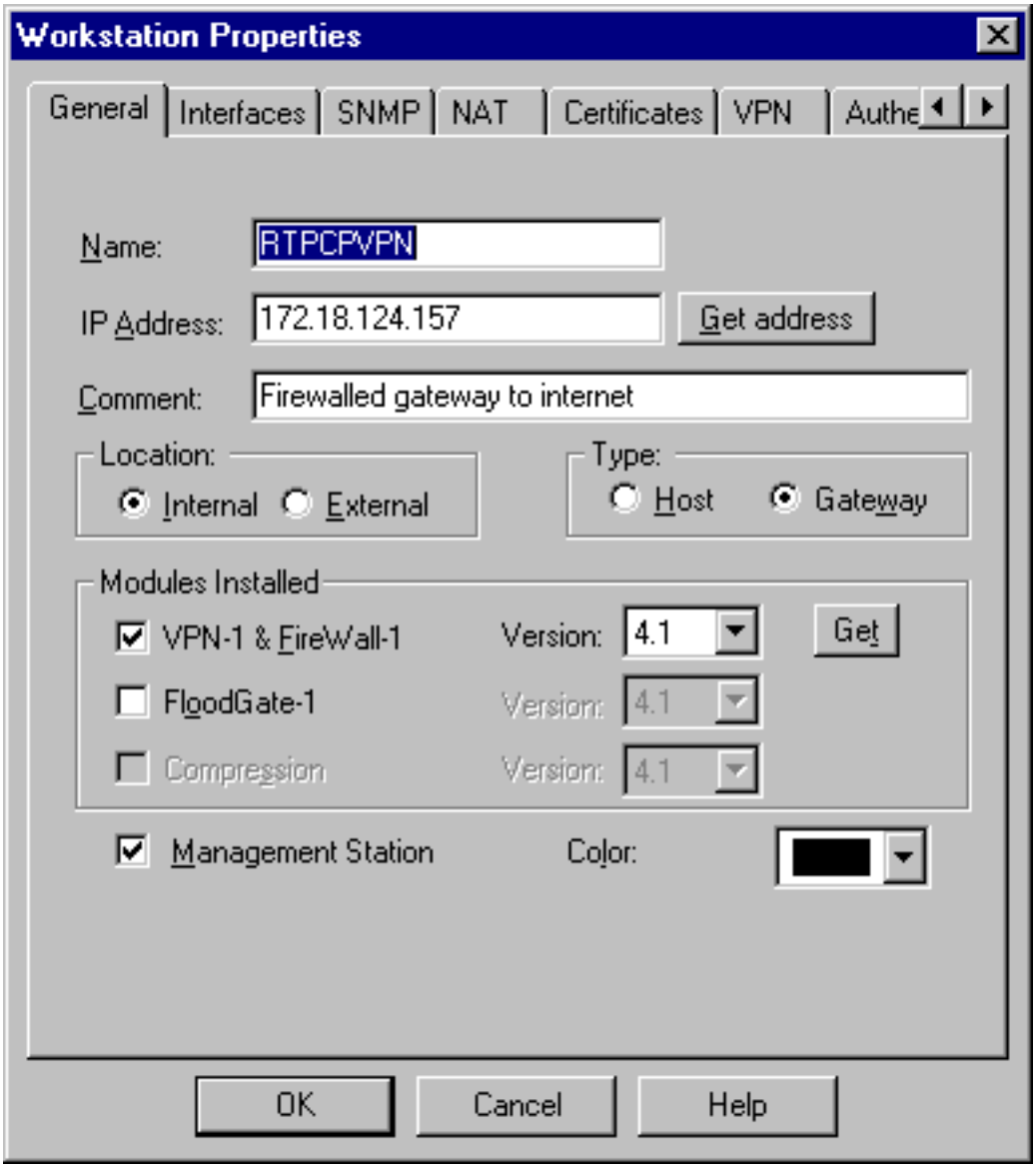
1. 选择**Properties > Encryption**设置Checkpoint IPSec寿命同意**KeyLifeSecs = 28800** vpn concentrator命令。**注意：** 留下Checkpoint Internet Key Exchange (IKE)寿命在默认。



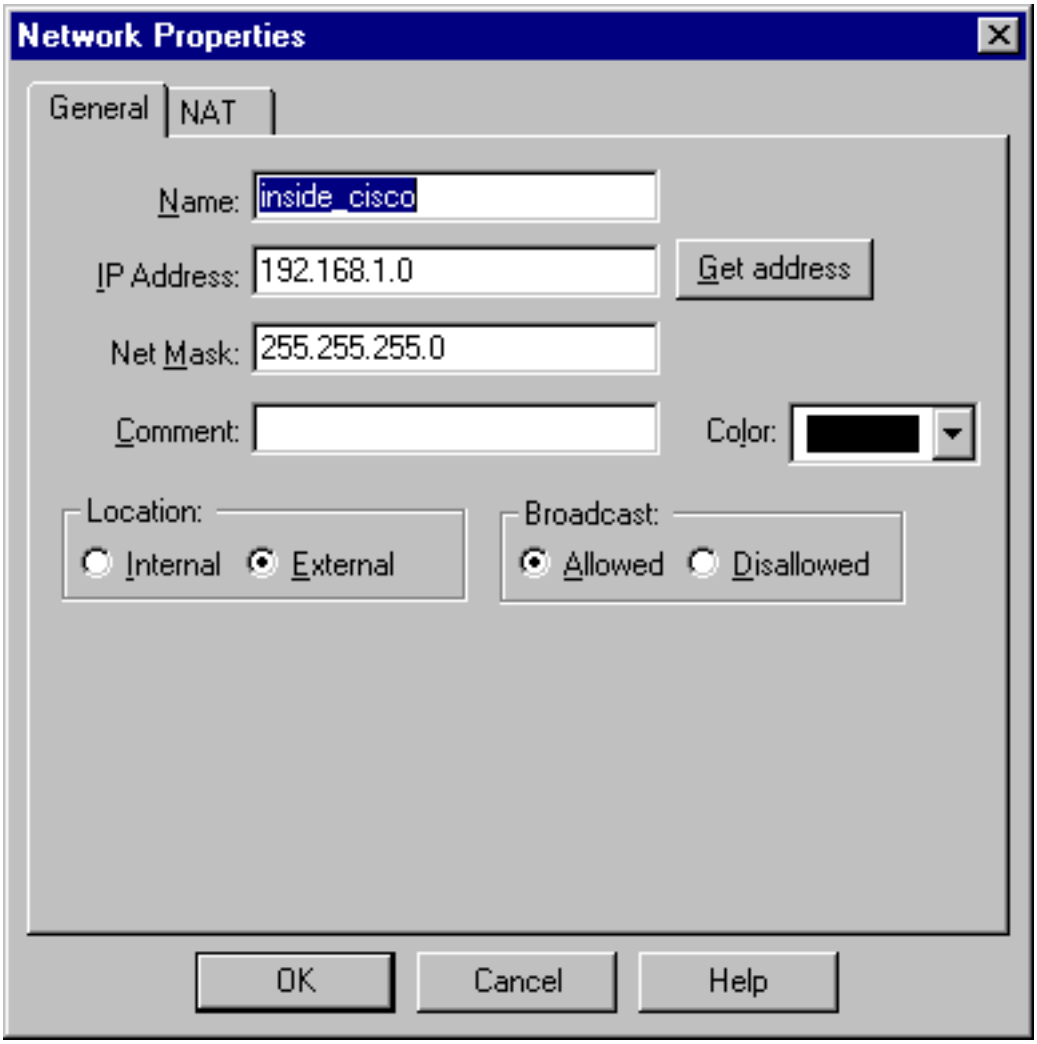
2. "选择Manage > Network objects > New (或 Edit) > Network，配置Checkpoint后的内部(""cpinside"") 网络的对象。"这应该与**对等体一致= "10.32.50.0/24"** vpn concentrator命令。



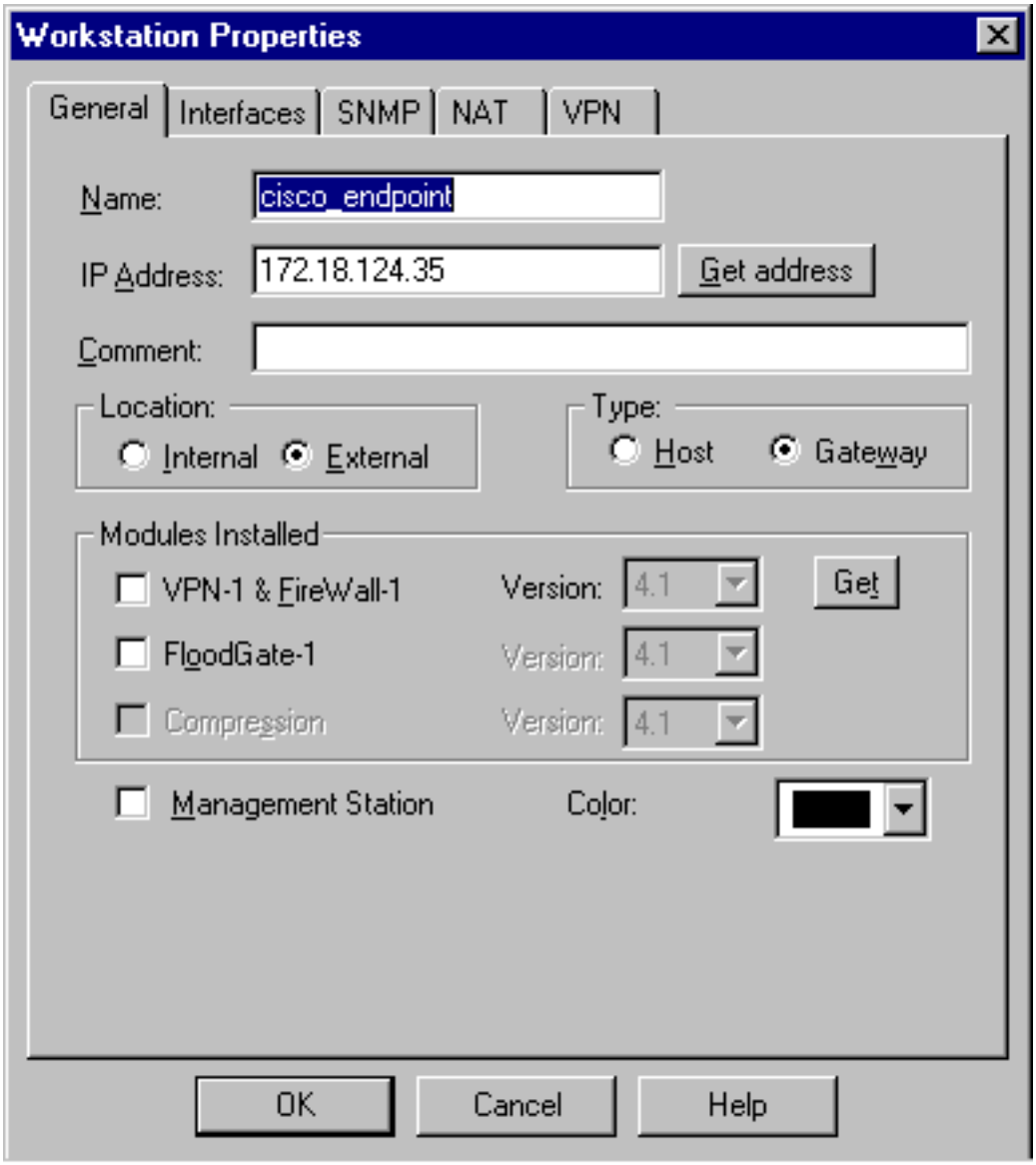
3. 选择**Manage > Network objects > Edit**编辑该网关(“RTPCPVPN” Checkpoint)的终端的对象对在**Partner = <ip>命令的**VPN集中器点。在“Location”下选择 **Internal**。选择类型的**网关**。检查**VPN-1 & FireWall-1**和**管理站**在安装的模块下。



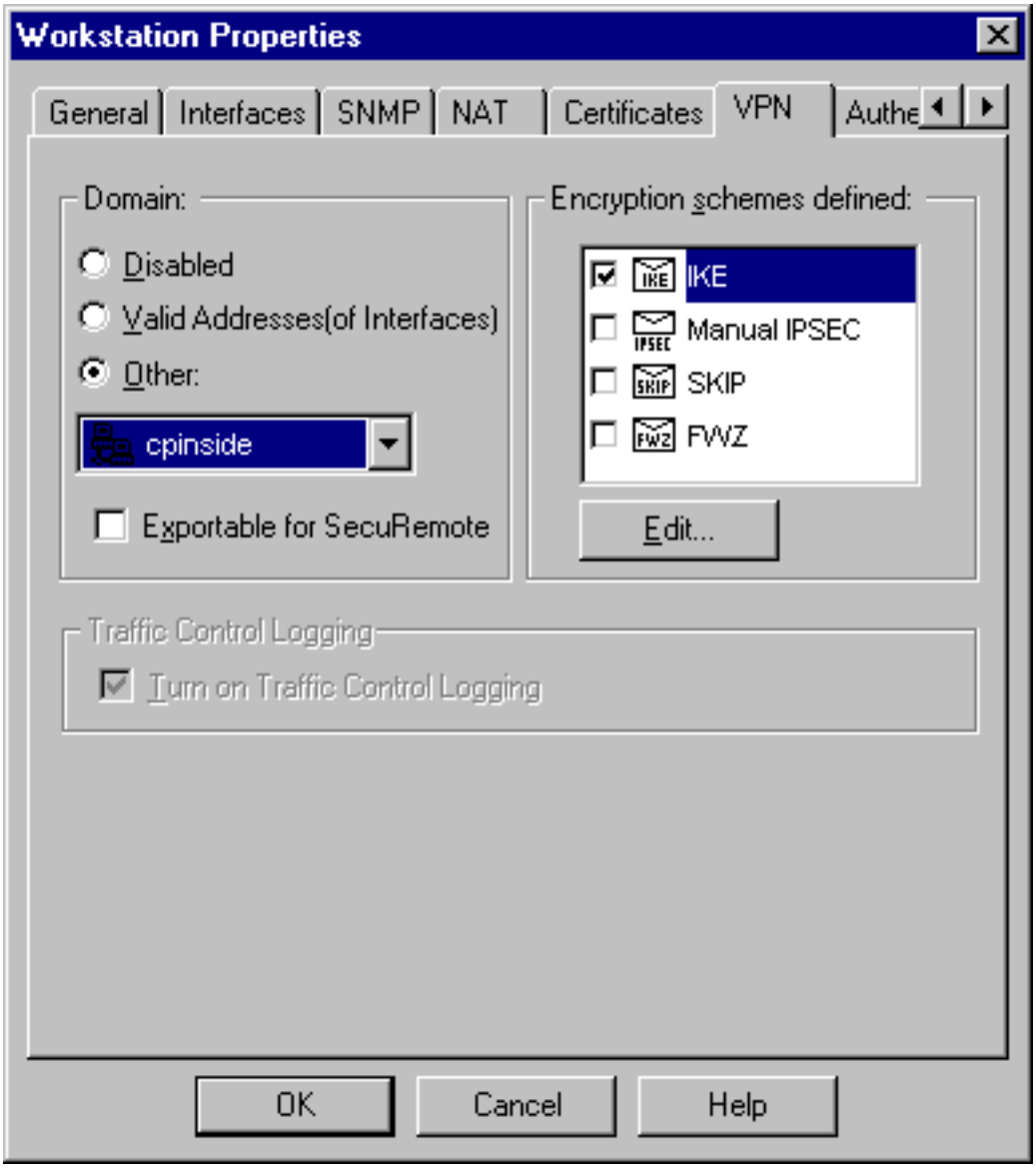
4. 选择 **Manage > Network objects > New (or Edit) > Network** 以配置 VPN 集中器后部的外部 ("inside_cisco") 网络的对象。这应该与vpn concentrator命令的**LocalAccess =的<192.168.1.0/24>一致**。



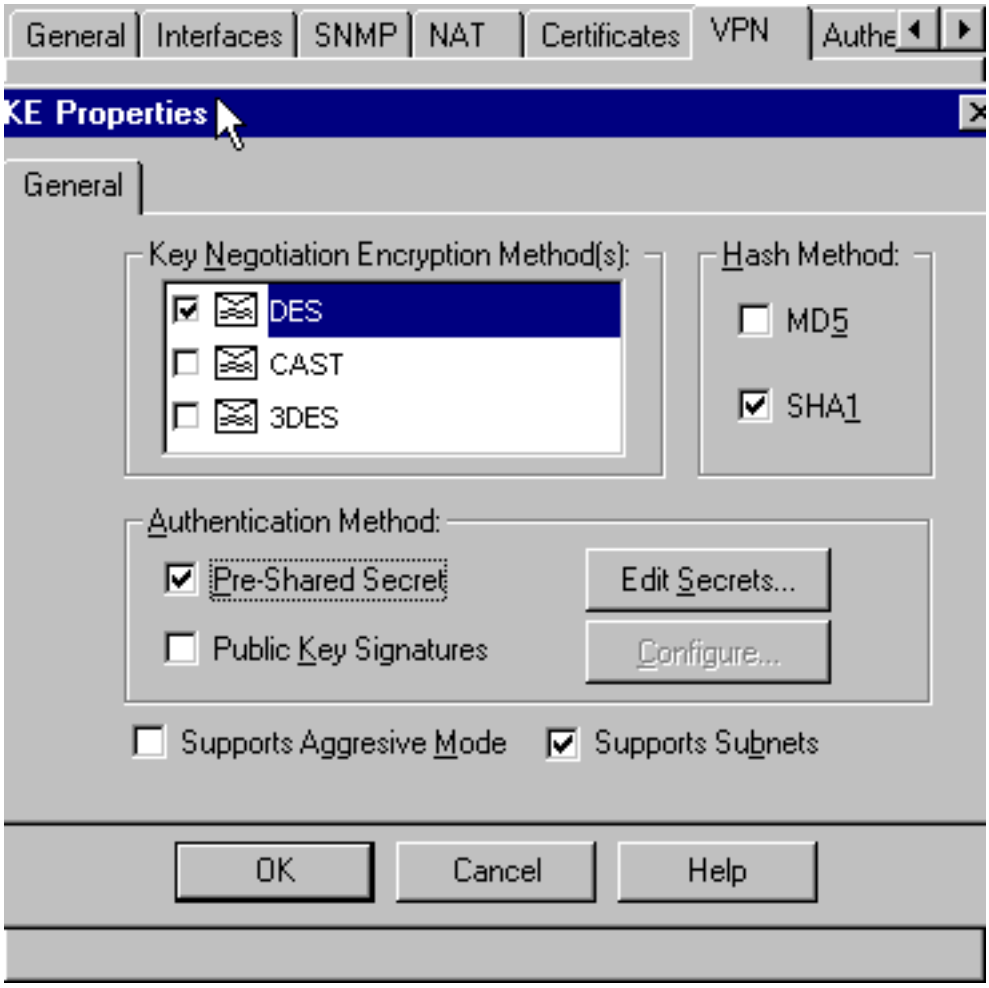
5. 选择 **Manage > Network objects > New > Workstation**，为外部 ("cisco_endpoint") VPN 集中器网关添加对象。这是VPN集中器的“外部”接口有连接的对Checkpoint (在本文，172.18.124.35是在**IPAddress = <ip>命令的**IP地址)。在“Location”下选择 **External**。选择类型的**网关**。**注意：** 请勿检查VPN-1/FireWall-1。



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**。

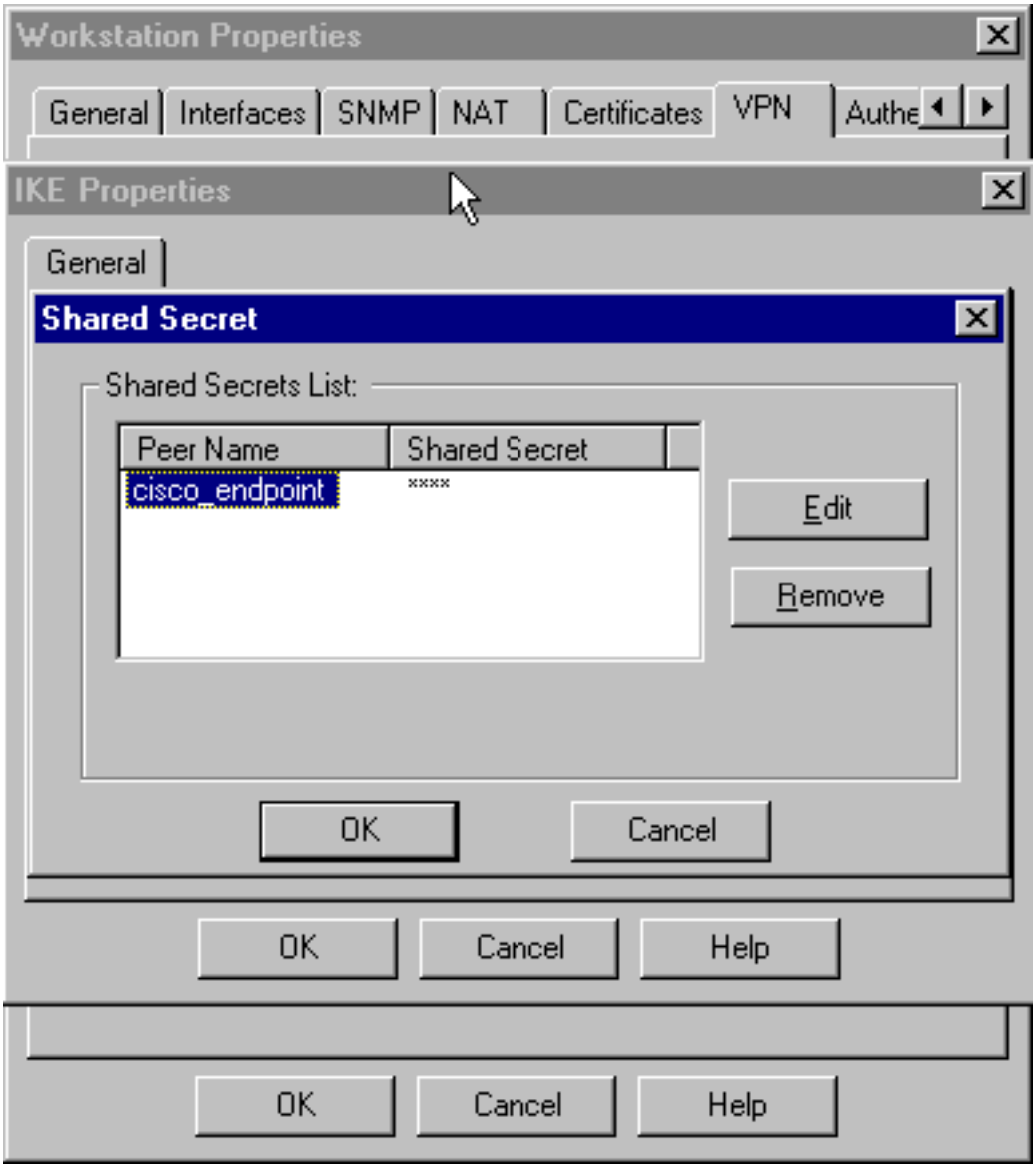


7. 更改切细IKE属性对**DES加密**和的**SHA1**同意**SHA_DES_G2 VPN**集中器命令。**注意：** "G2"参阅Diffie-Hellman group1或2。在测试，发现Checkpoint收下"G2"或"G1."更改这些设置：取消选定积极模式。选中 **Supports Subnets**。在“Authentication Method”下，选中 **Pre-Shared**

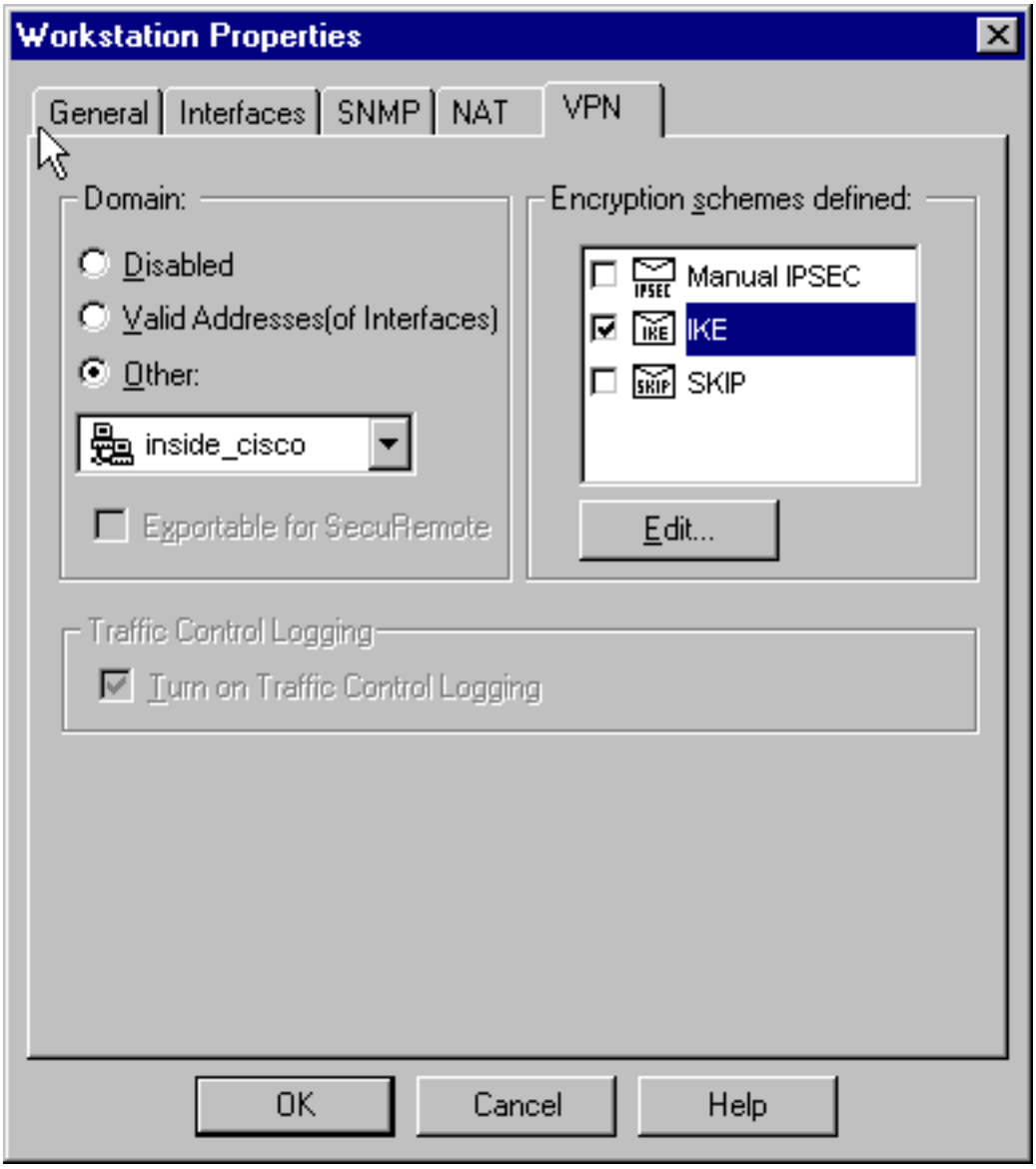


Secret。

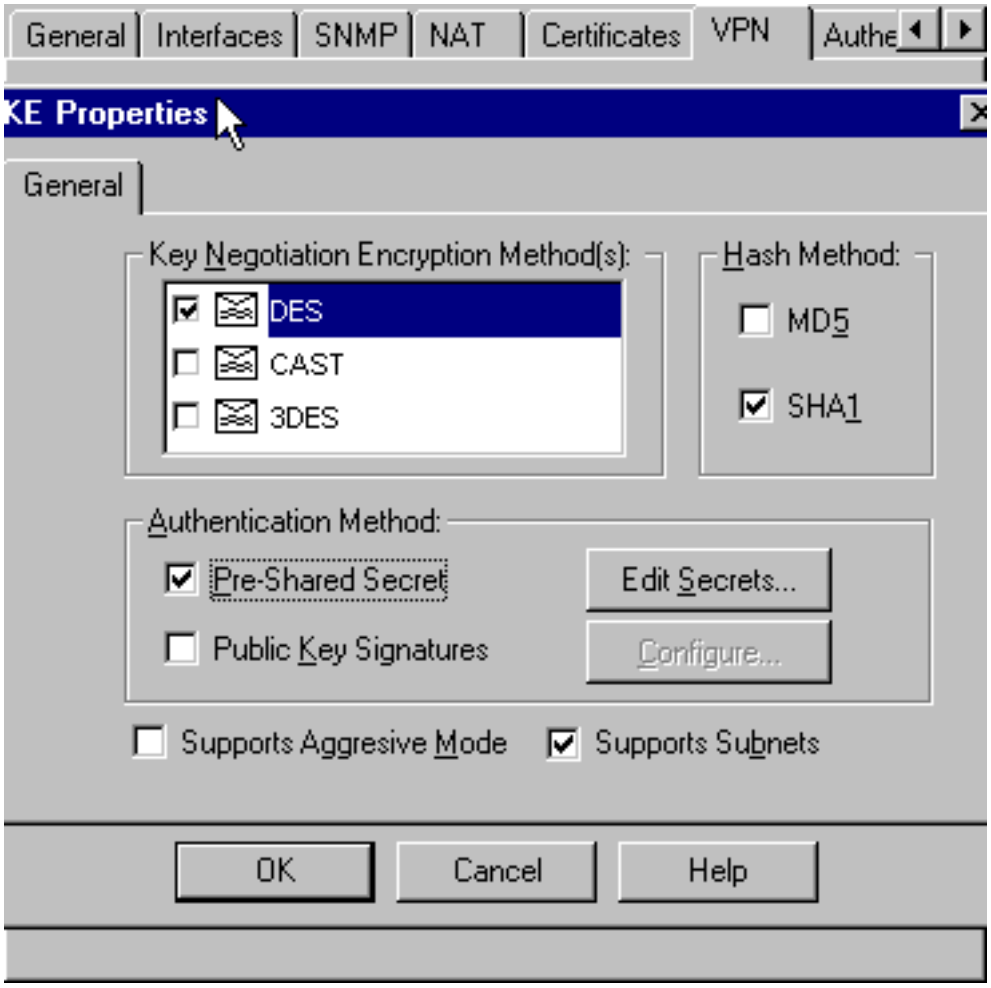
8. 单击**编辑秘密**设置预先共享密钥同意**Sharedkey= <key> VPN**集中器命令。



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

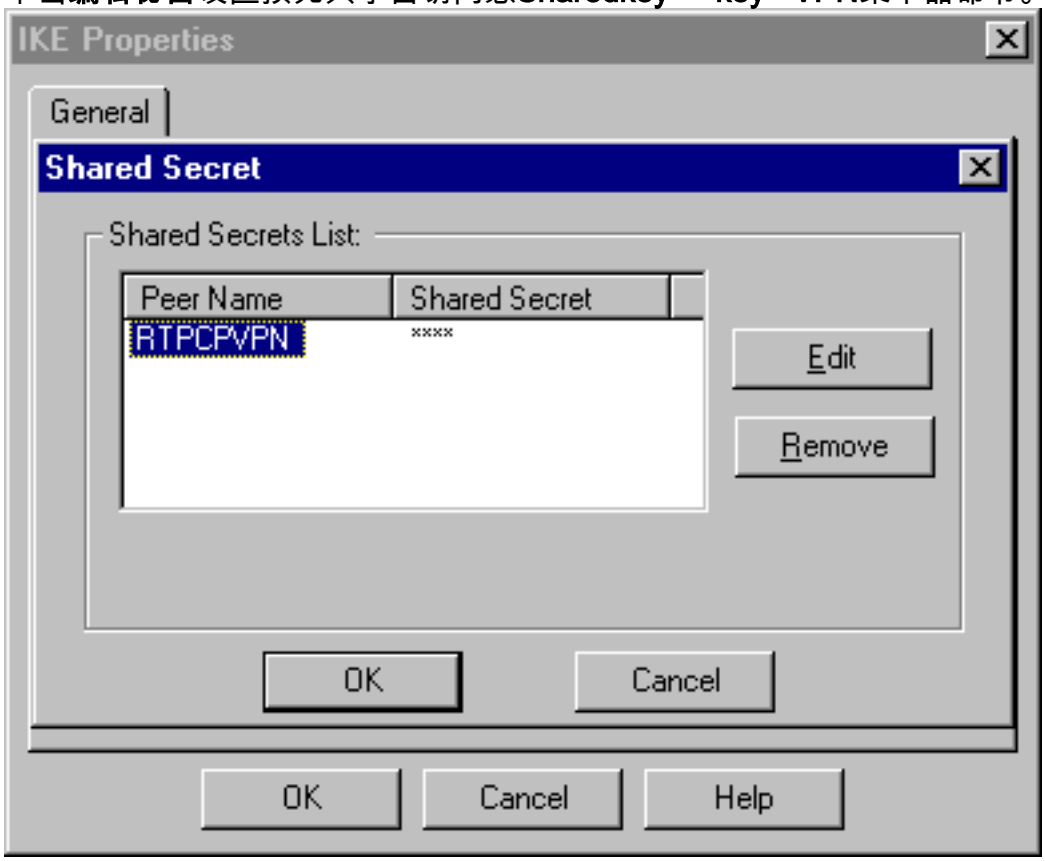


10. 更改切细IKE属性对**DES加密**和的**SHA1**同意**SHA_DES_G2 VPN**集中器命令。**注意：** "G2"参阅Diffie-Hellman group1或2。在测试，发现Checkpoint收下"G2"或"G1."更改这些设置：取消选定积极模式。选中 **Supports Subnets**。在“Authentication Method”下，选中 **Pre-Shared**



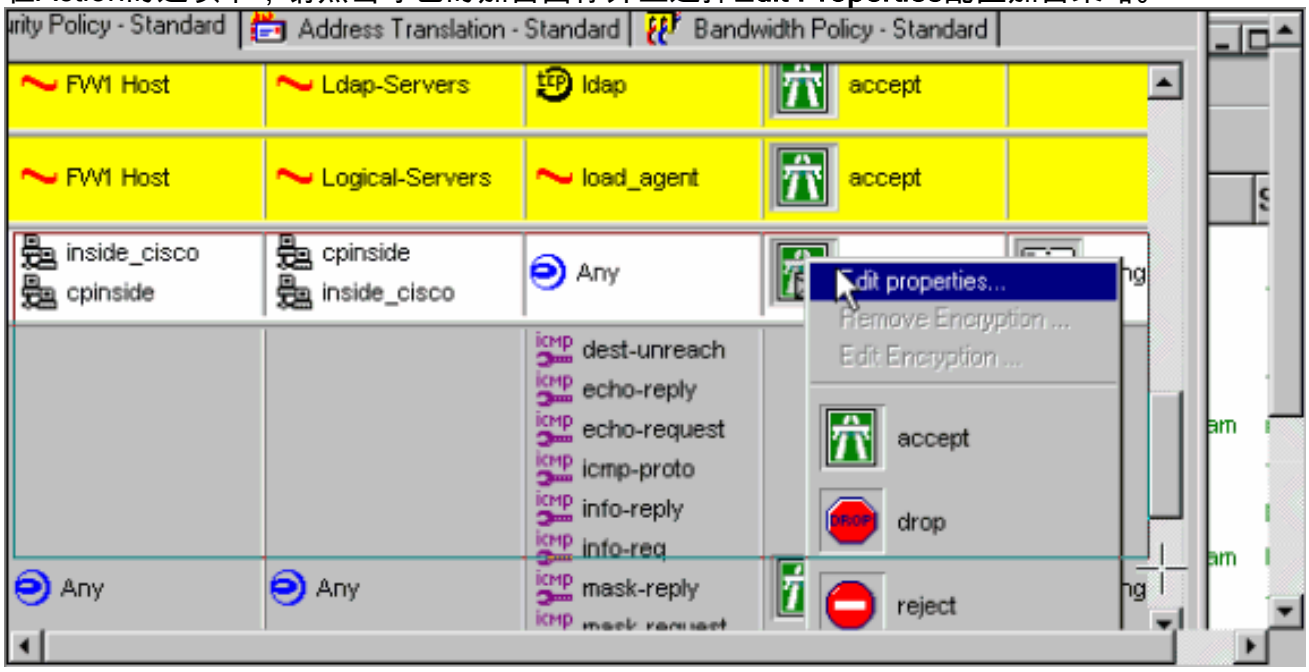
Secret。

11. 单击**编辑秘密**设置预先共享密钥同意**Sharedkey= <key> VPN**集中器命令。

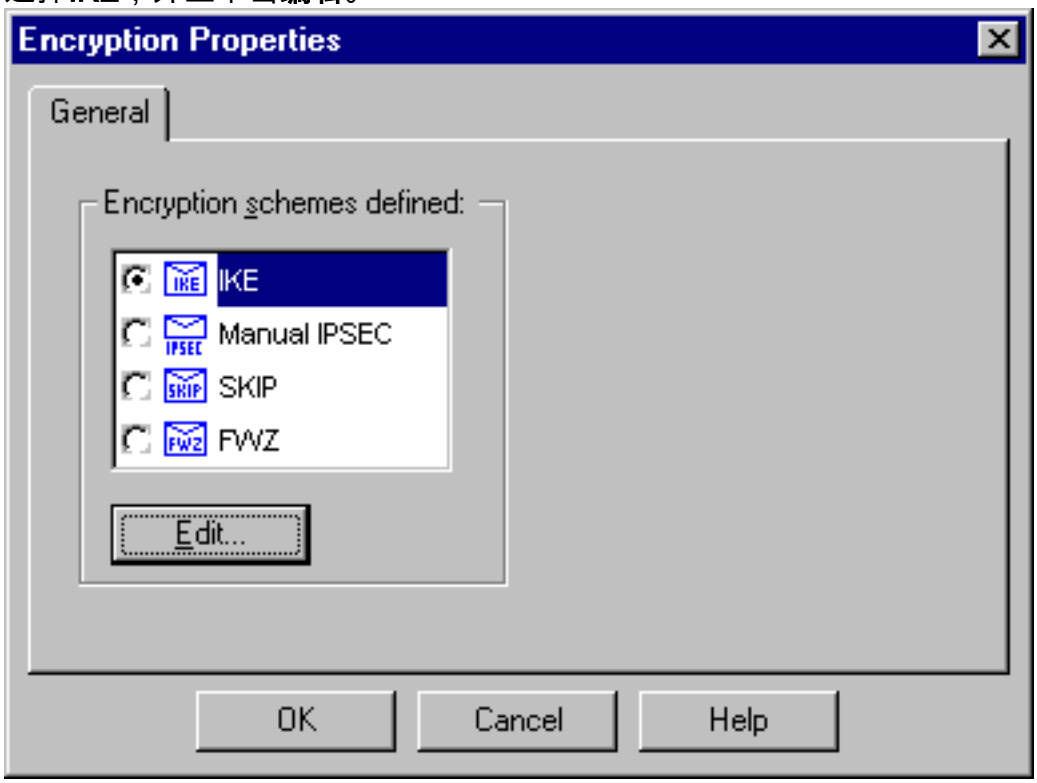


12. 在策略编辑器窗口，插入源和目的为“inside_cisco”和“cpinside”(双向)这一规则。设置 **Service=Any、Action=Encrypt** 和 **Track=Long**。

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。

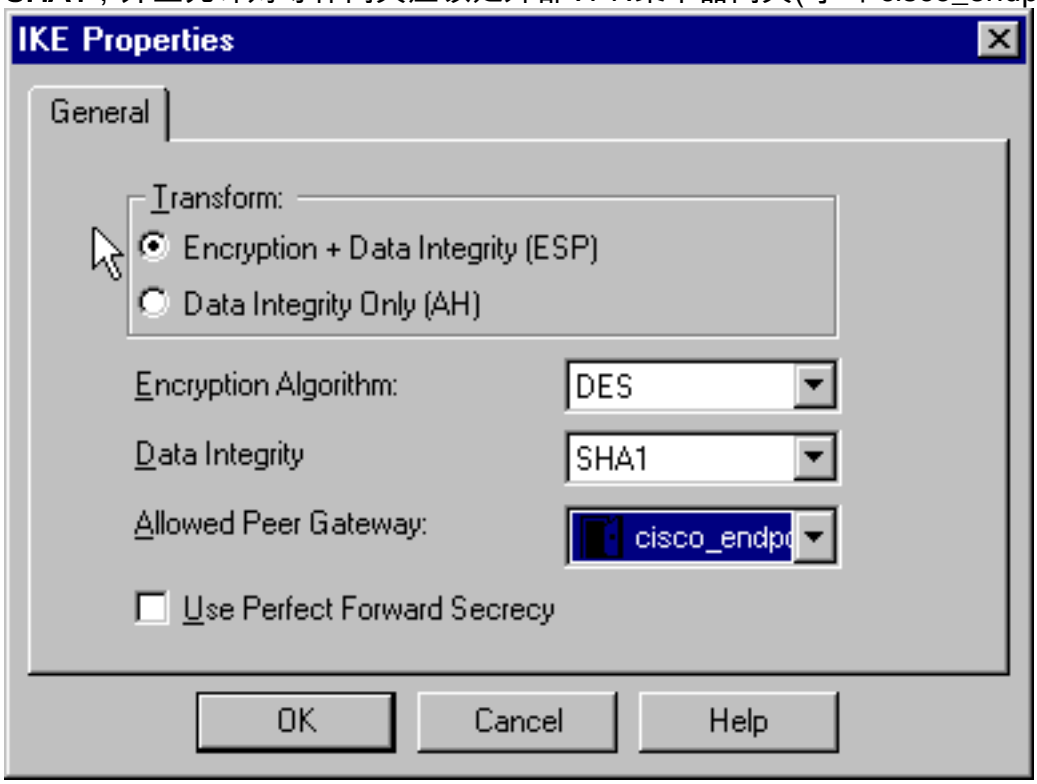


14. 选择**IKE**，并且单击**编辑**。



15. 在IKE Properties窗口，请更改这些属性同意**转换=特别是(sha， des)** vpn concentrator命令

。下面请变换，选择**加密+数据完整性(ESP)**。加密算法应该是**DES**，数据完整性应该是**SHA1**，并且允许对等体网关应该是外部VPN集中器网关(呼叫“cisco_endpoint”)。单击 **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： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **全的vpn trace dump**显示关于所有匹配VPN连接的信息，包括关于时间、VPN编号、对等体的实际IP地址，脚本运行了和一旦错误，错误出现软件代码的惯例和线路号的信息。
- **show system log buffer** —显示内部日志缓冲区的内容。
- **show vpn statistics** —显示用户、合作伙伴和总计的此信息两个的。(对于模块化模型，显示包括每模块插槽的一个部分。参考Sample Debug Output部分。)—当前活动连接。`Negot` —当前协商的连接。并发活跃连接较高的值从最后重新启动。—成功的连接总数从最后重新启动。`Tunnel OK` —没有错误通道的数量。—通道开始数量。—通道数量有错误的。
- **show vpn statistics verbose** —显示ISAKMP协商统计数据和许多激活连接统计数据。

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。由于跟踪为在策略编辑器窗口的设置(如在步骤12中看到)，拒绝的数据流在日志查看器应该用红色出现为红色。更多冗长的调试可以得到：

```
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
```

发出这些命令清除在检查点的安全关联(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