

# 配置IPSec隧道- Cisco路由器到Checkpoint防火墙

## 4.1

### 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[网络汇总](#)

[Checkpoint](#)

[调试输出示例](#)

[相关信息](#)

### 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：Cisco 路由器内的 192.168.1.x 专用网络和 Checkpoint 防火墙内的 10.32.50.x 专用网络。

### 先决条件

#### 要求

此配置示例假设，在开始配置之前，流量从路由器和 Checkpoint 流到 Internet（此处由 172.18.124.x 网络来表示）。

#### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 3600 路由器
- Cisco IOS® 软件 (C3640-JO3S56I-M)，版本 12.1(5)T，发布软件 (fc1)
- Checkpoint Firewall 4.1

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](#)。

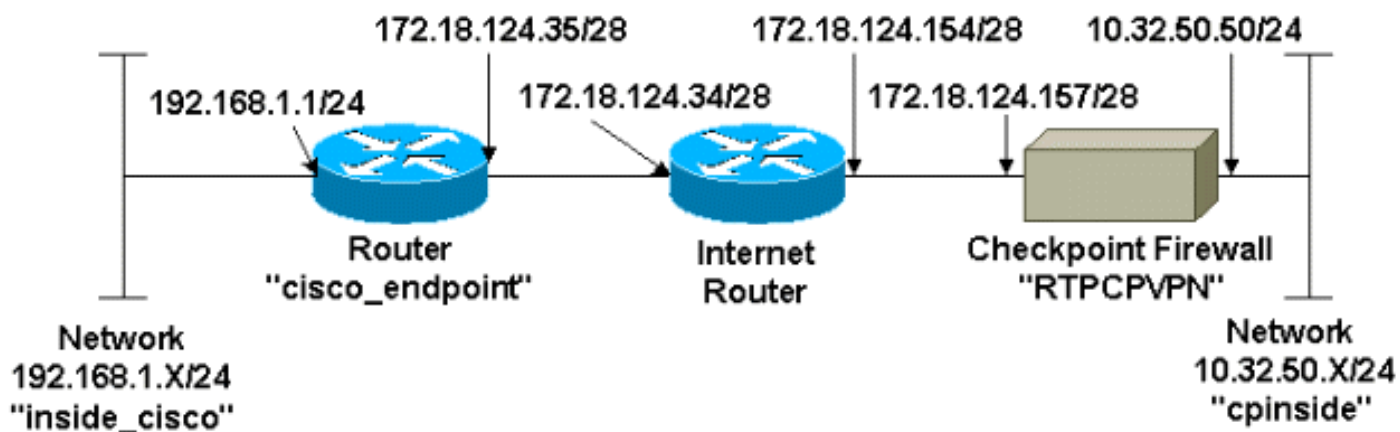
## 配置

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。

- [路由器配置](#)
- [Checkpoint 防火墙配置](#)

## 路由器配置

### Cisco 3600 路由器配置

```
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
!
```

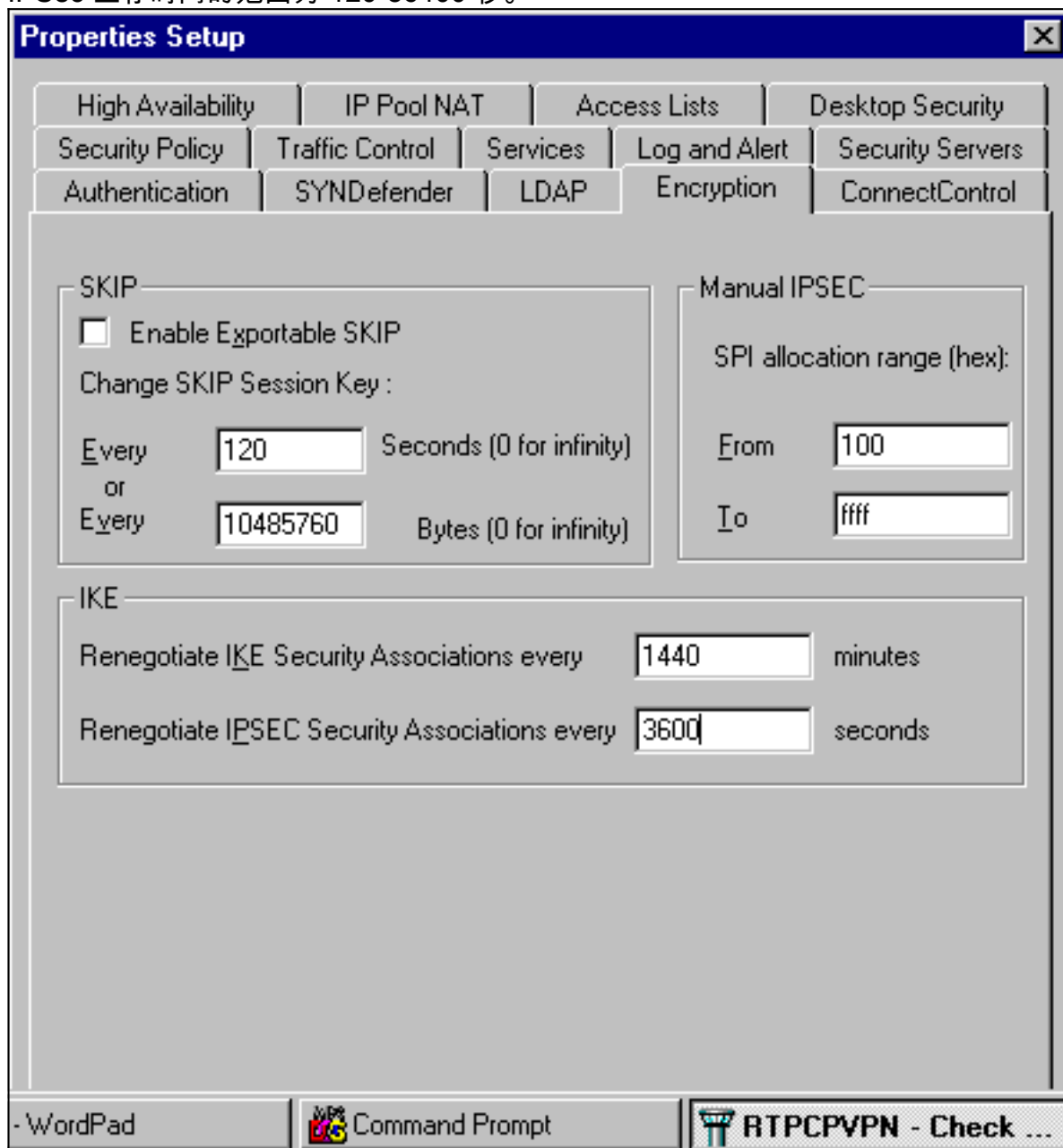
```
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des 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 防火墙配置

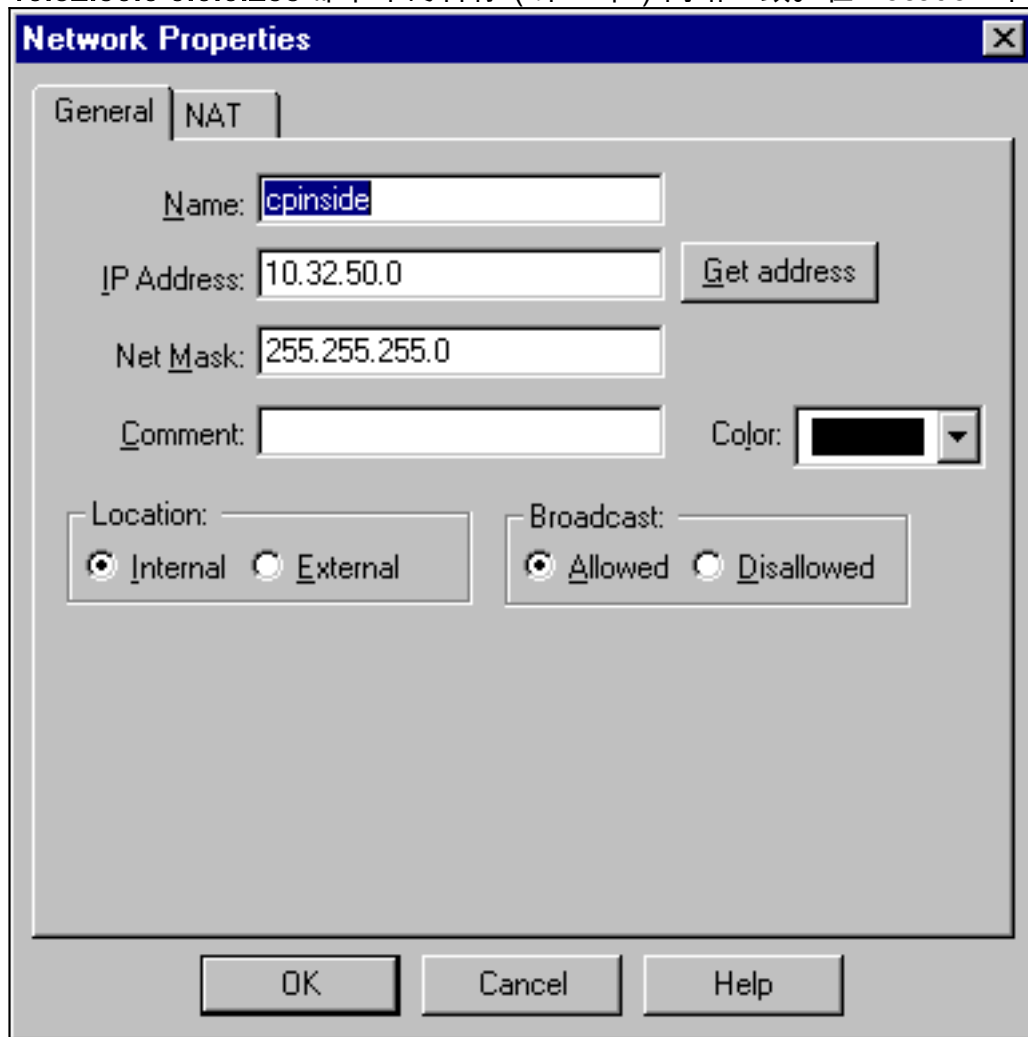
完成以下步骤以配置 Checkpoint 防火墙。

1. 由于各供应商之间的 IKE 和 IPsec 默认生存时间各不相同，因此请选择 **Properties > Encryption** 以将 Checkpoint 生存时间设置为与 Cisco 默认设置一致。Cisco 默认 IKE 生存时间为 86400 秒（即 1440 分钟），可通过以下命令进行修改：**crypto isakmp policy #寿命#**可配置的 Cisco IKE 生存时间的范围为 60-86400 秒。Cisco 默认 IPsec 生存时间为 3600 秒，可通过 **crypto ipsec security-association lifetime seconds #** 命令进行修改。可配置的 Cisco IPsec 生存时间的范围为 120-86400 秒。

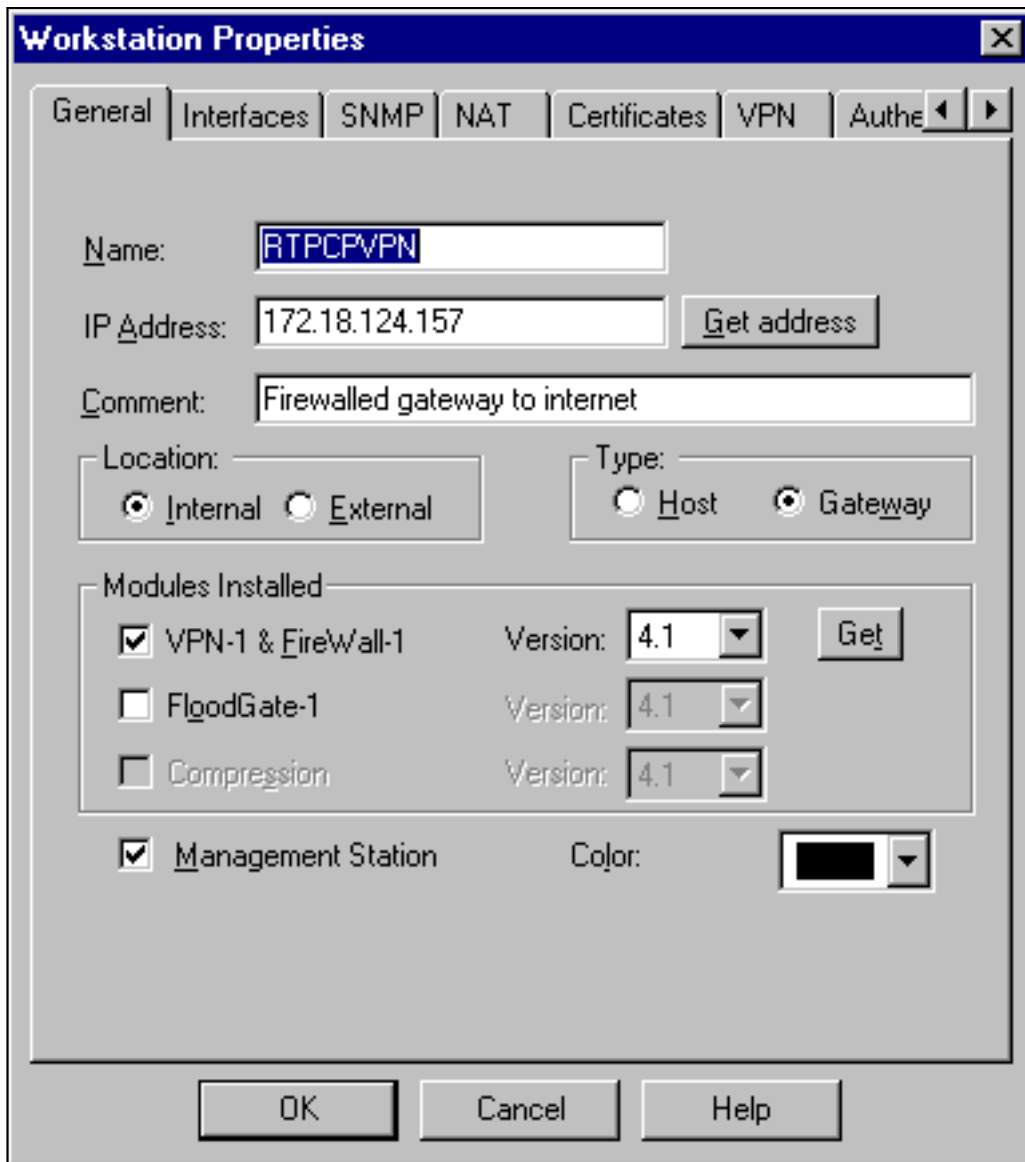


2. 选择 **Manage > Network objects > New ( 或 Edit ) > Network**，为 Checkpoint 后面的内部网

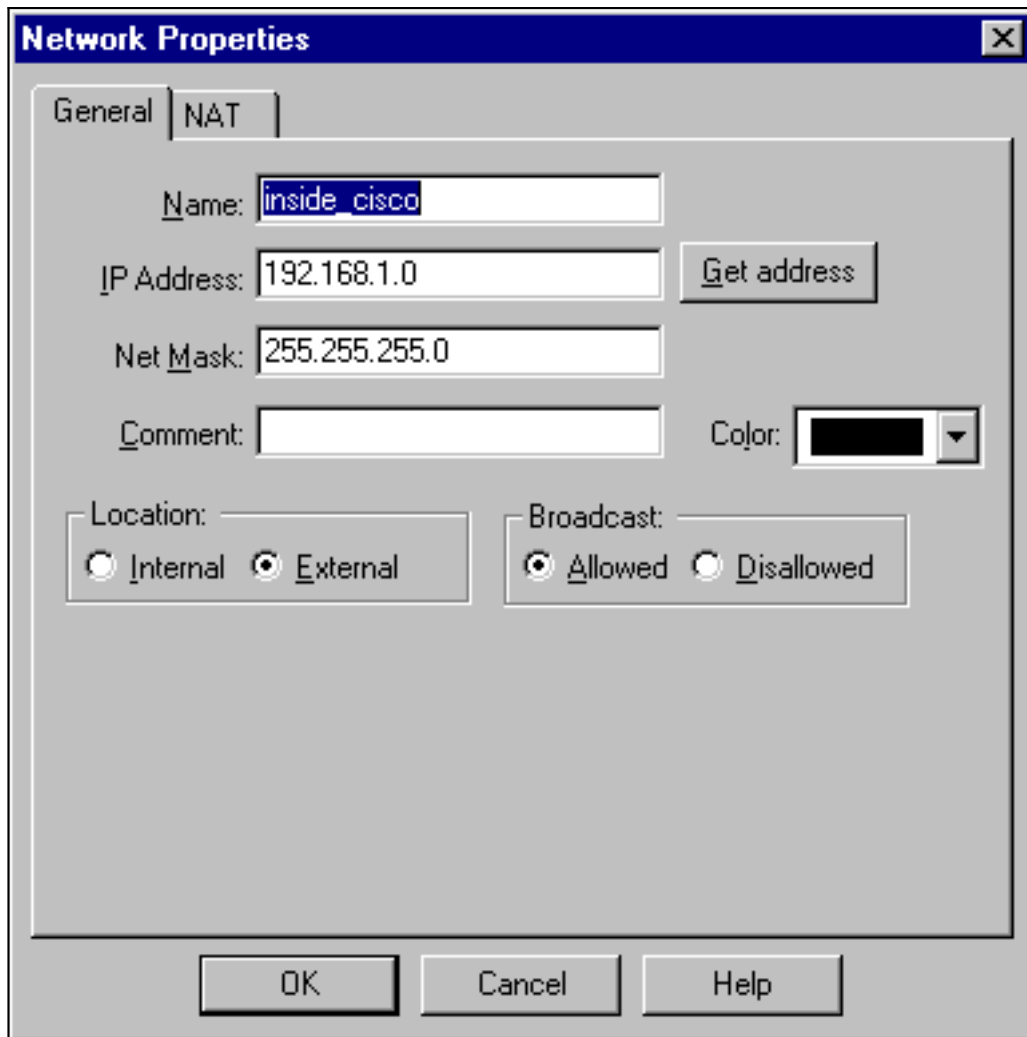
络 (称为“cpinside”) 配置对象。这应与 Cisco `access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255` 命令中的目标 (第二个) 网络一致。在“Location”下选择 **Internal**。



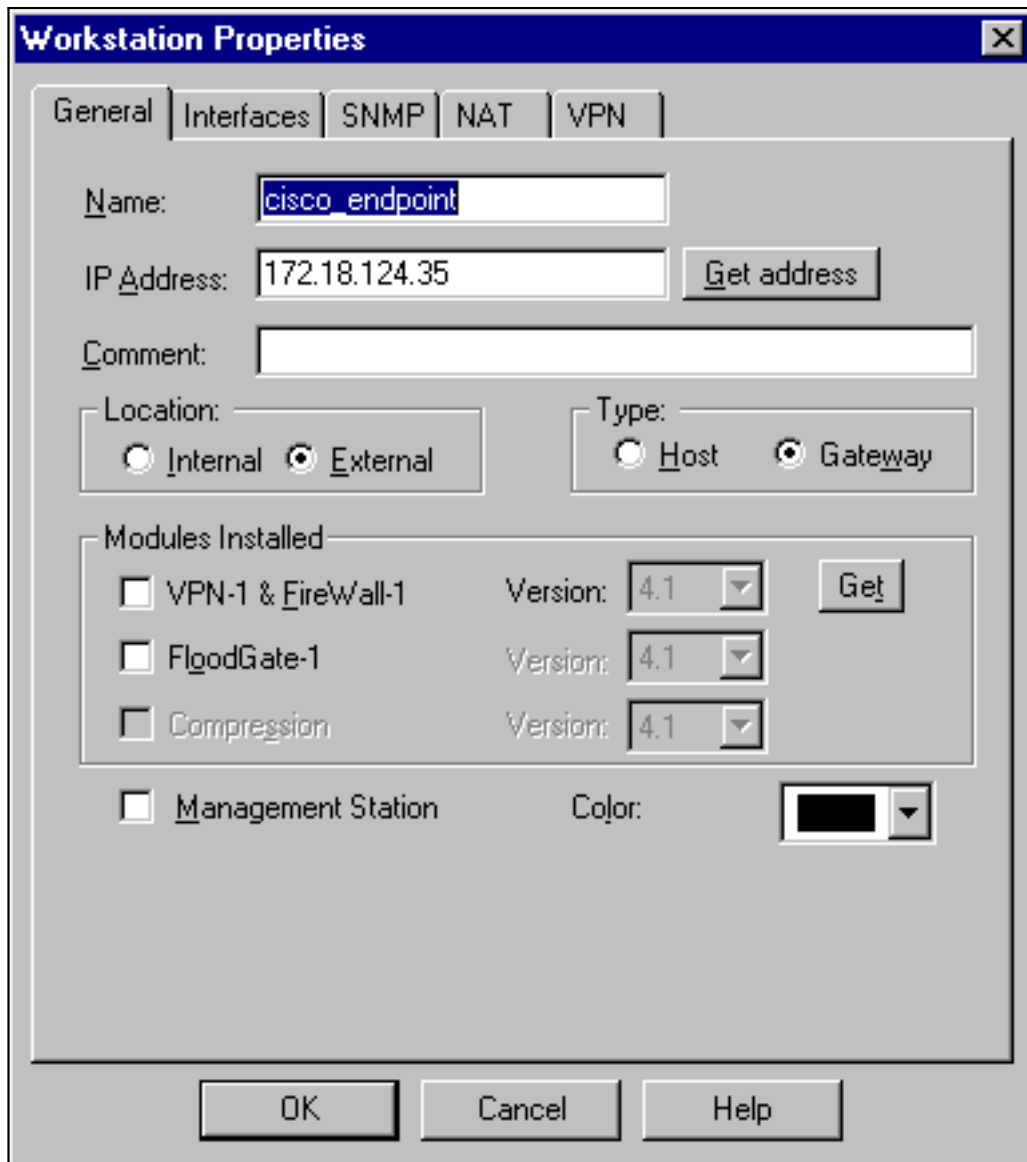
3. 选择 **Manage > Network objects > Edit** 以编辑 `set peer 172.18.124.157` 命令中 Cisco 路由器所指向的 RTPCPVPN Checkpoint (网关) 端点的对象。在“Location”下选择 **Internal**。对于“Type”，选择 **Gateway**。在安装的模块下，选择 **VPN-1 & FireWall-1** 复选框，并选择 **Management Station** 复选框



4. 选择 **Manage > Network objects > New > Network**，为 Cisco 路由器后面的外部网络（称为“inside\_cisco”）配置对象。这应与 Cisco `access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255` 命令中的源（第一个）网络一致。在“Location”下选择 **External**。

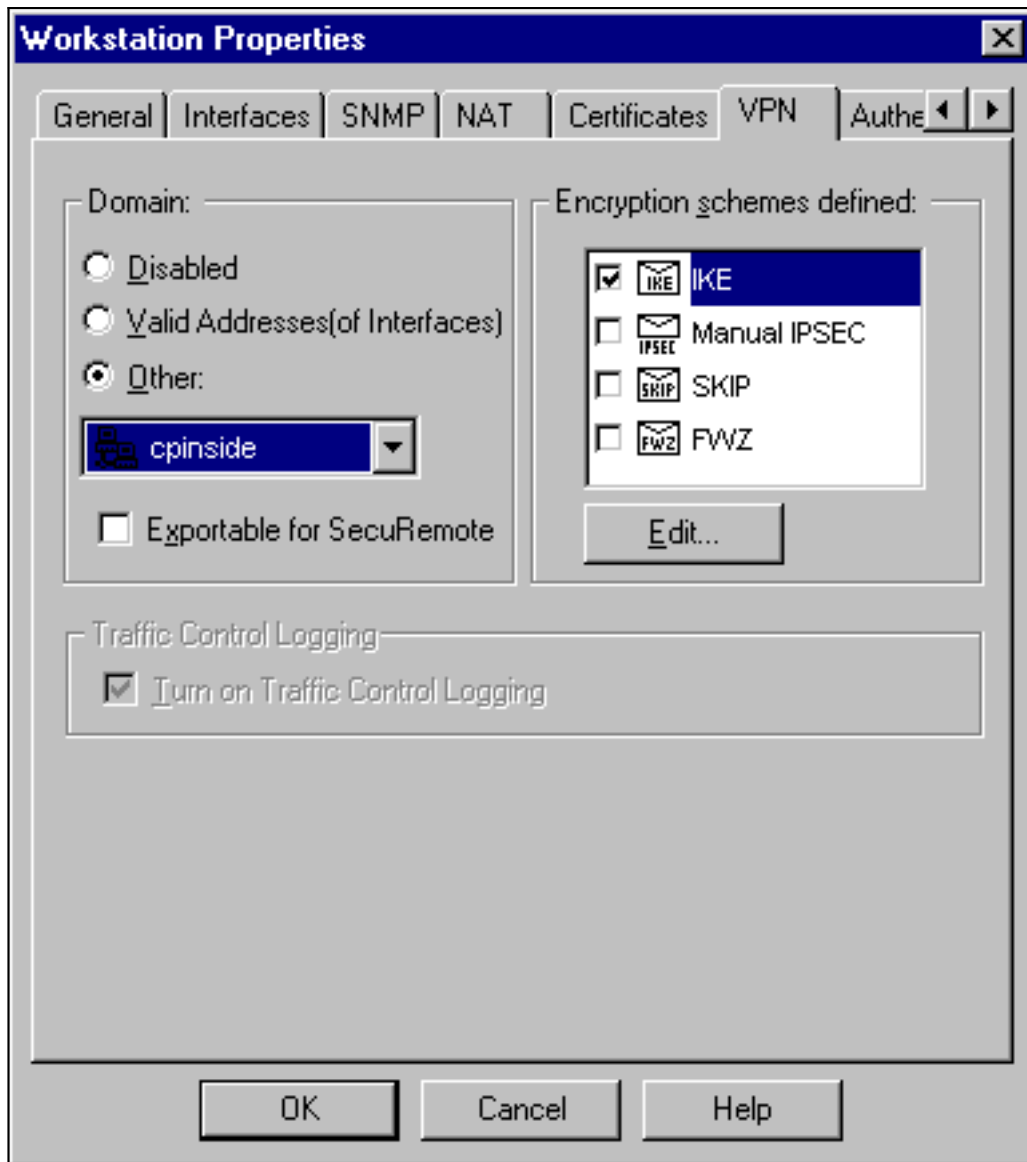


5. 选择 **Manage > Network objects > New > Workstation** 以添加外部 Cisco 路由器网关（称为“cisco\_endpoint”）的对象。这是应用 **crypto map name** 命令的 Cisco 接口。在“Location”下选择 **External**。对于“Type”，选择 **Gateway**。注意：请勿选中“VPN-1/FireWall-1”复选框。

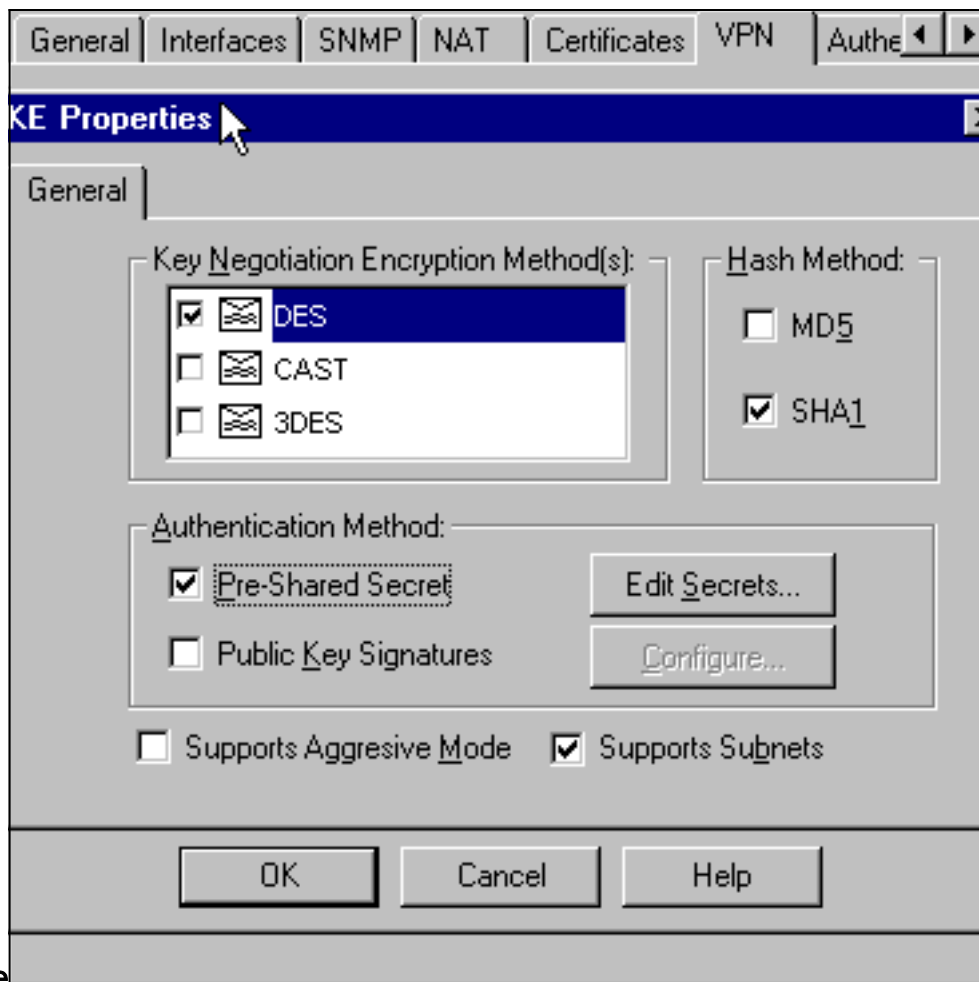


6. 选择 **Manage > Network objects > Edit** 以编辑 Checkpoint 网关端点 (称为“RTPCVPN”) VPN 选项卡。在域下, 请选择**其他**然后从下拉列表中选择Checkpoint网络(称“cpinside”)。在被定义的加密机制下, 精选的**IKE**, 然后点击**编辑**。



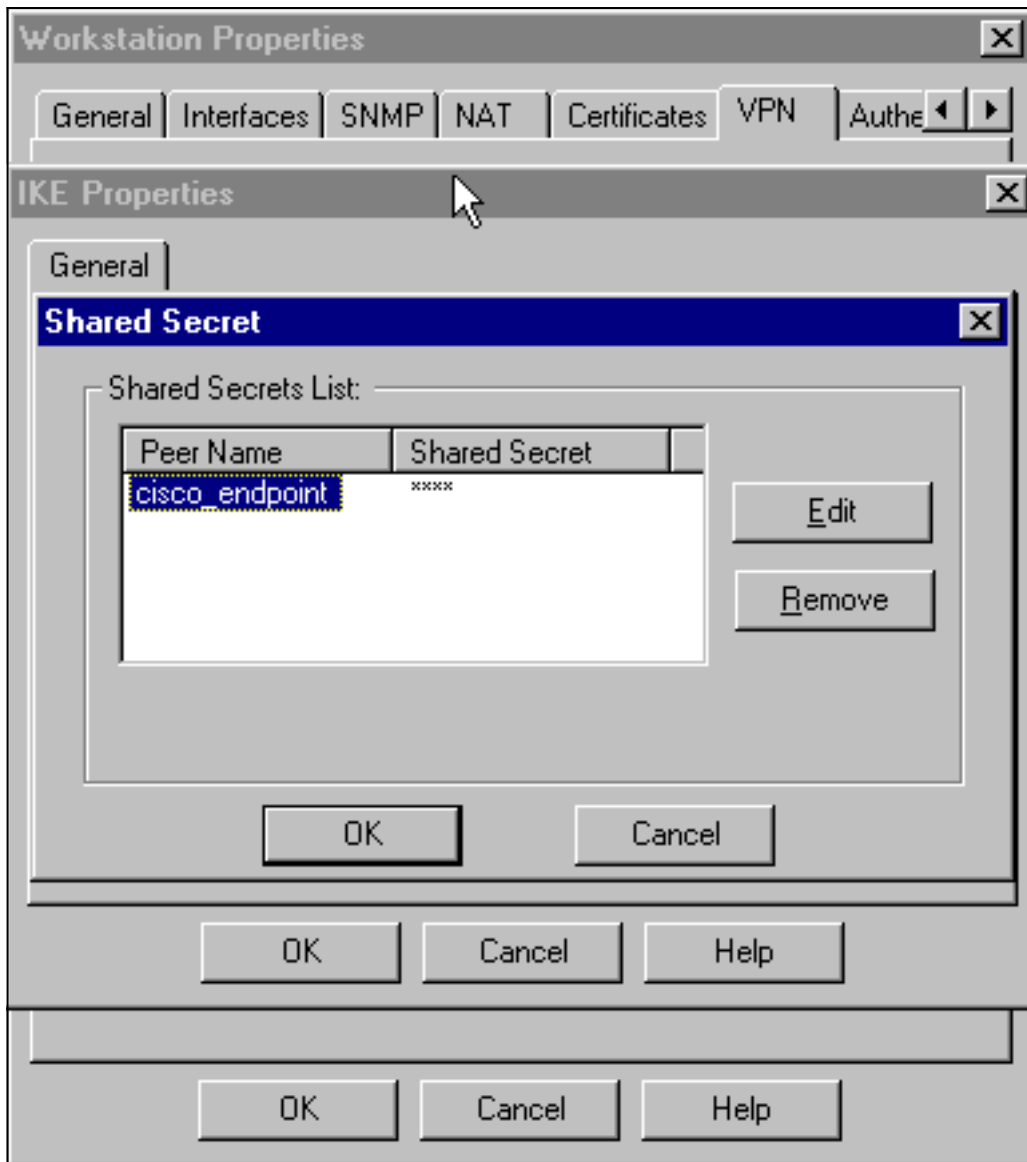


7. 更改 DES 加密的 IKE 属性，以便与以下命令一致：`crypto isakmp policy #encryption des`注意：DES 加密是默认设置，因此在 Cisco 配置中看不见。
8. 更改 SHA1 散列的 IKE 属性，以便与以下命令一致：`crypto isakmp policy #hash sha`注意：SHA 散列算法是默认算法，因此在 Cisco 配置中看不见。更改这些设置：取消选定积极模式。选中 **Supports Subnets**。在“Authentication Method”下，选中 **Pre-Shared Secret**。这与以下命令一致：`crypto isakmp policy #authentication pre-`



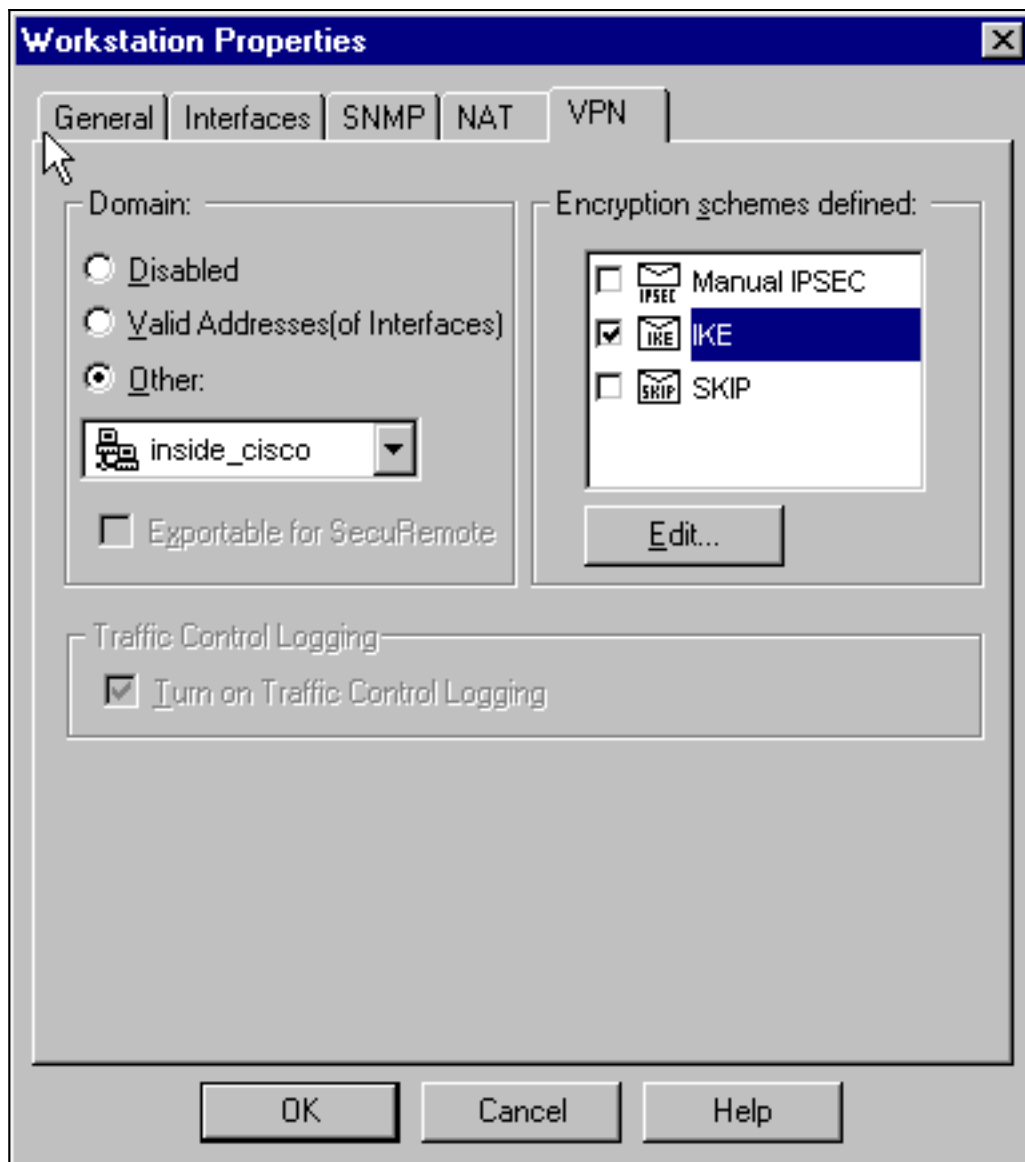
share

9. 单击 **Edit Secrets** 设置预共享密钥，以便与 Cisco `crypto isakmp key key address address` 命

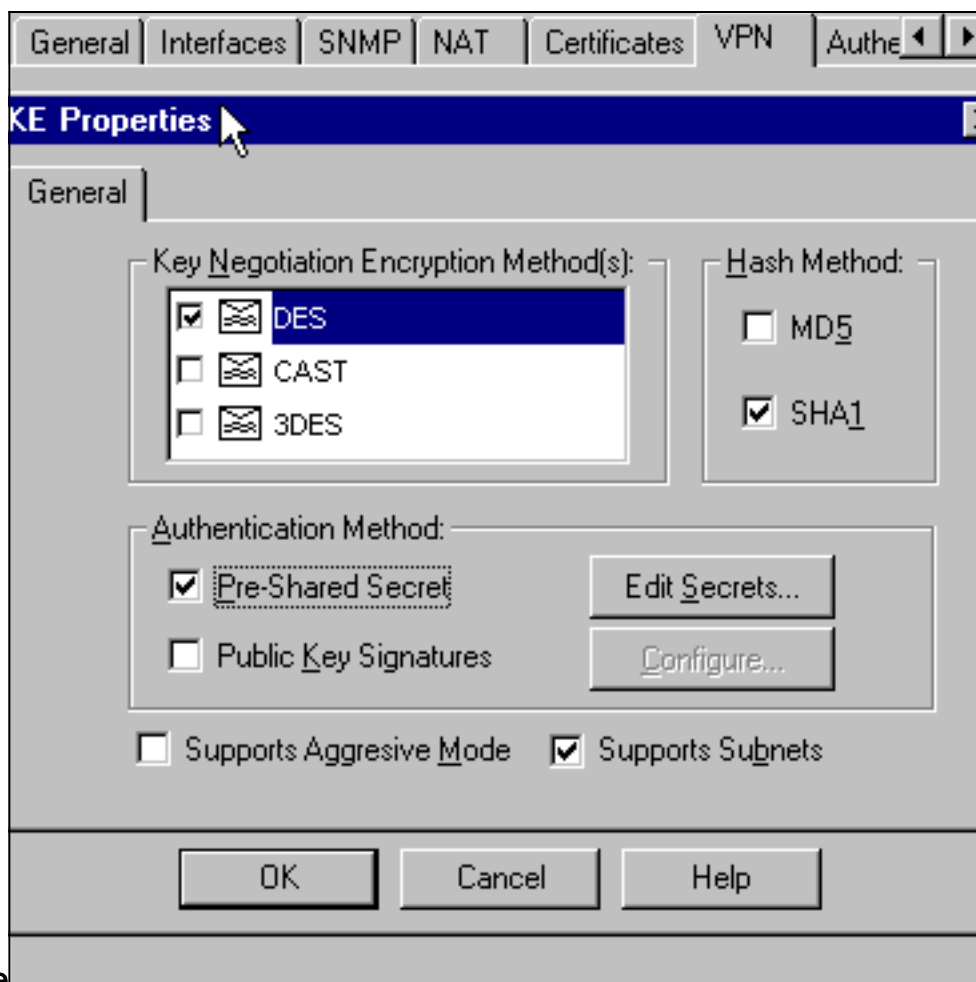


令一致：

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**。

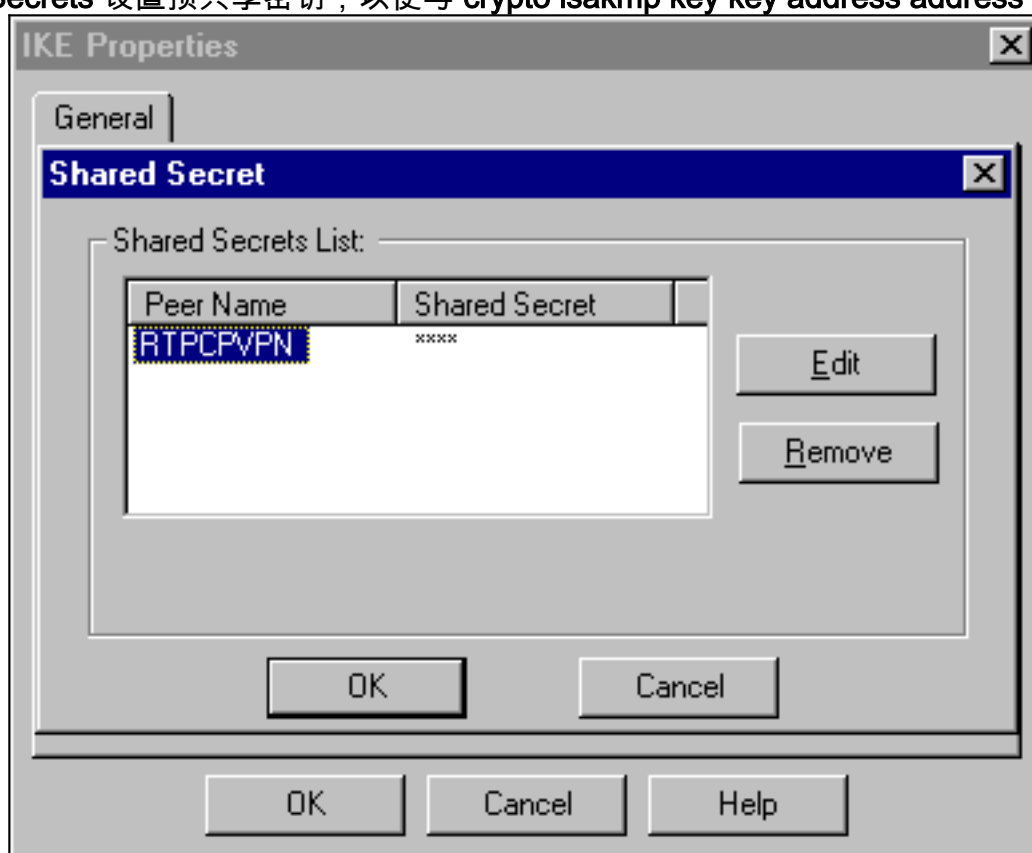


11. 更改 DES 加密的 IKE 属性，以便与以下命令一致：`crypto isakmp policy #encryption des`注意：DES 加密是默认设置，因此在 Cisco 配置中看不见。
12. 更改 SHA1 散列的 IKE 属性，以便与以下命令一致：`crypto isakmp policy #hash sha`注意：SHA 散列算法是默认算法，因此在 Cisco 配置中看不见。更改这些设置：取消选定积极模式。选中 **Supports Subnets**。在“Authentication Method”下，选中 **Pre-Shared Secret**。这与以下命令一致：`crypto isakmp policy #authentication pre-`



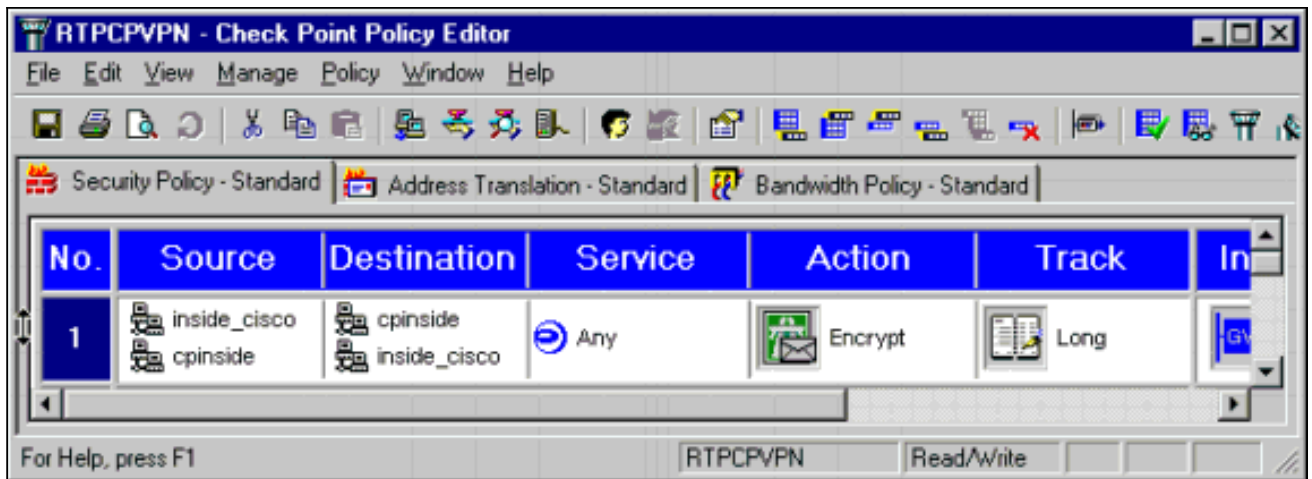
share

13. 单击 **Edit Secrets** 设置预共享密钥，以便与 `crypto isakmp key key address address Cisco`

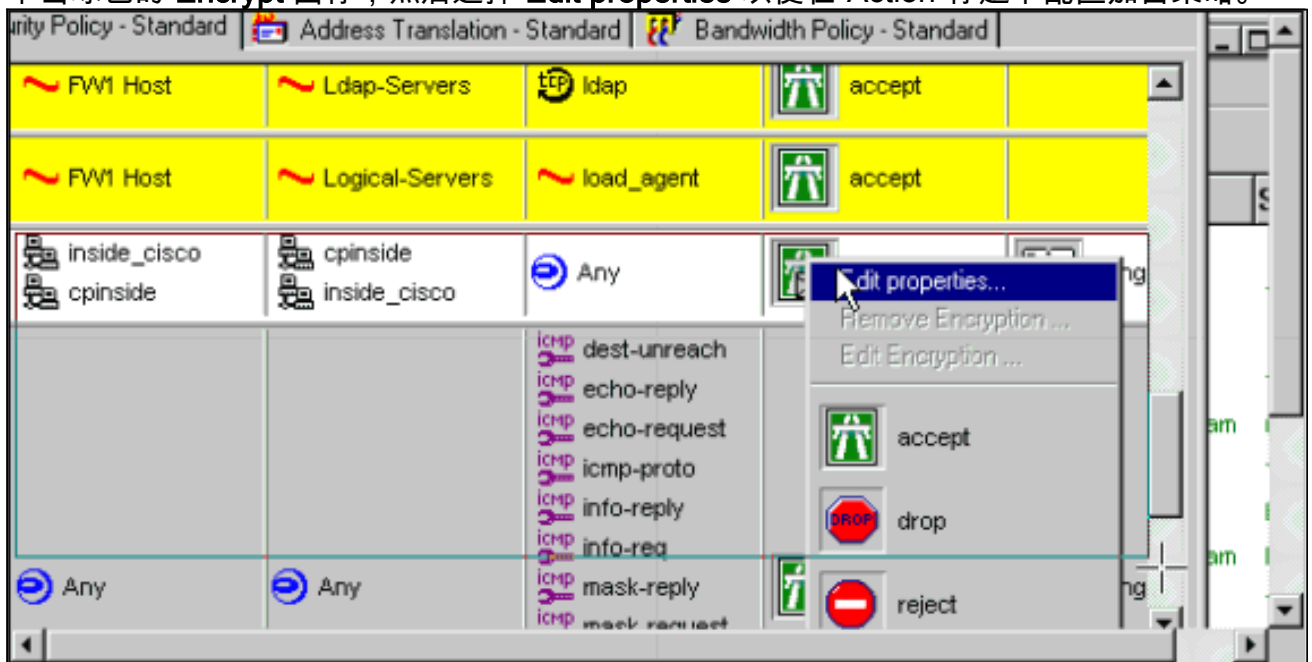


命令一致。

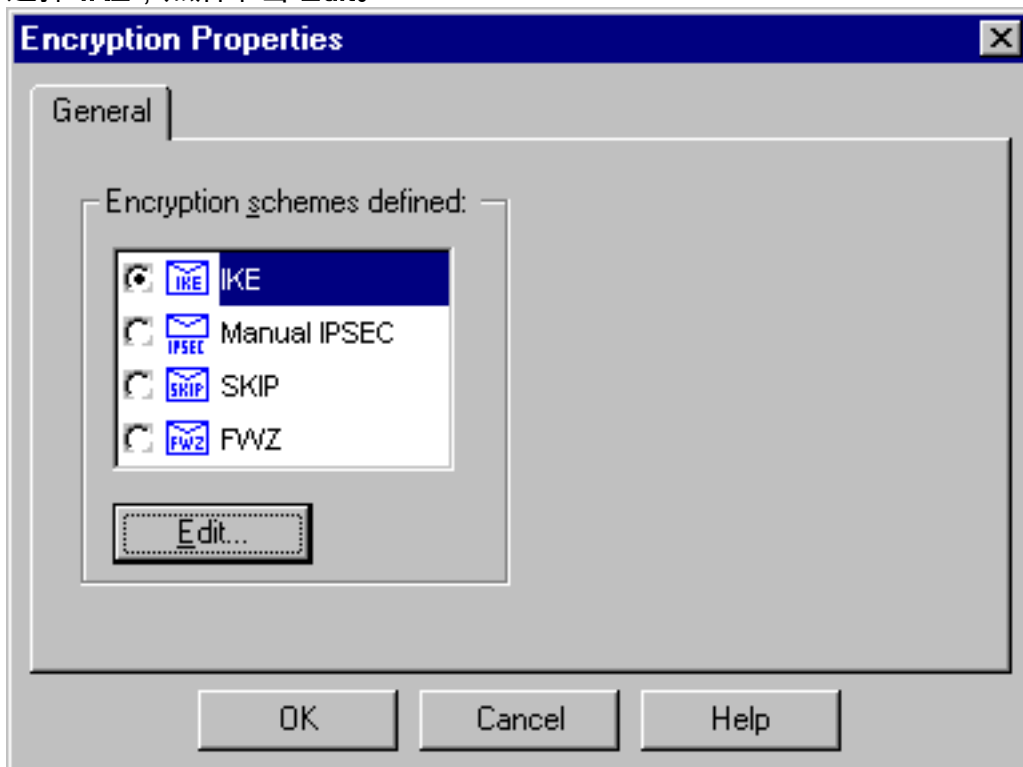
14. 在策略编辑器窗口，插入源和目的为“inside\_cisco”和“cpinside”(双向)这一规则。设置 **Service=Any**、**Action=Encrypt** 和 **Track=Long**。



15. 单击绿色的 **Encrypt** 图标，然后选择 **Edit properties** 以便在“Action”标题下配置加密策略。

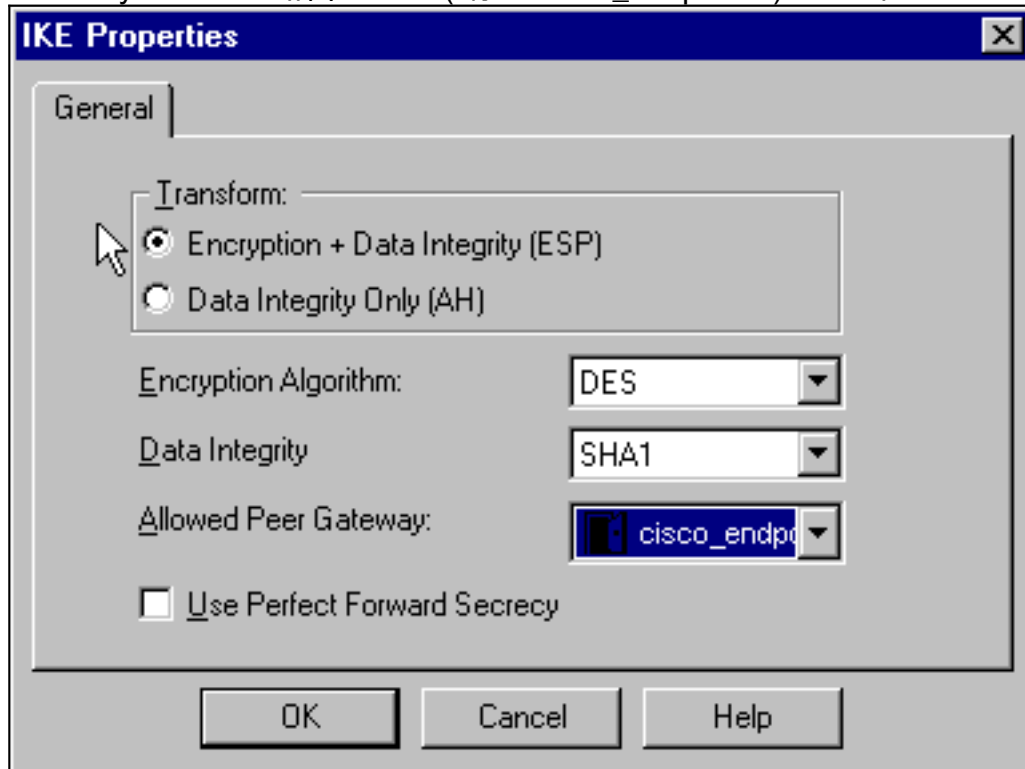


16. 选择 **IKE**，然后单击 **Edit**。



17. 在“IKE Properties”窗口中更改以下属性，以便与 `crypto ipsec transform-set rtplib esp-des`

`esp-sha-hmac` 命令中的 Cisco IPSec 转换一致：下面请变换，选择加密+数据完整性 (ESP)。“Encryption Algorithm”应为 DES，“Data Integrity”应为 SHA1，“Allowed Peer Gateway”应为外部路由器网关（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

本部分所提供的信息可用于确认您的配置是否正常工作。

[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。

- `show crypto isakmp sa` - 查看对等体上的所有当前 IKE 安全连接 (SA)。
- `show crypto ipsec sa` - 查看当前 SA 使用的设置。

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

### 故障排除命令

**注意：** 使用 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- `debug crypto engine` - 显示关于加密引擎的调试消息，进行加密和解密。
- `debug crypto isakmp` — 显示关于 IKE 事件的消息。
- `debug crypto ipsec` — 显示 IPSec 事件。
- `clear crypto isakmp` - 清除所有活动的 IKE 连接。
- `clear crypto sa` - 清除所有 IPSec SA。

## 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。如果路由器未配置为匹配，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

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：

```
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

```

并且在另一个窗口：

```

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

```

**注意：** 这是Microsoft Windows NT安装。

发出以下命令以清除 Checkpoint 上的 SA：

```

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
```

在出现“Are you sure?”提示时，回答 **yes** 提示。

## 调试输出示例

```
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

```

## [相关信息](#)

- [IPsec 协商/IKE 协议](#)
- [配置 IPSec 网络安全](#)
- [配置 Internet 密钥交换安全协议](#)
- [技术支持和文档 - Cisco Systems](#)