配置 IPSec 隧道 - Cisco VPN 3000 集中器到 Checkpoint 4.1 防火墙

目录

简介

本文档说明如何使用预共享密钥来构建 IPSec 隧道以加入两个专用网络：

- 思科 VPN 3000 集中器 (192.168.1.x) 内部的一个专用网络。
- 检查点 4.1 防火墙 (10.32.50.x) 内部的一个专用网络。

假设在此配置开始之前，流量从 VPN 集中器内和检查点内流向互联网（本文档中用 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：

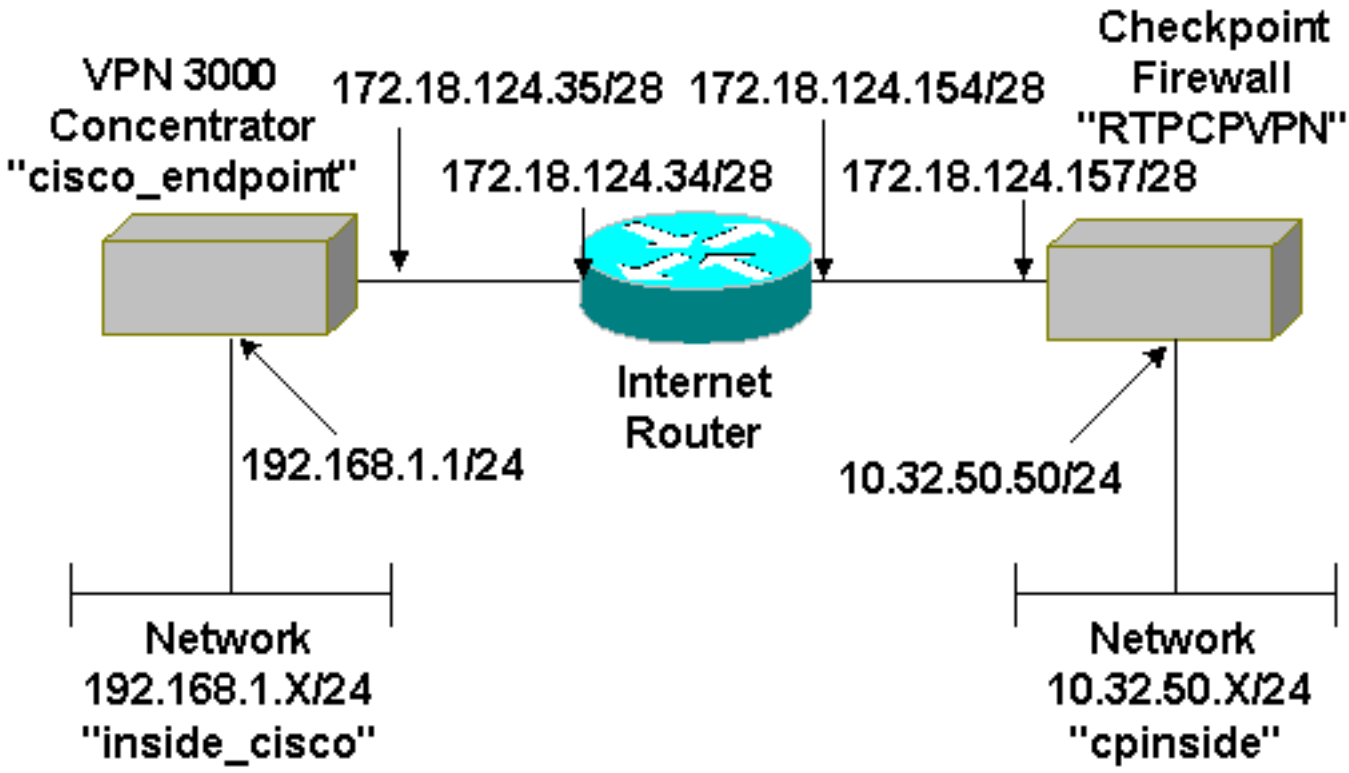
- VPN 3000 集中器

- VPN 3000 集中器软件 2.5.2.F 版本
- 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。

网络图

本文档使用以下网络设置：



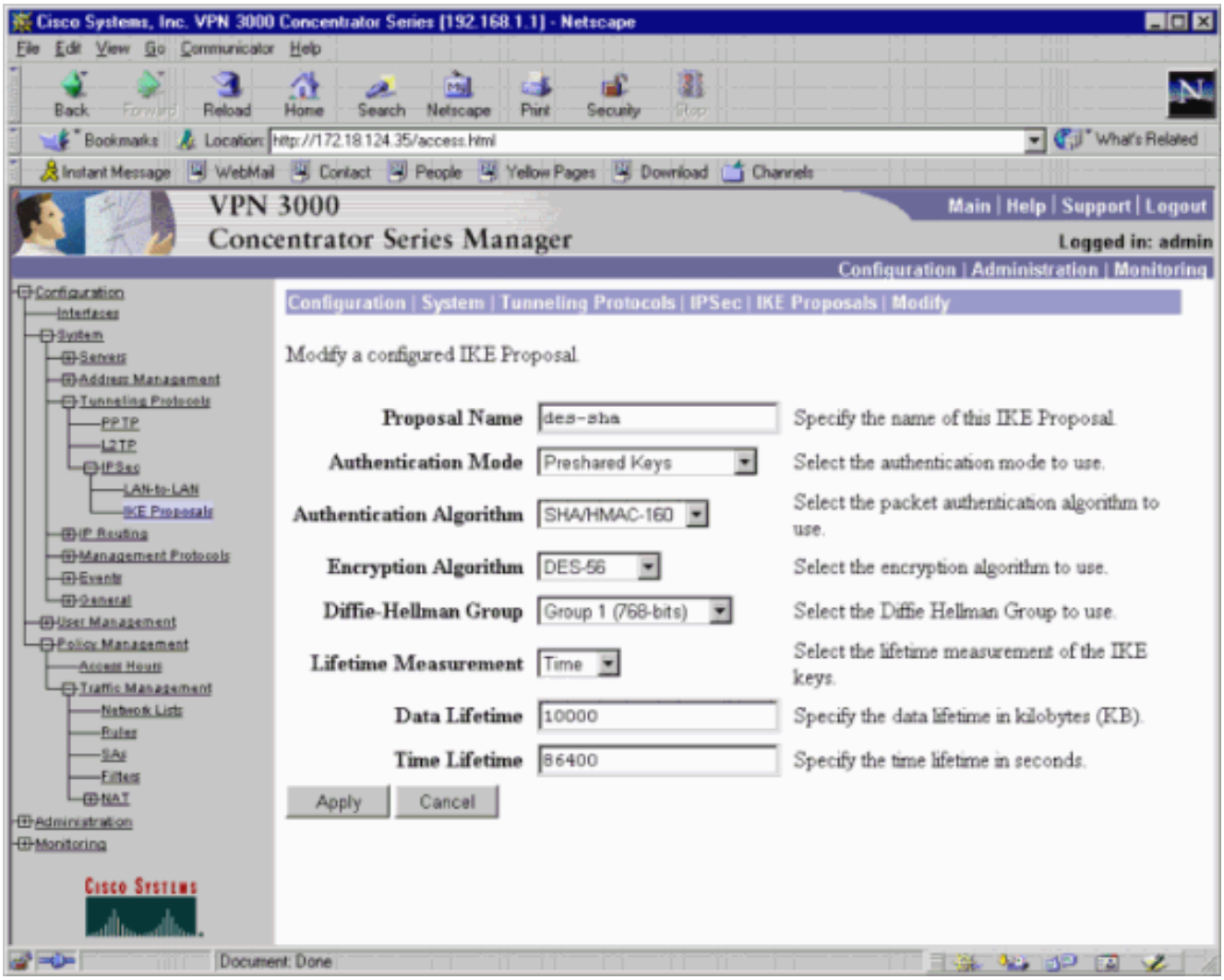
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

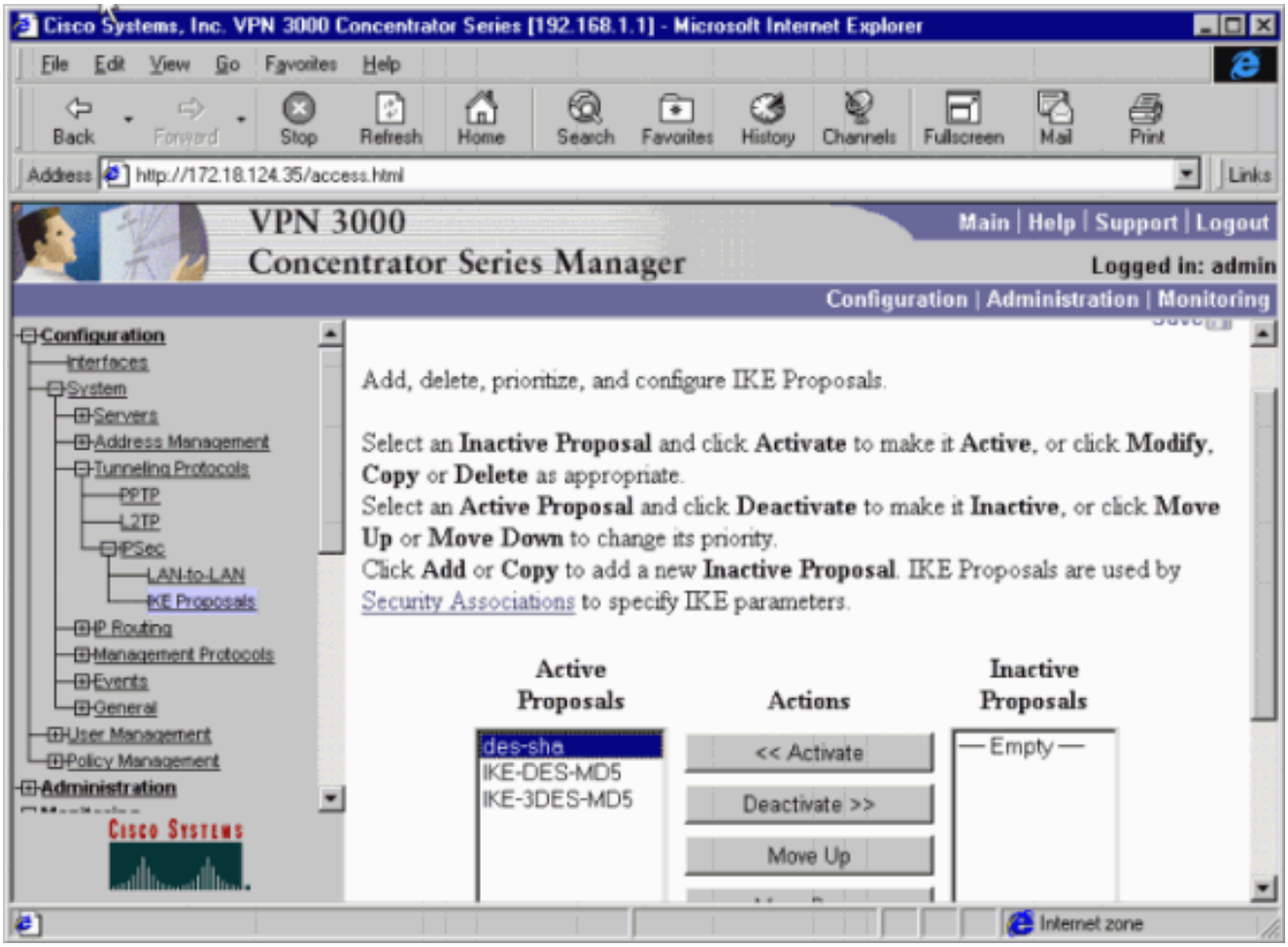
配置VPN 3000集中器

完成以下步骤，以配置 VPN 3000 集中器。

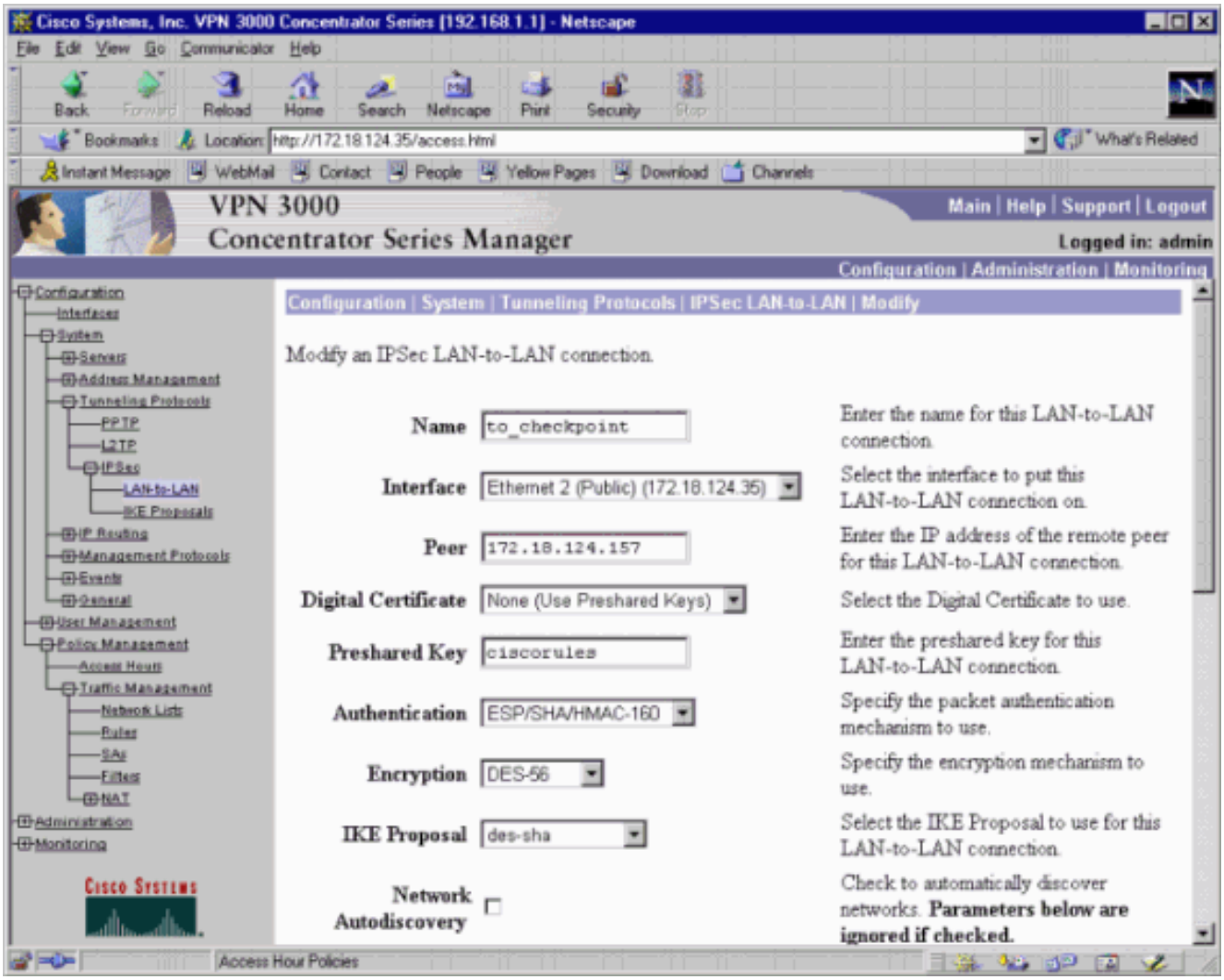
1. 选择 **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Modify**，使用安全哈希算法 (SHA) 哈希、数据加密标准 (DES) 和 Diffie-Hellman 组 1 创建名为 "des-sha" 的互联网密钥交换 (IKE) 协议。将生命周期保留为默认值 86400 秒。**注意：** VPN 集中器 IKE 生命周期的有效范围为 60-2147483647 秒。

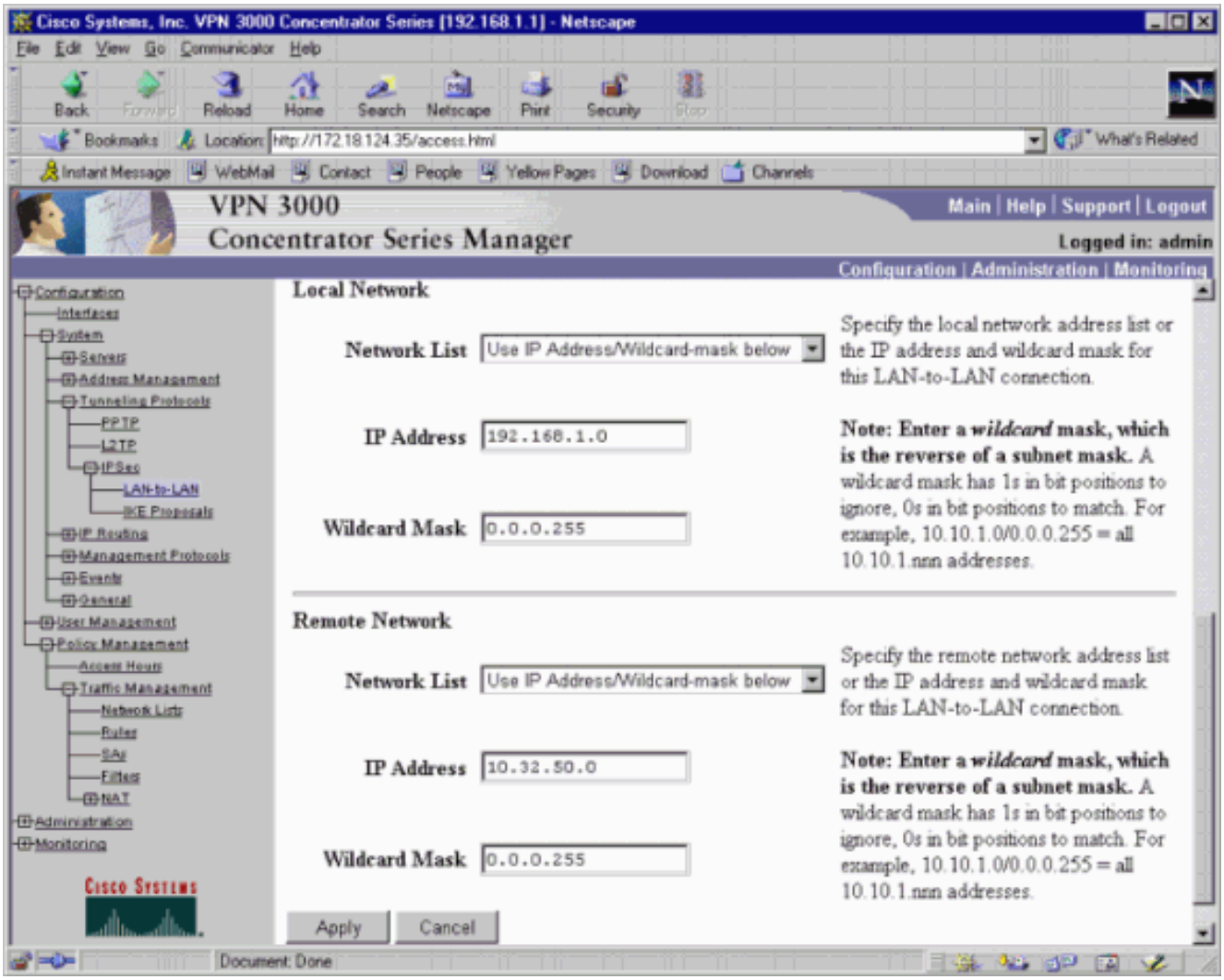


2. 选择 **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**。选择 "des-sha" 并点击 **Activate** 以激活 IKE 提议。

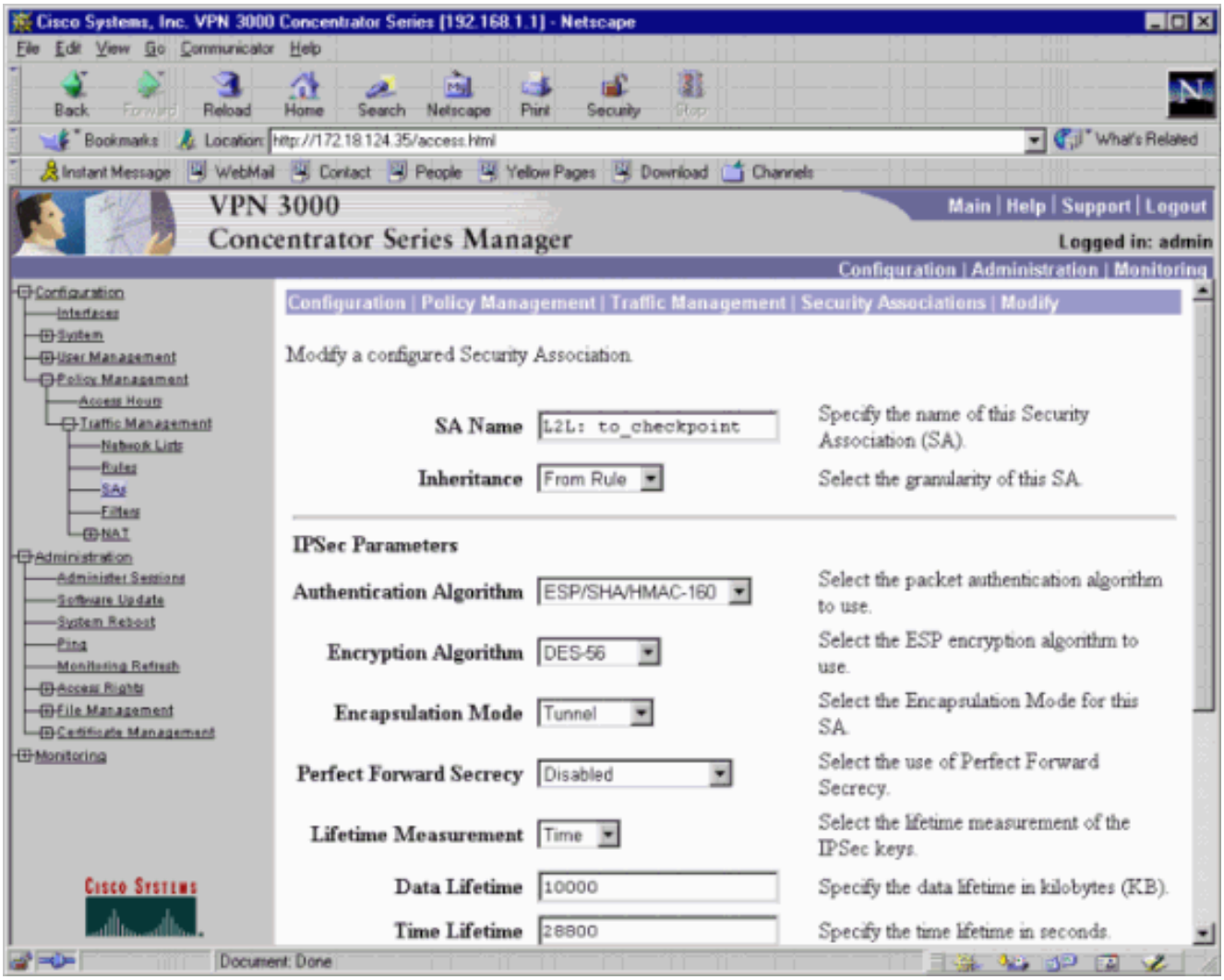


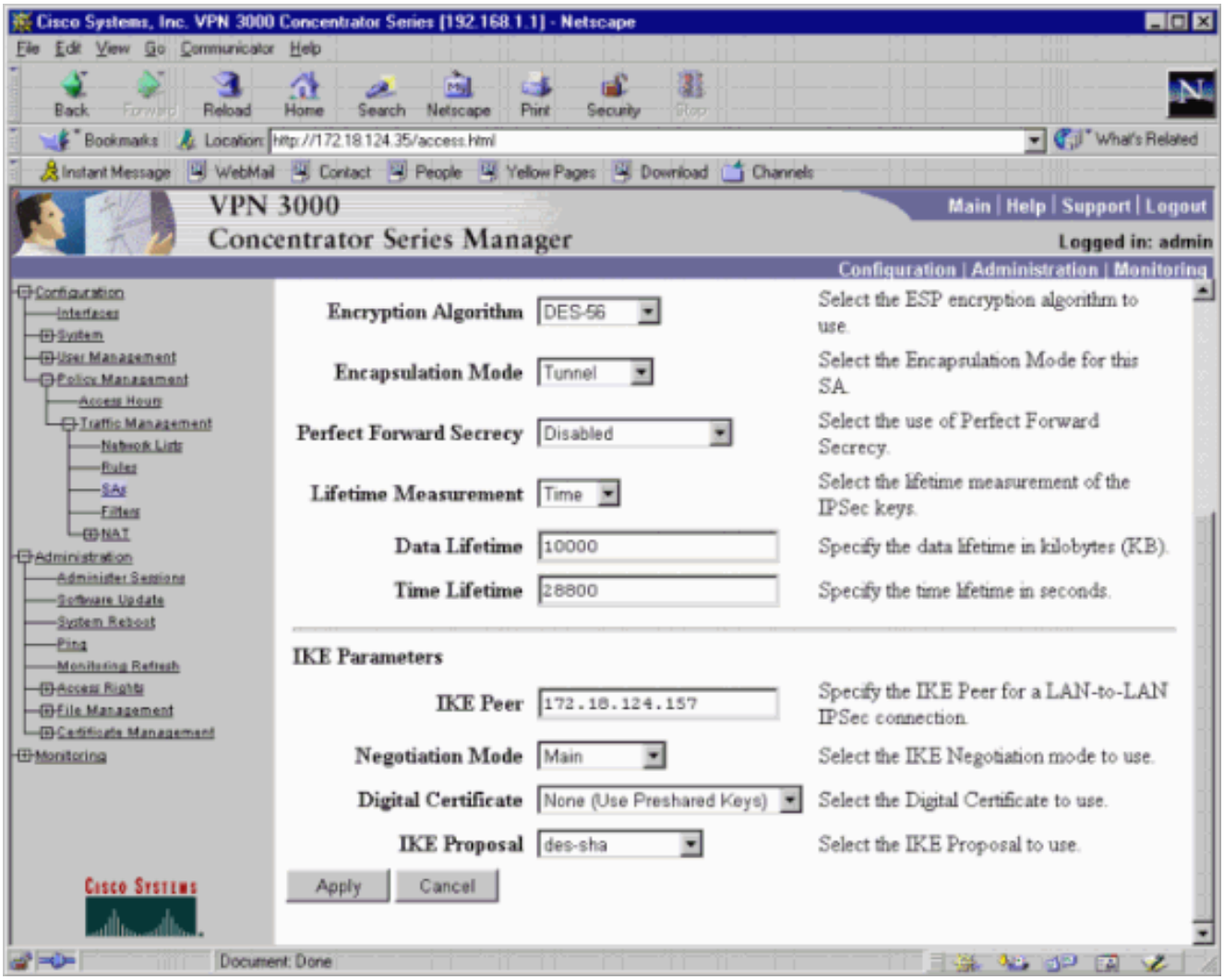
3. 选择 **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add**。使用检查点地址作为对等体，设置名为 "to_checkpoint" 的 IPSec 隧道。对于预共享密钥，请输入实际密钥。在 Authentication 下，选择 ESP/SHA/HMAC-160，然后选择 DES-56 for Encryption。输入 IKE 提议（本例中为 "des-sha"）以及本地网络和远程网络。


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
IP Routing
Management Protocols
Events
General
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify
Modify an IPSec LAN-to-LAN connection.
Name
to_checkpoint
Enter the name for this LAN-to-LAN connection.
Interface
Ethernet 2 (Public) (172.18.124.35)
Select the interface to put this LAN-to-LAN connection on.
Peer
172.18.124.157
Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate
None (Use Preshared Keys)
Select the Digital Certificate to use.
Preshared Key
ciscorules
Enter the preshared key for this LAN-to-LAN connection.
Authentication
ESP/SHA/HMAC-160
Specify the packet authentication mechanism to use.
Encryption
DES-56
Specify the encryption mechanism to use.
IKE Proposal
des-sha
Select the IKE Proposal to use for this LAN-to-LAN connection.
Network Autodiscovery
Check to automatically discover networks. Parameters below are ignored if checked.
Access Hour Policies



4. 选择 **Configuration > Policy Management > Traffic Management > Security Associations > Modify**。确认“完全向前保密”处于**禁用状态**，并将 IPsec 生命周期保留为默认值 **28800** 秒。**注意：** VPN 集中器 IPSec 生命周期的有效范围为 60-2147483647 秒。


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Administer Sessions
Software Update
System Reboot
Ping
Monitoring Refresh
Access Rights
File Management
Certificate Management
Monitoring
Cisco Systems
Configuration | Policy Management | Traffic Management | Security Associations | Modify
Modify a configured Security Association.
SA Name L2L: to_checkpoint Specify the name of this Security Association (SA).
Inheritance From Rule Select the granularity of this SA.
IPSec Parameters
Authentication Algorithm ESP/SHA/HMAC-160 Select the packet authentication algorithm to use.
Encryption Algorithm DES-56 Select the ESP encryption algorithm to use.
Encapsulation Mode Tunnel Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy Disabled Select the use of Perfect Forward Secrecy.
Lifetime Measurement Time Select the lifetime measurement of the IPSec keys.
Data Lifetime 10000 Specify the data lifetime in kilobytes (KB).
Time Lifetime 28800 Specify the time lifetime in seconds.
Document: Done

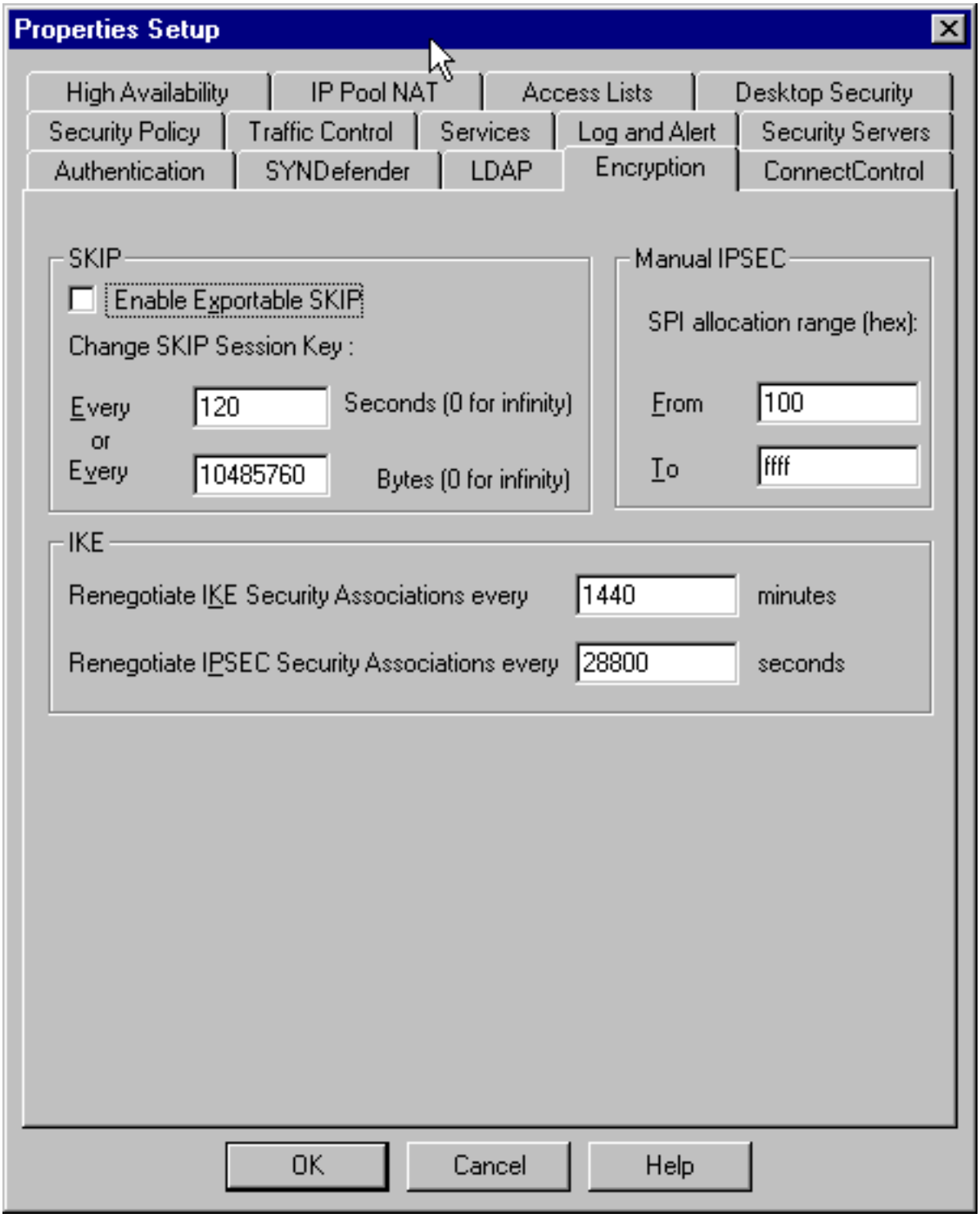


5. 保存配置。

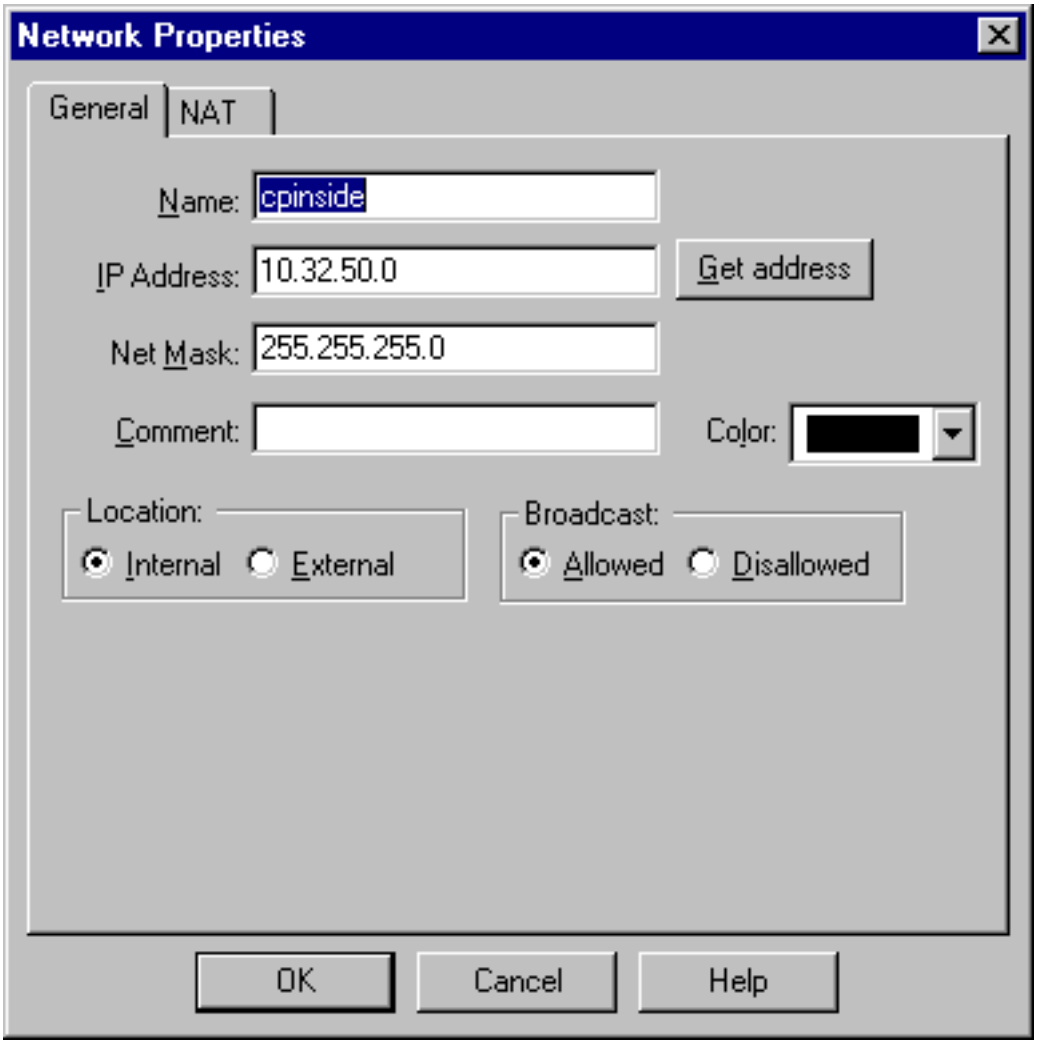
配置检查点 4.1 防火墙

完成以下步骤，以配置检查点 4.1 防火墙。

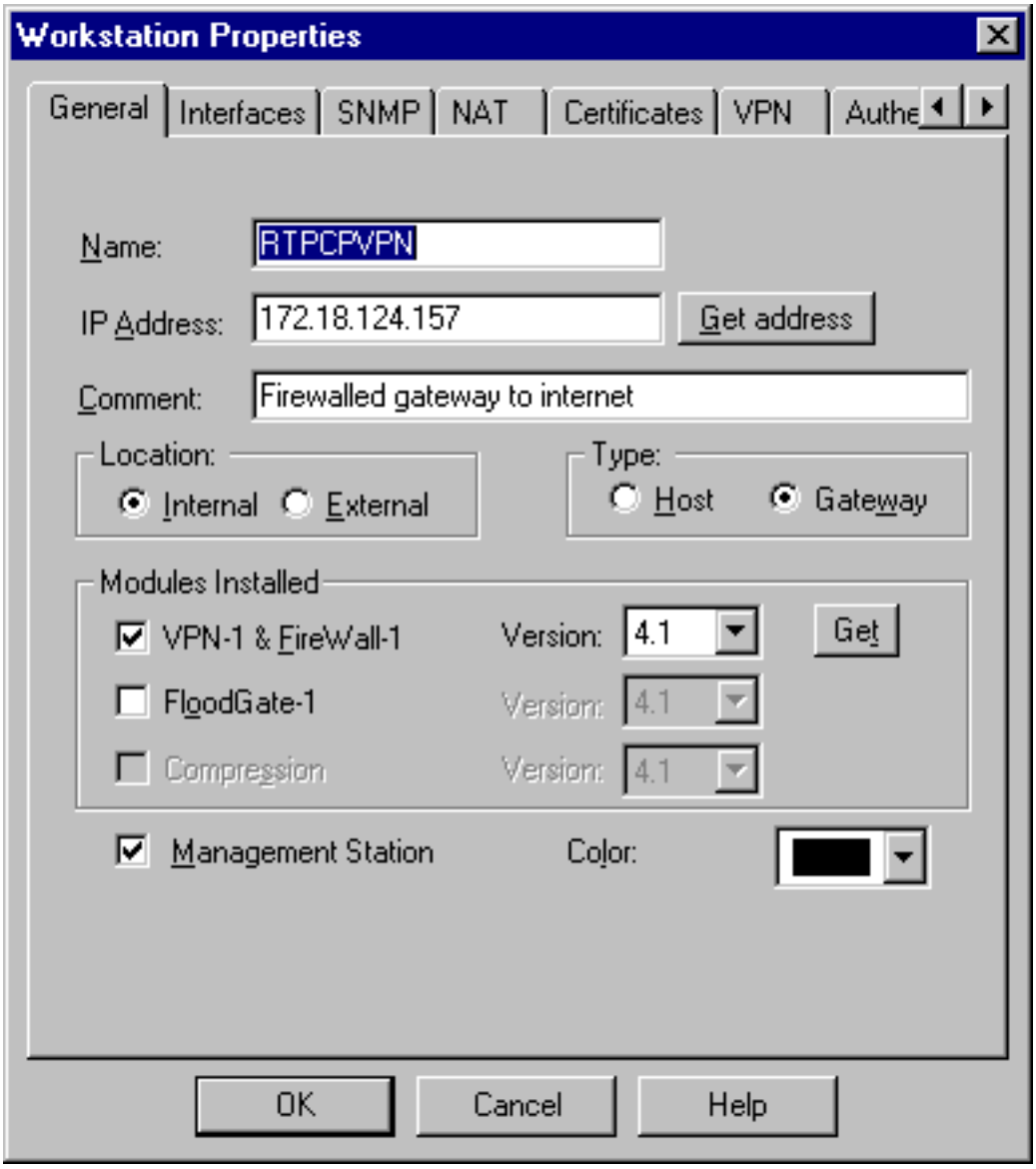
1. 由于不同的供应商设置的 IKE 和 IPSec 默认生命周期存在差异，因此请选择 **Properties > Encryption** 以将检查点生命周期设置为与 VPN 集中器默认值一致。VPN 集中器的默认 IKE 生命周期为 86400 秒（=1440 分钟）。VPN 集中器的默认 IPSec 生命周期为 28800 秒。



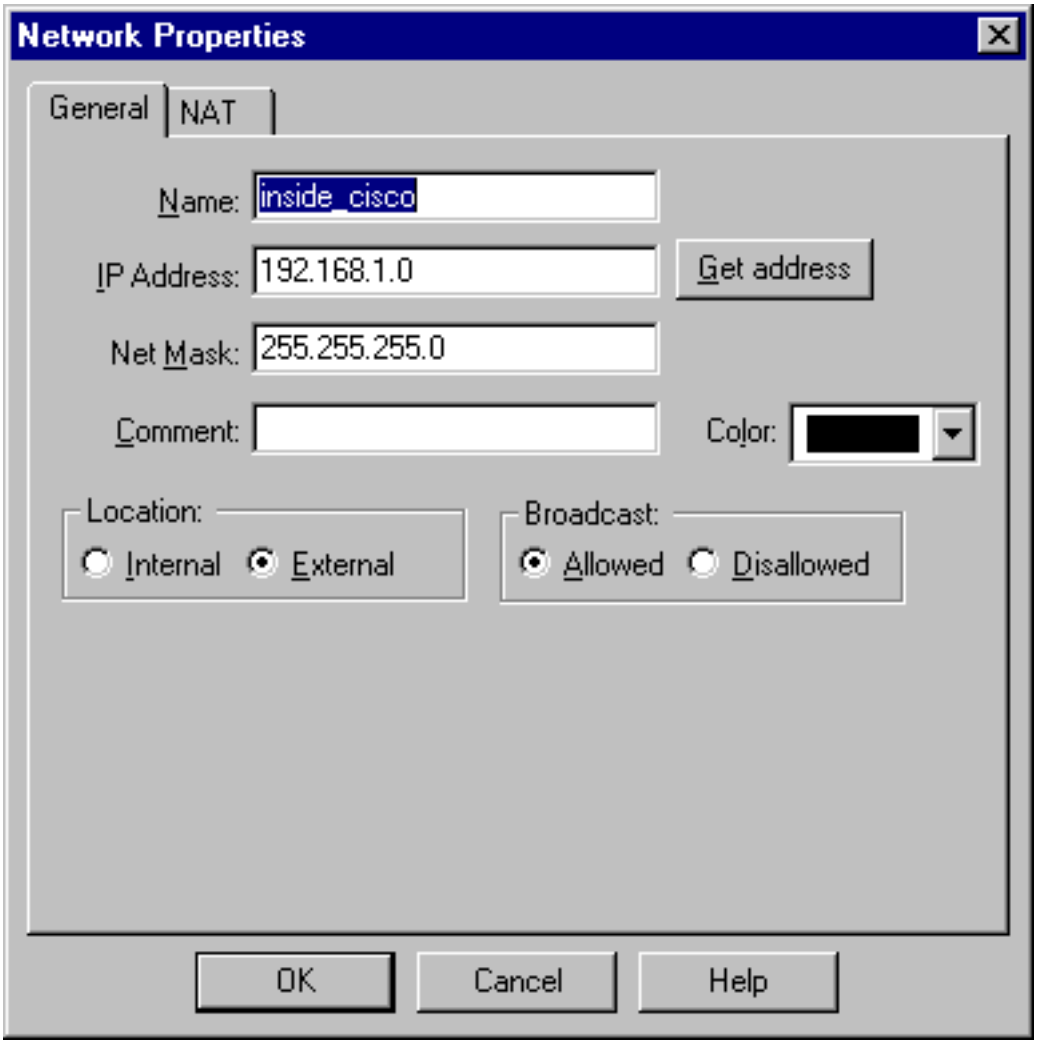
2. "选择Manage > Network objects > New (或 Edit) > Network，配置Checkpoint后的内部 (""cpinside"") 网络的对象。"这应与 VPN 集中器中的“远程网络”一致。



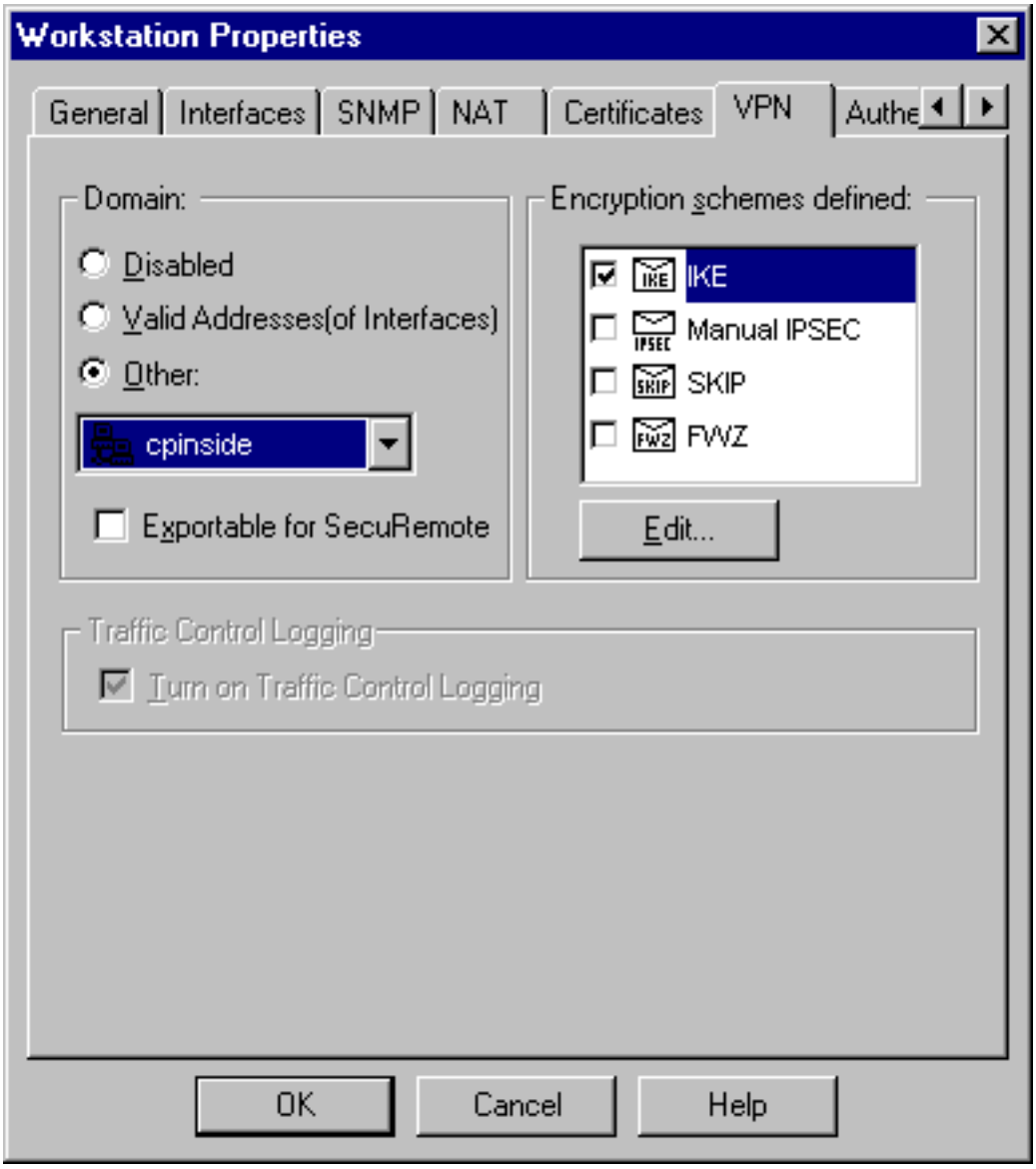
3. 选择 **Manage > Network objects > Edit** 以编辑 VPN 集中器在其对等体参数中设置的网关（"RTPCPVPN" 检查点）终端的对象。在 Location 下，请选择 **Internal**。对于“Type”，选择 **Gateway**。在 Modules Installed 下，选中 **VPN-1 & FireWall-1** 并选中**Management Station**。



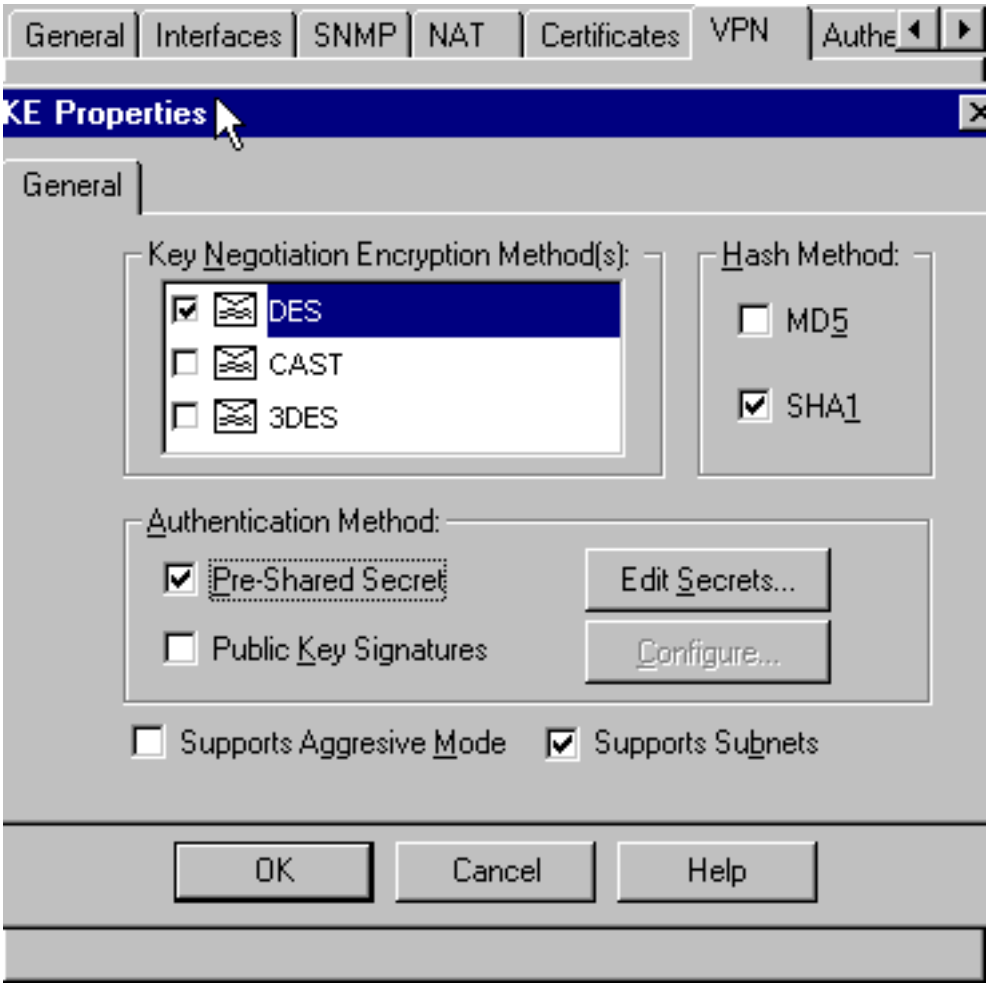
4. 选择 **Manage > Network objects > New (or Edit) > Network** 以配置 VPN 集中器后部的外部 ("inside_cisco") 网络的对象。这应与 VPN 集中器中的“本地”网络一致。



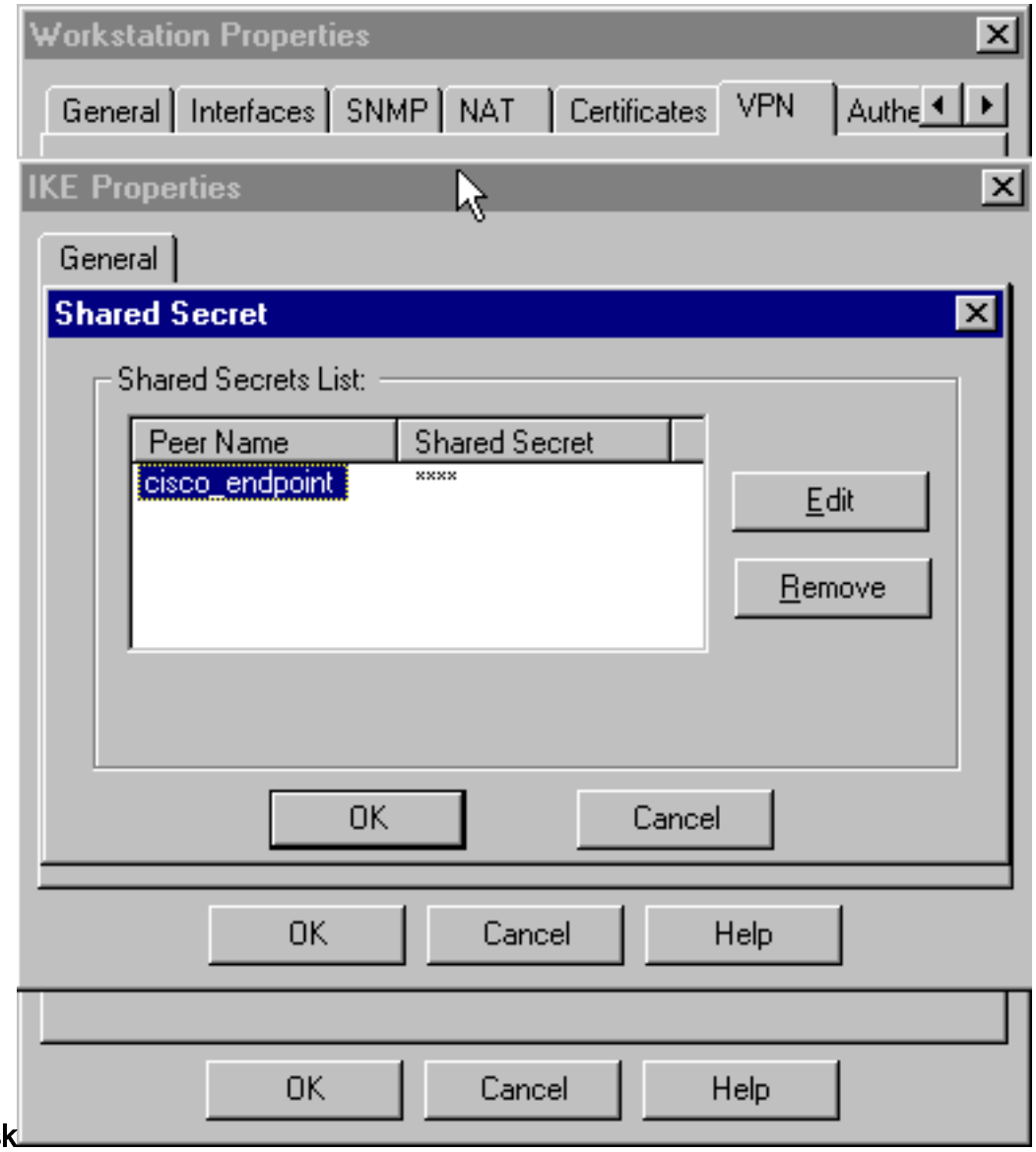
5. 选择 **Manage > Network objects > New > Workstation**，为外部 ("cisco_endpoint") VPN 集中器网关添加对象。这是 VPN 集中器的“公用”接口。在 Location 下，选择 **External**。对于“Type”，选择 **Gateway**。**注意：** 请勿选中“VPN-1/FireWall-1”复选框。
6. 选择 **Manage > Network objects > Edit** 以编辑 Checkpoint 网关端点（称为“RTPCPVPN”）VPN 选项卡。在域下，请选择**其他**然后从下拉列表中选择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 DES 加密的 IKE 属性，使其与 VPN 集中器中的 **DES-56** 和**加密算法**一致。
8. 将 IKE 属性更改为 SHA1 哈希，以便与 VPN 集中器中的 **SHA/HMAC-160** 算法一致。取消选定积极模式。选中 **Supports Subnets**。在“Authentication Method”下，选中 **Pre-Shared Secret**。这与 VPN 集中器身份验证模式（预共享密钥）一致。

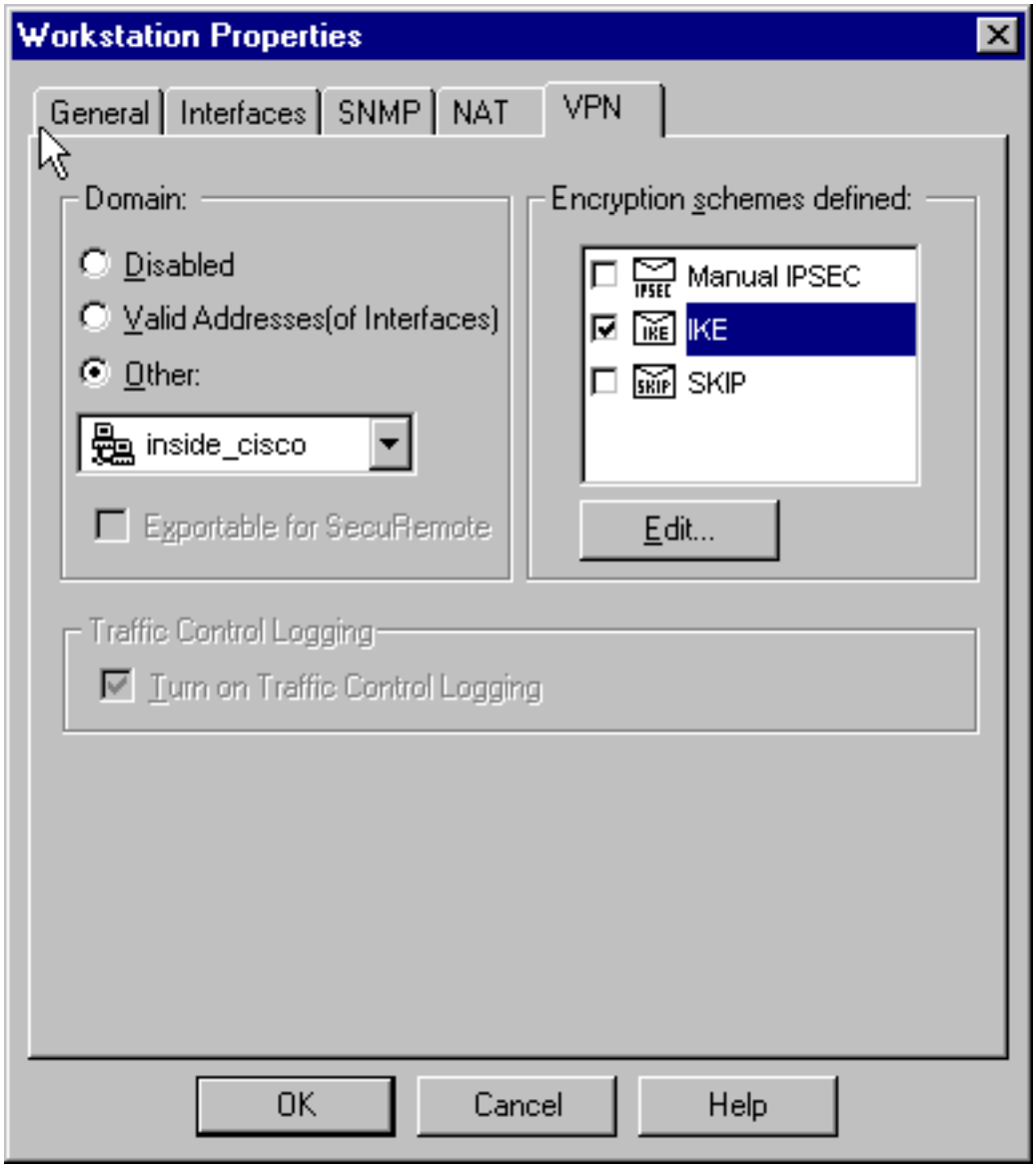


9. 点击 **Edit Secrets**，以将预共享密钥设置为与实际 VPN 集中器**预共享密钥**一致。**isakmp key key address address netmask**

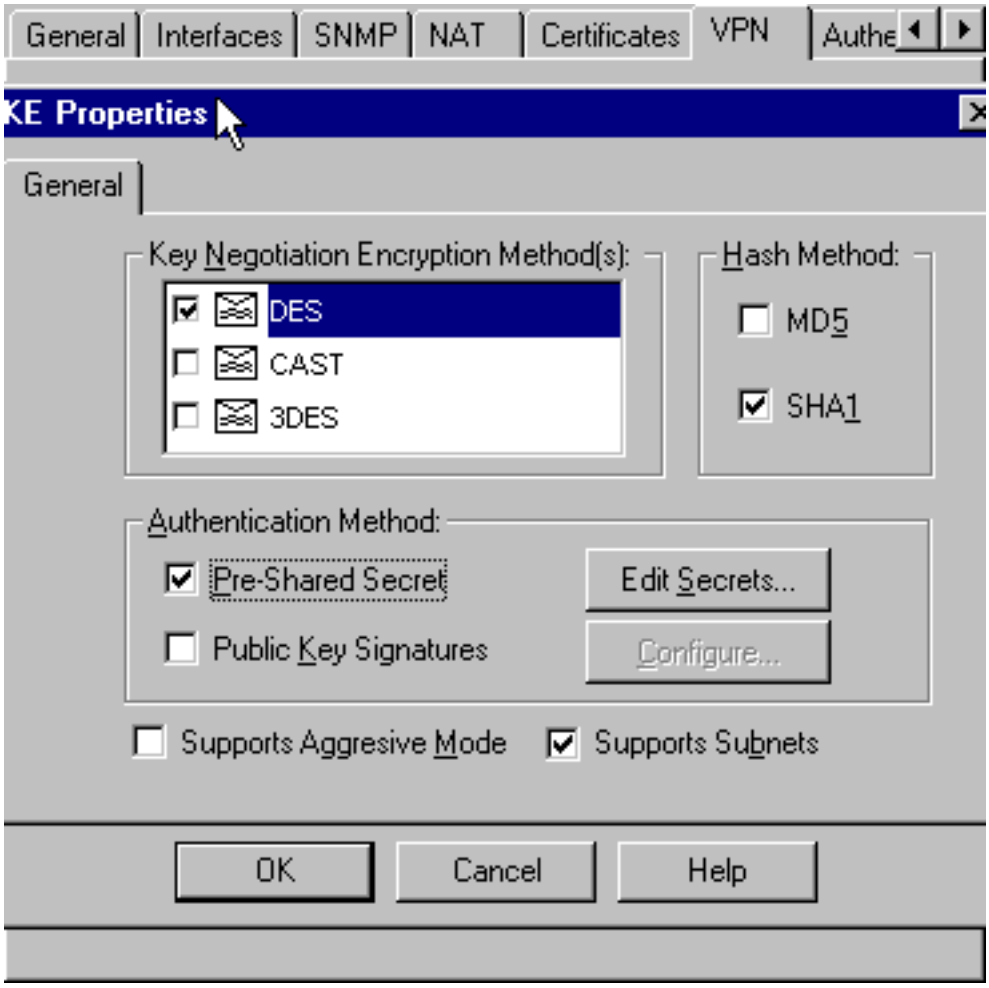


netmask

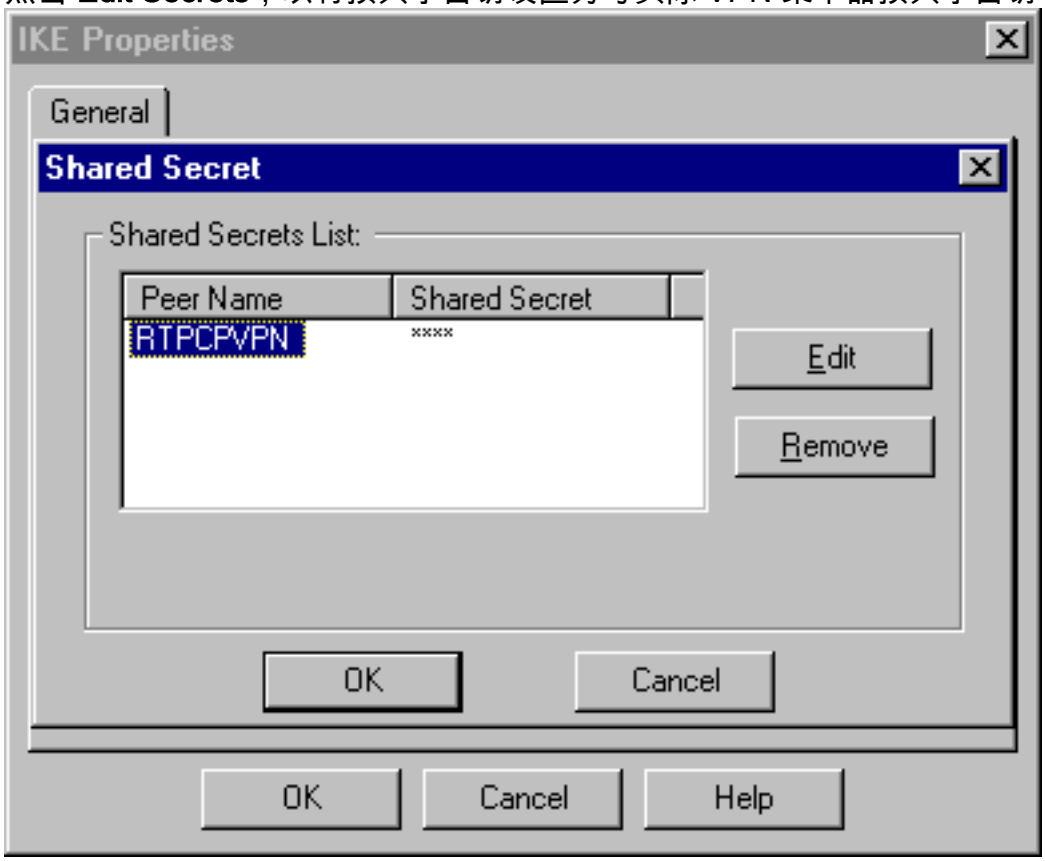
10. 选择 **Manage > Network objects > Edit** 以编辑“cisco_endpoint”VPN 选项卡。在“Domain”下，选择 **Other**，然后选择 Cisco 网络内部（称为“inside_cisco”）。在被定义的加密机制下，精选的**IKE**，然后点击**编辑**。



11. 更改 DES 加密的 IKE 属性，使其与 VPN 集中器中的 **DES-56、加密算法**一致。
12. 将 IKE 属性更改为 SHA1 哈希，以便与 VPN 集中器中的 **SHA/HMAC-160** 算法一致。更改这些设置：取消选择积极**模式**。选中 **Supports Subnets**。在“Authentication Method”下，选中 **Pre-Shared Secret**。这与 VPN 集中器身份验证模式（预共享密钥）一致。

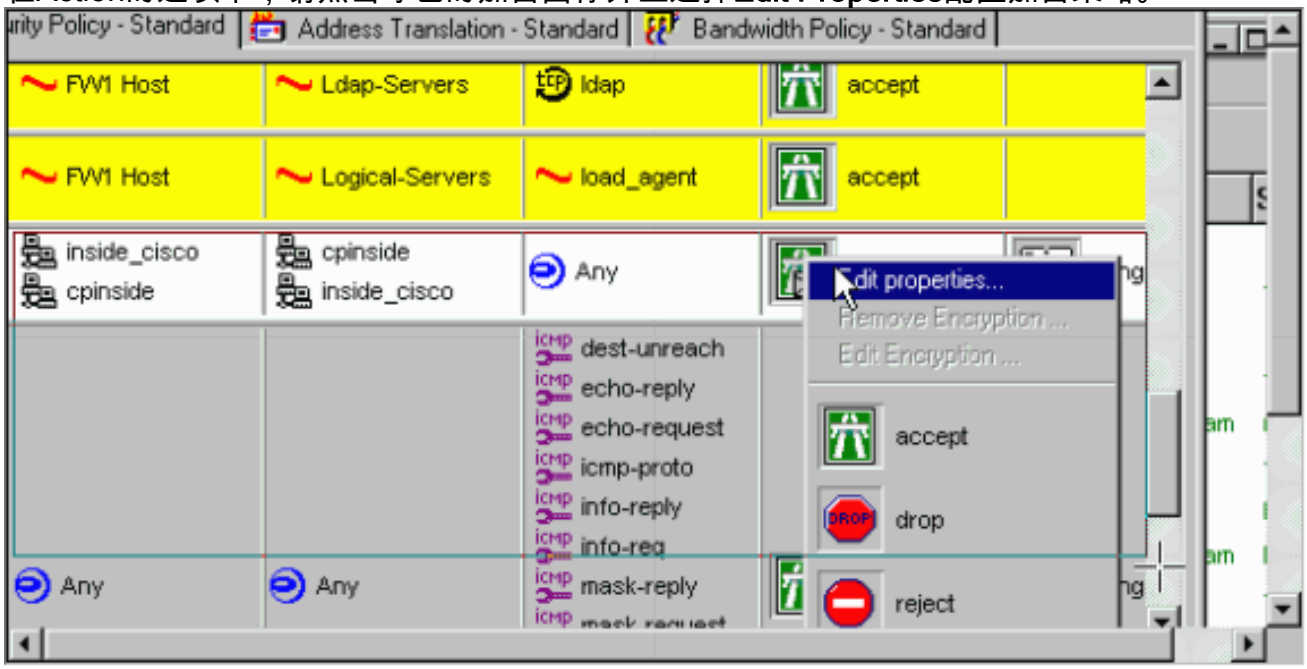


13. 点击 **Edit Secrets**，以将预共享密钥设置为与实际 VPN 集中器预共享密钥一致。

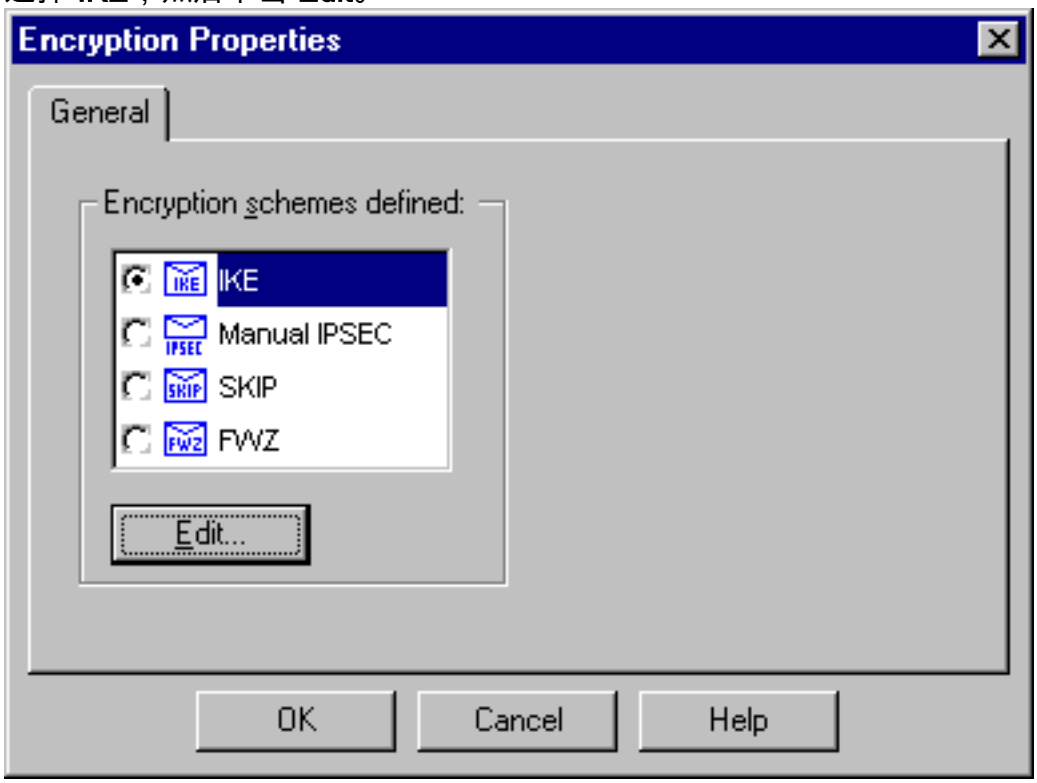


14. 在策略编辑器窗口，插入源和目的为“inside_cisco”和“cpinside”(双向)这一规则。设置 **Service=Any、Action=Encrypt** 和 **Track=Long**。

15. 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。

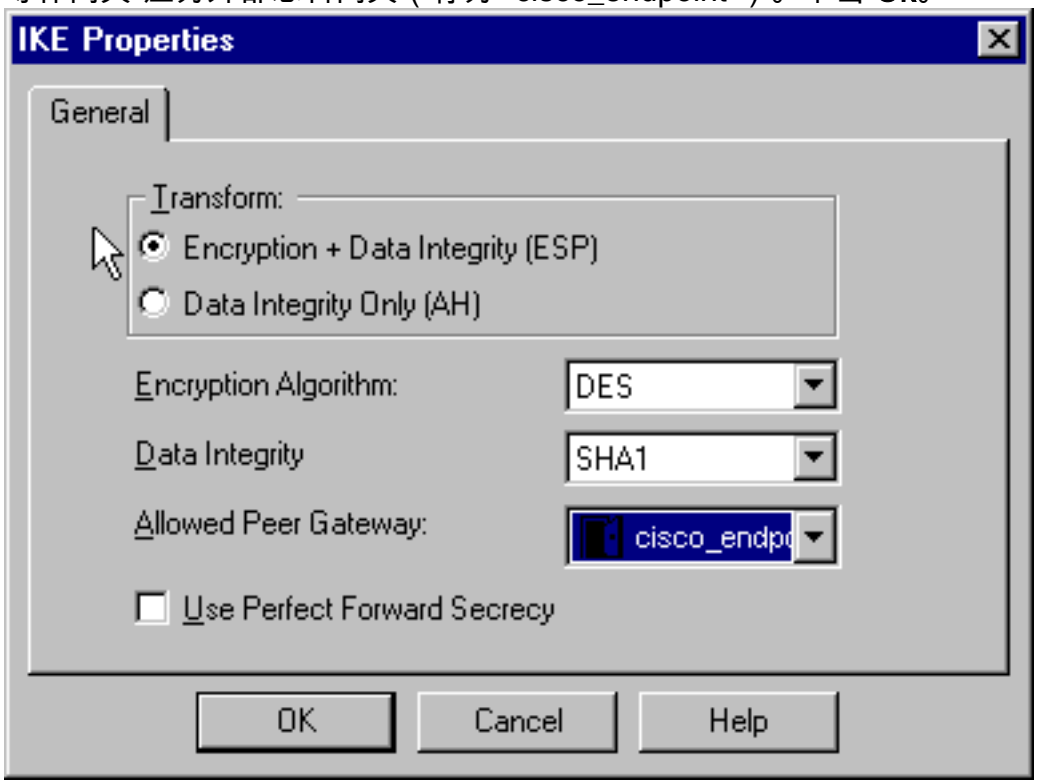


16. 选择 **IKE**，然后单击 **Edit**。



17. 在 IKE Properties 窗口中，将以下属性更改为与 VPN 集中器 IPsec 转换一致。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，“允许的对等体网关”应为外部思科网关（称为 "cisco_endpoint"）。单击 **Ok**。



18. 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

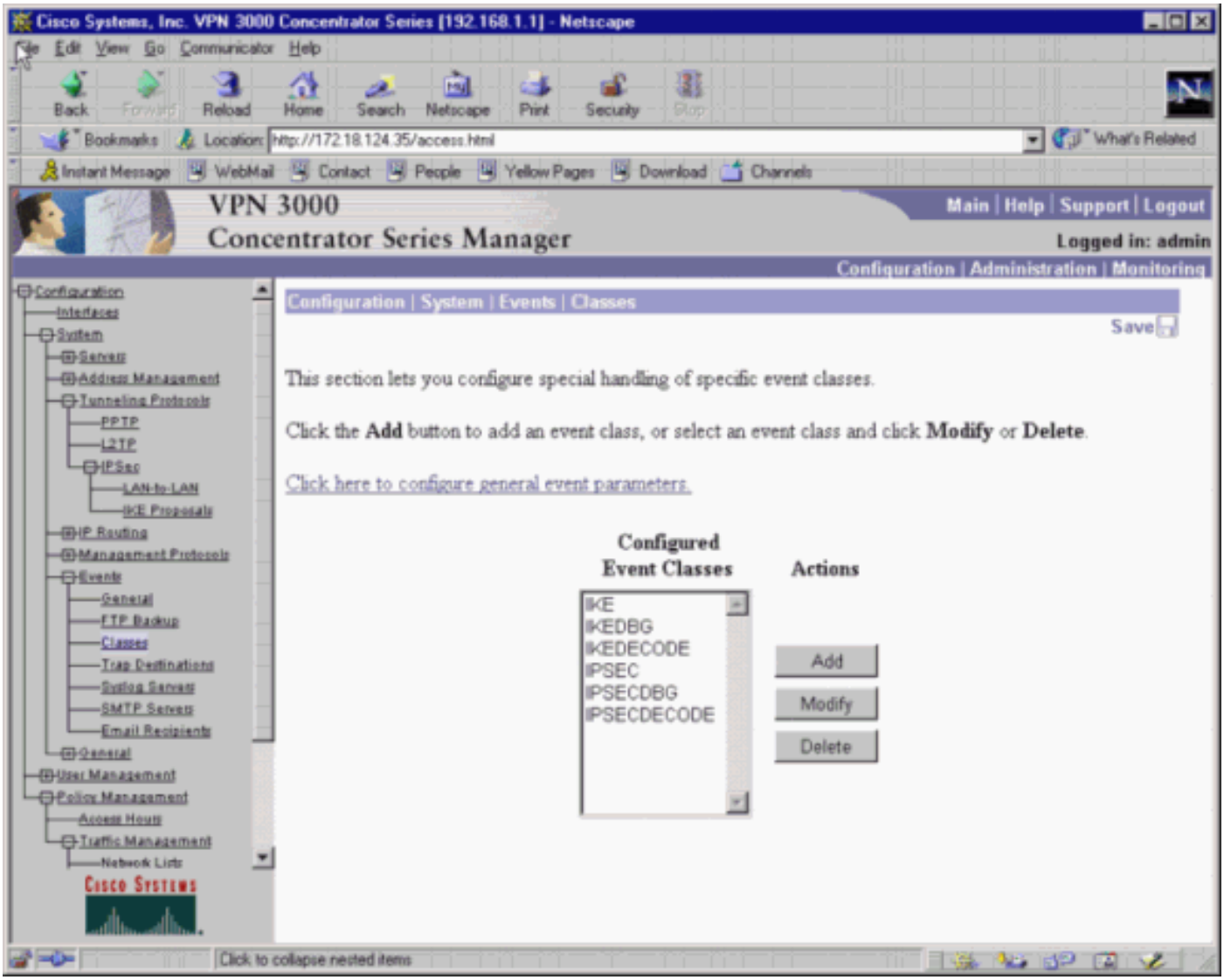
本部分提供的信息可用于对配置进行故障排除。

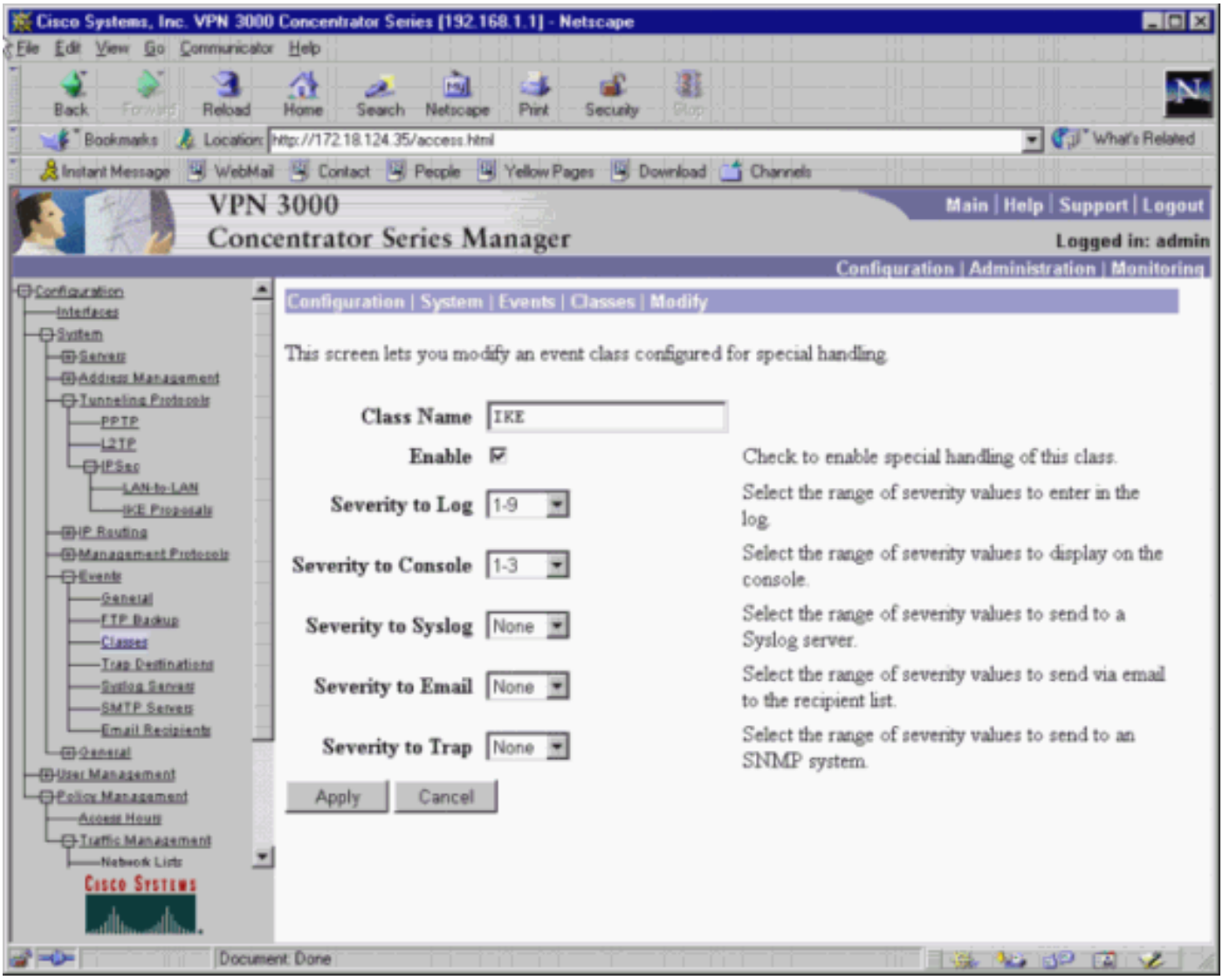
网络汇总

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。

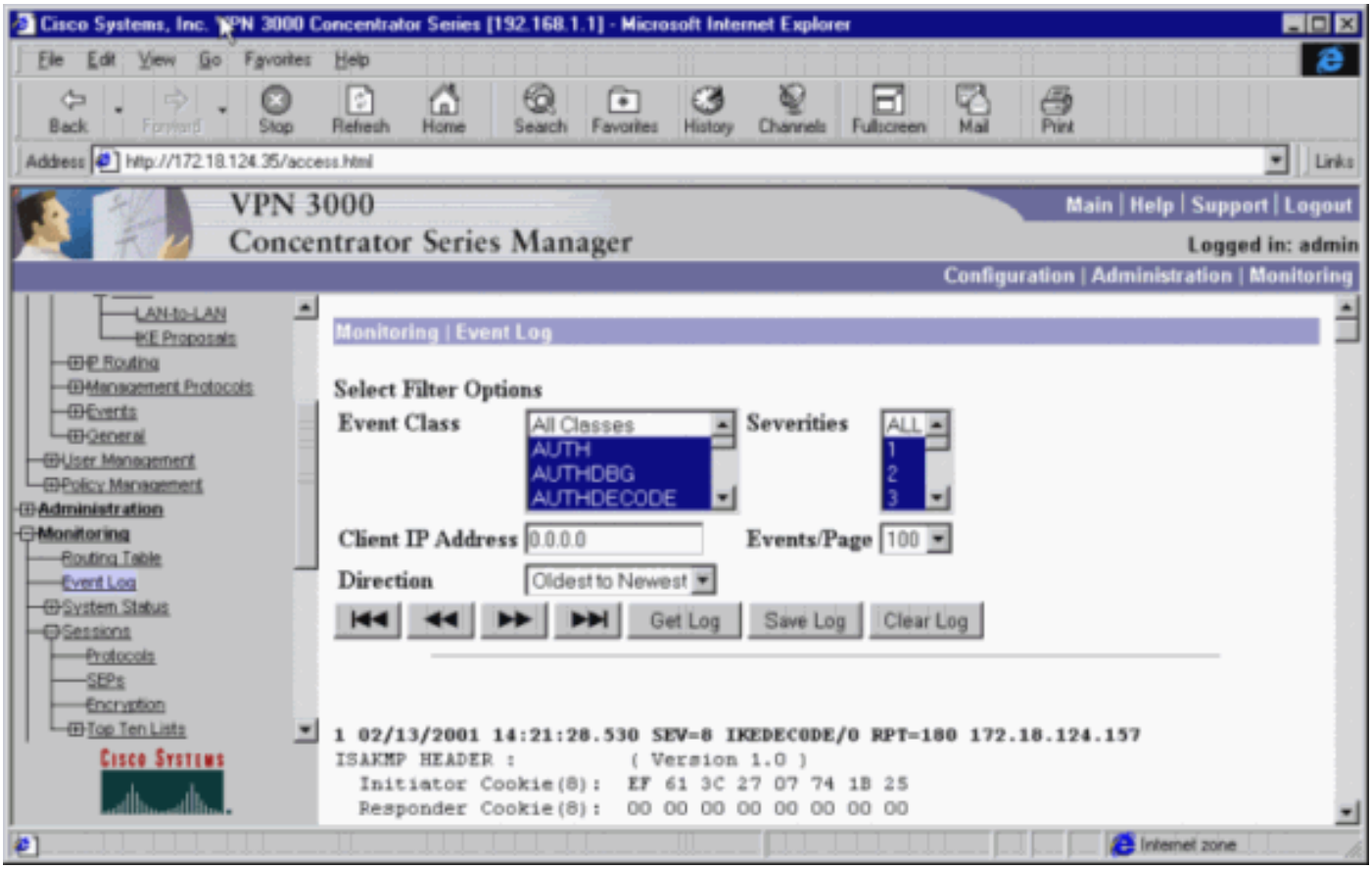
VPN 3000 集中器调试

可能的 VPN 集中器调试包括 IKE、IKEDBG、IKEDECODE、IPSEC、IPSECDBG、IPSECDECODE。此调试是通过 **Configuration > System > Events > Classes** 中进行设置。

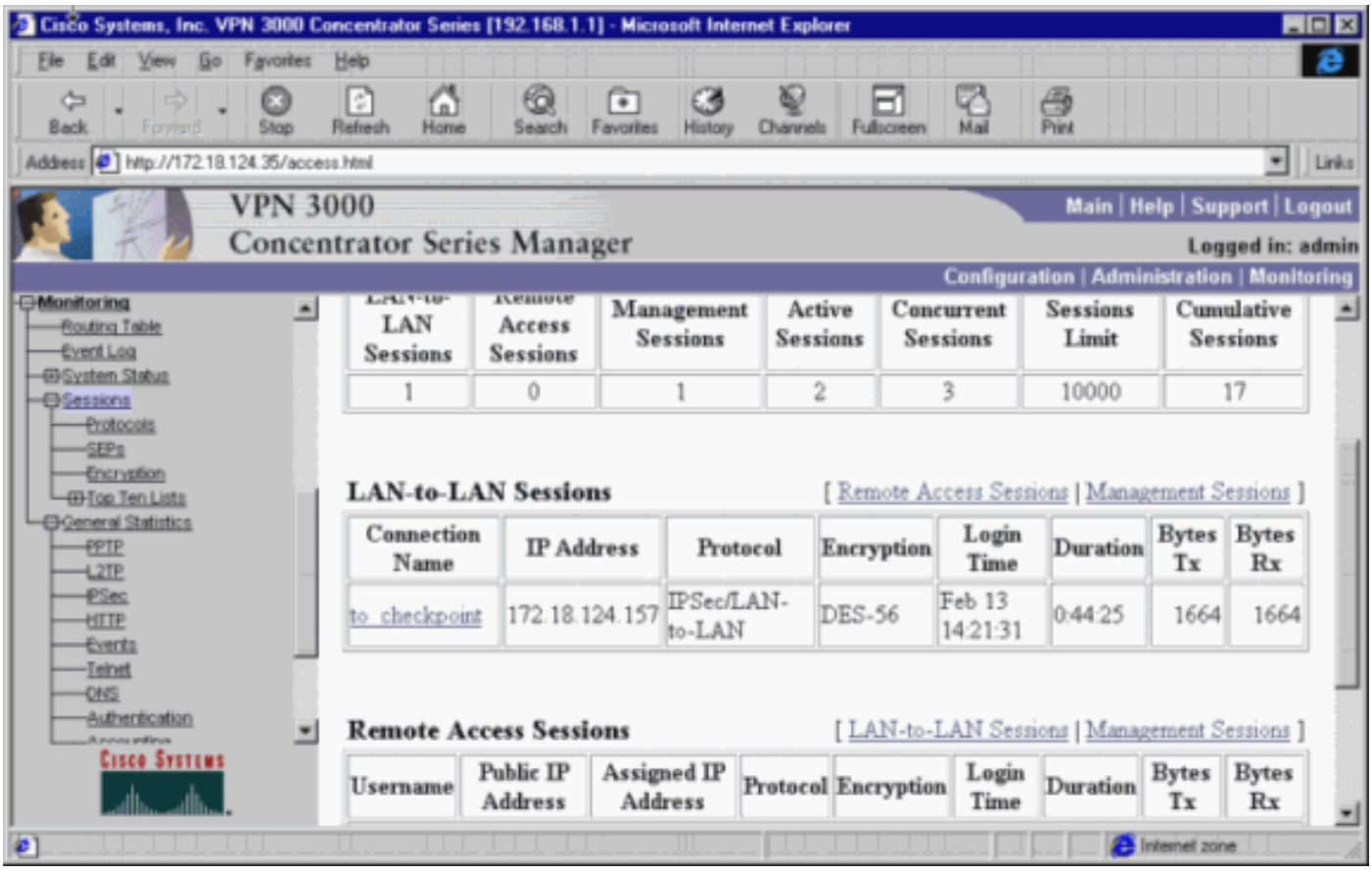

Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
IP Routing
Management Protocols
Events
General
FTP Backup
Classes
Trap Destinations
Syslog Servers
SMTP Servers
Email Recipients
General
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Cisco Systems
Configuration | System | Events | Classes
Save
This section lets you configure special handling of specific event classes.
Click the Add button to add an event class, or select an event class and click Modify or Delete.
Click here to configure general event parameters.
Configured Event Classes
Actions
IKE
IKEDBG
IKEDECODE
IPSEC
IPSECDBG
IPSECDECODE
Add
Modify
Delete
Click to collapse nested items



您可以通过 Monitoring > Event log > Get Log 查看调试。



选择 Monitoring > Sessions 以监视 LAN 到 LAN 的隧道流量。



选择 Administration > Administer Sessions > LAN-to-LAN sessions > Actions - Logout 以清除隧道。

Checkpoint 4.1 防火墙Debug

注意： 这是Microsoft Windows NT安装。由于已在“Policy Editor”窗口中将“Tracking”设置为“Long”，因此拒绝的流量应 Log Viewer 中显示为红色。可通过以下命令获取更详细的调试：

```
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 Checkpoint 上的 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 VPN 3000 集中器

```
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
```

相关信息

- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems