配置 IPSec 隧道 - Cisco Secure PIX 防火墙到 Checkpoint 4.1 防火墙

目录

简介

此示例配置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。在我们的示例中，被加入的网络是思科安全PIX防火墙(PIX)内部的192.168.1.X 专用网络和Checkpoint内部的10.32.50.X专用网络。假设在开始此配置之前，流量从PIX内部和Checkpoint 4.1防火墙内部流向Internet（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：

- PIX软件版本5.3.1
- 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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

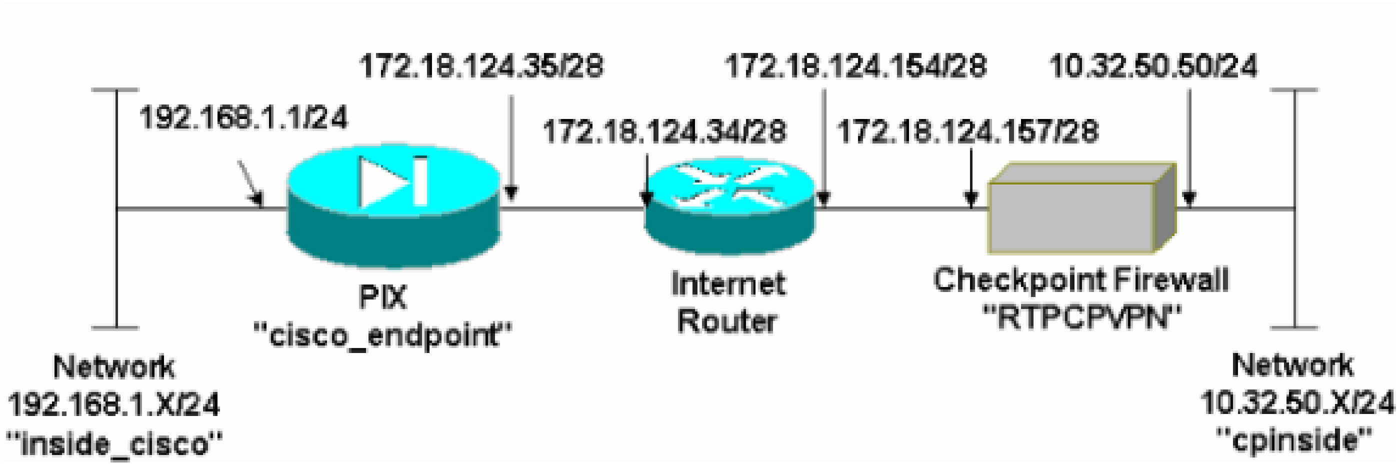
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用此图中所示的网络设置：



配置

本文使用在此部分显示的配置。

PIX 配置

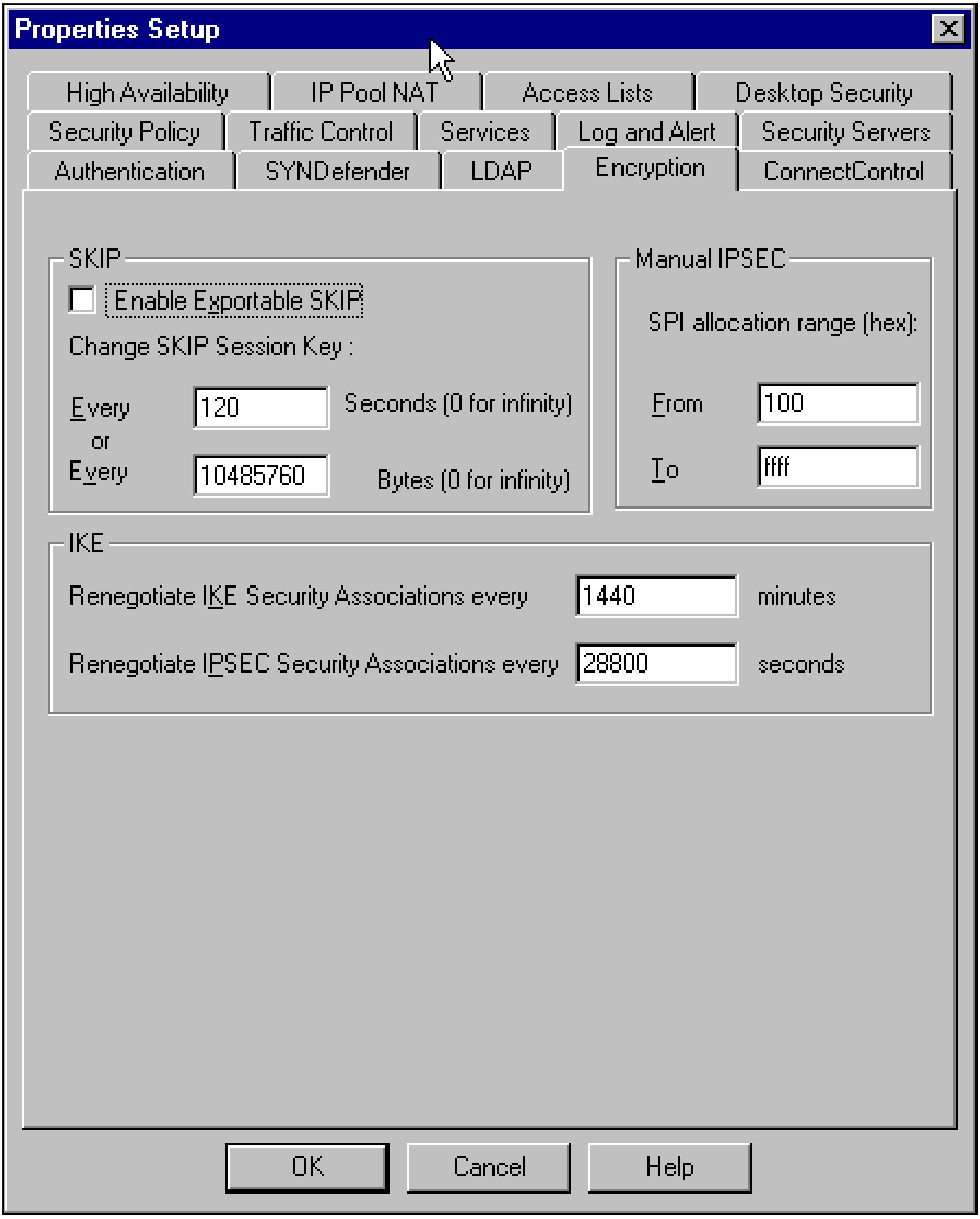
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
10.32.50.0 255.255.255.0
access-list 115 deny ip 192.168.1.0 255.255.255.0 any
```

```
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
logging monitor debugging
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.35 255.255.255.240
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.36
nat (inside) 0 access-list 115
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.34 1
timeout xlate 3:00:00g SA 0x80bd6a10, conn_id = 0
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- IPSec configuration sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp
crypto map rtpmap 10 match address 115
crypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap 10 set security-association lifetime
seconds
3600 kilobytes 4608000
crypto map rtpmap interface outside
!--- IKE configuration isakmp enable outside
isakmp key ******** address 172.18.124.157 netmask
255.255.255.240
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
```

```
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

检查点防火墙

1. 由于供应商之间IKE和IPSec的默认寿命各不相同，选择Properties>Encryption ，设置PIX默认的Checkpoint寿命。PIX默认IKE生存期为86400秒（=1440分钟），可通过以下命令修改：**isakmp policy # lifetime 86400**PIX IKE生命期可以配置在60-86400秒之间。PIX默认IPSec生命期为28800秒，可通过以下命令修改：**crypto ipsec security-association lifetime seconds #**您可以配置120-86400秒之间的PIX IPSec生存期。



SKIP

□ Enable Exportable SKIP

Change SKIP Session Key :

Every 120 Seconds (0 for infinity)

or

Every 10485760 Bytes (0 for infinity)

Manual IPSEC

SPI allocation range (hex):

From 100

To ffff

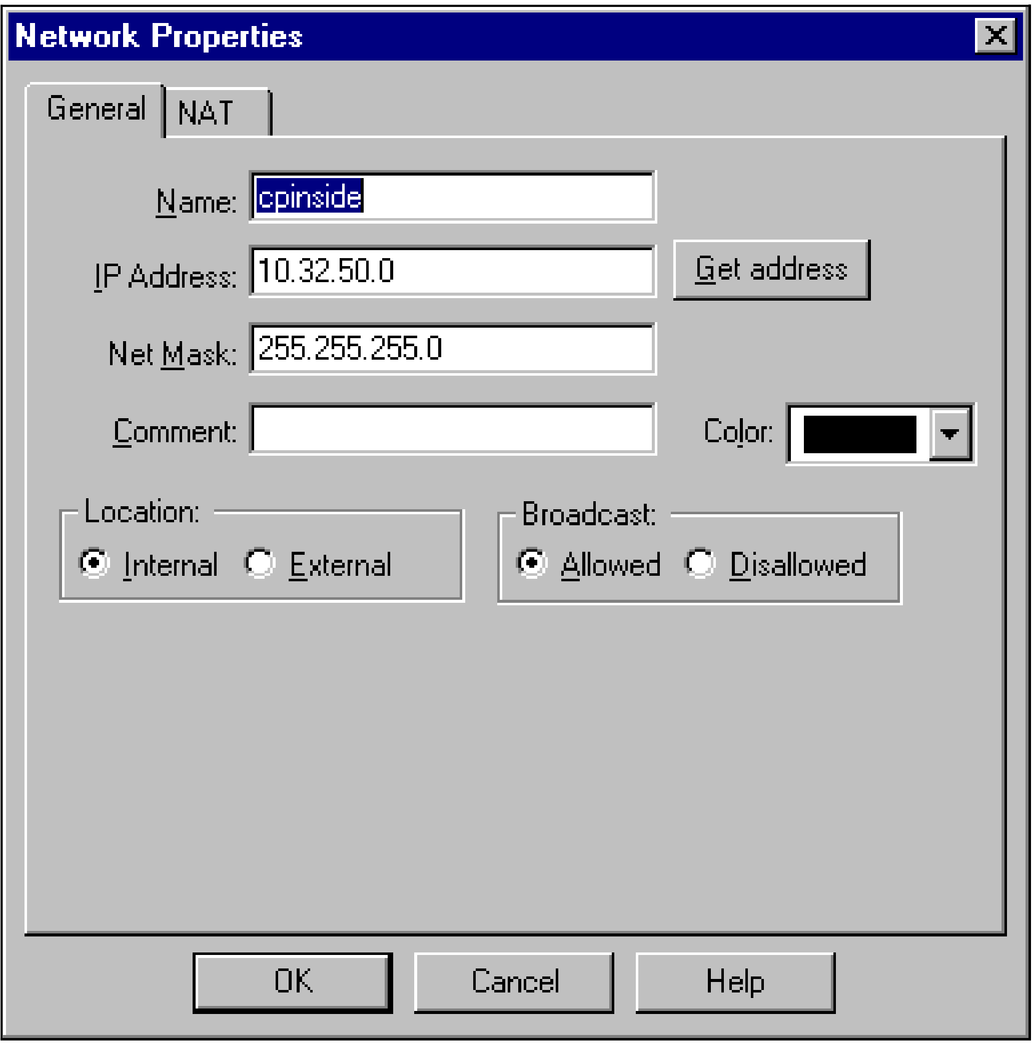
IKE

Renegotiate IKE Security Associations every 1440 minutes

Renegotiate IPSEC Security Associations every 28800 seconds

2. "选择Manage > Network objects > New (或 Edit) > Network，配置Checkpoint后的内部(""cpinside"") 网络的对象。"这必须与此PIX命令中的目标（秒）网络一致：**access-list 115**

permit ip 192.168.1.0 255.255.255.0 10.32.50.0 255.255.255.0



Network Properties

Name: cpinside

IP Address: 10.32.50.0

Net Mask: 255.255.255.0

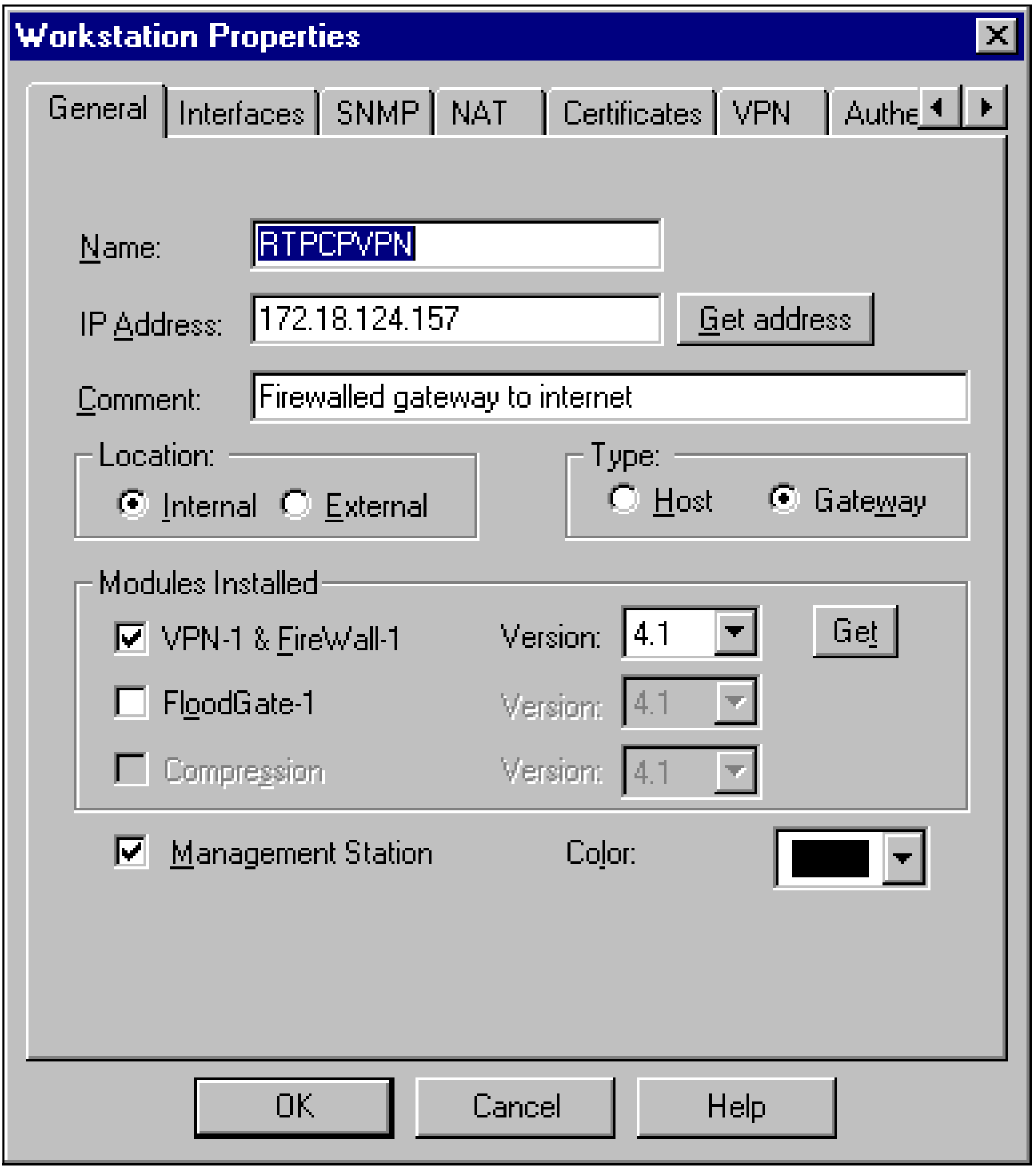
Comment:

Color: ■

Location: ● Internal ○ External

Broadcast: ● Allowed ○ Disallowed

3. 选择**Manage** > **Network objects** > **Edit** 以编辑PIX在此命令中指向的网关(“RTPCPVPN” Checkpoint)终端的对象：**crypto map name # set peer ip_address**在 Location 下，请选择 **Internal**。对于“Type”，选择 **Gateway**。在Modules Installed下，选中**VPN-1 & FireWall-1复选**框，并选中Management Station复**选框**



Workstation Properties

General | Interfaces | SNMP | NAT | Certificates | VPN | Authe

Name: RTPCPVPN

IP Address: 172.18.124.157 [Get address]

Comment: Firewalled gateway to internet

Location: ● Internal ○ External

Type: ○ Host ● Gateway

Modules Installed

☑ VPN-1 & FireWall-1 Version: 4.1 [Get]

□ FloodGate-1 Version: 4.1

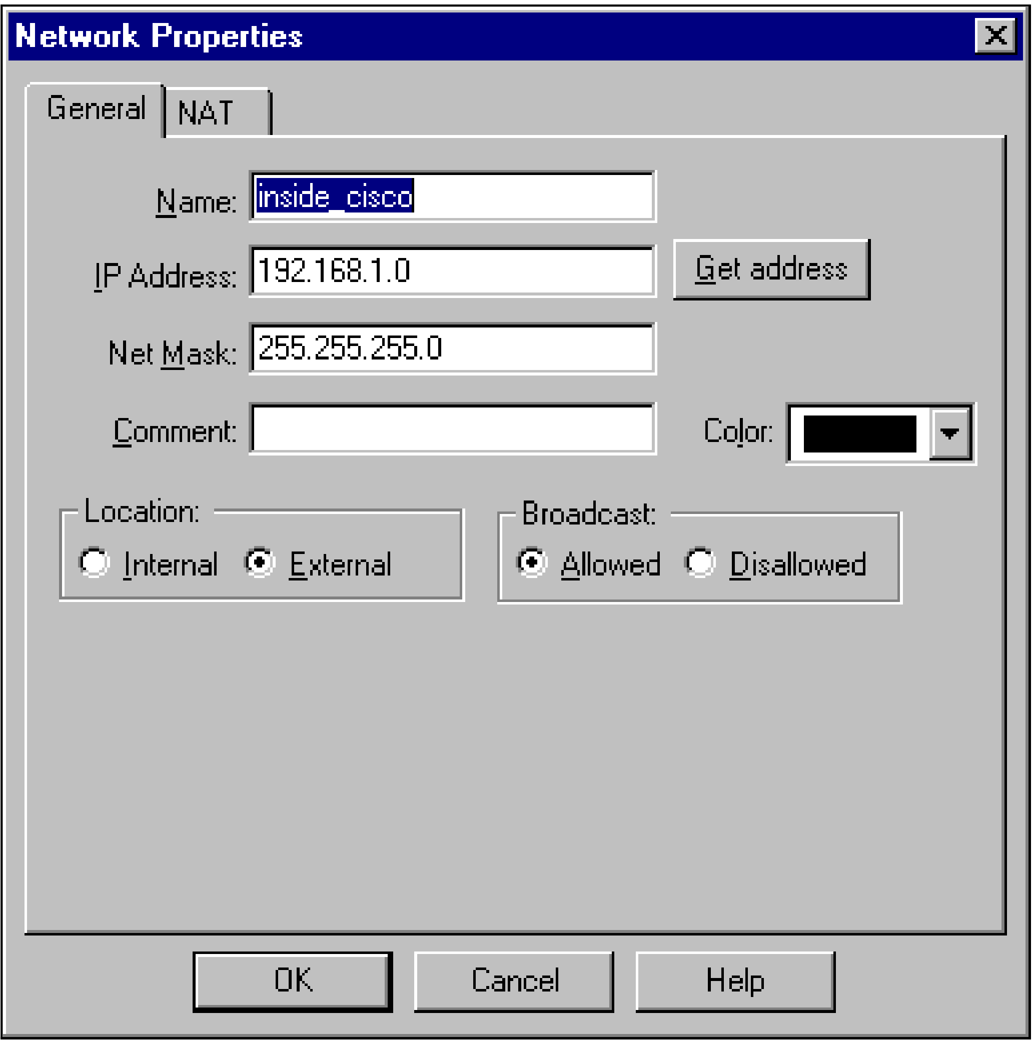
□ Compression Version: 4.1

☑ Management Station Color: ■

[OK] [Cancel] [Help]

:

4. 选择Manage > Network objects > New (or Edit) > Network，配置PIX后的外部("inside_cisco") 网络的对象。这必须与此PIX命令中的源（第一个）网络一致：**access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**



Network Properties

General | NAT

Name: inside_cisco

IP Address: 192.168.1.0

Net Mask: 255.255.255.0

Comment:

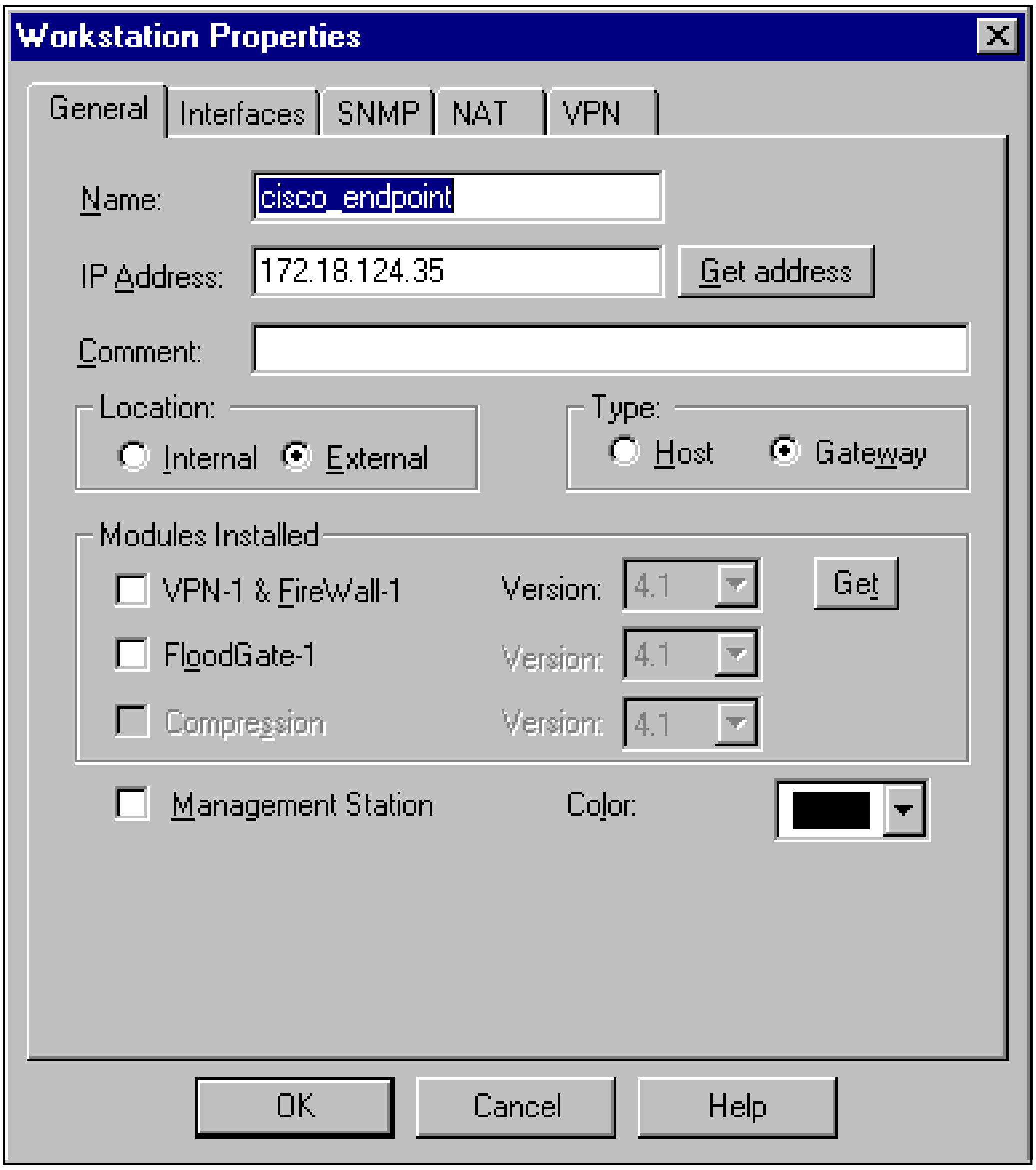
Color: ■

Location: ○ Internal ● External

Broadcast: ● Allowed ○ Disallowed

255.255.255.0

5. 选择**Manage** > **Network objects** > **New** > **Workstation** 为外部("cisco_endpoint")PIX网关添加对象。这是应用此命令的PIX接口：**加密映射名称接口外部**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。



Name: cisco_endpoint

IP Address: 172.18.124.35

Comment:

Location: ○ Internal ● External

Type: ○ Host ● Gateway

Modules Installed

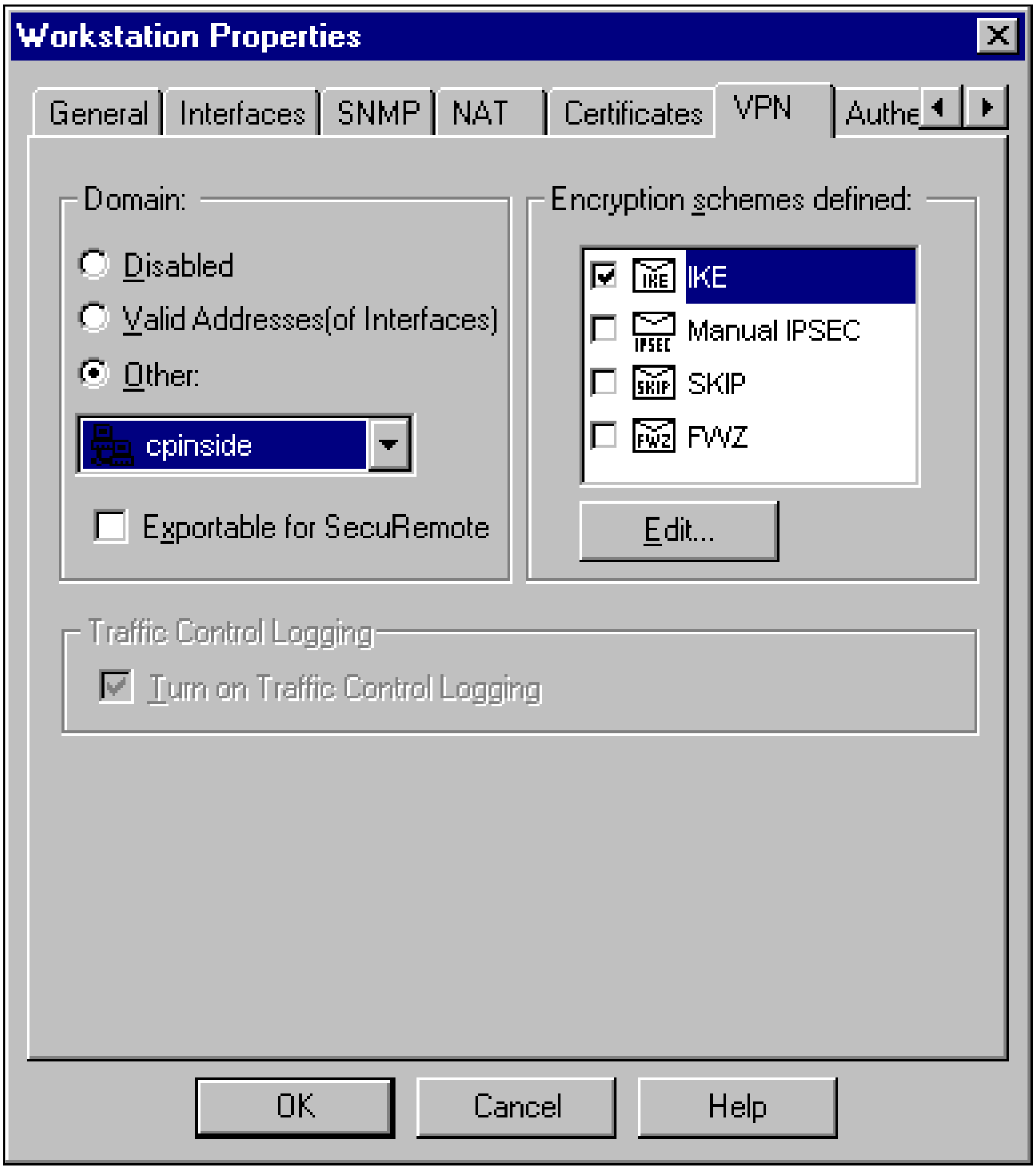
□ VPN-1 & FireWall-1 Version: 4.1

□ FloodGate-1 Version: 4.1

□ Compression Version: 4.1

□ Management Station Color: ■

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。**



Workstation Properties

General Interfaces SNMP NAT Certificates VPN Authe

Domain:

○ Disabled

○ Valid Addresses(of Interfaces)

● Other:

cpinside

□ Exportable for SecuRemote

Encryption schemes defined:

☑ IKE

□ Manual IPSEC

□ SKIP

□ FWZ

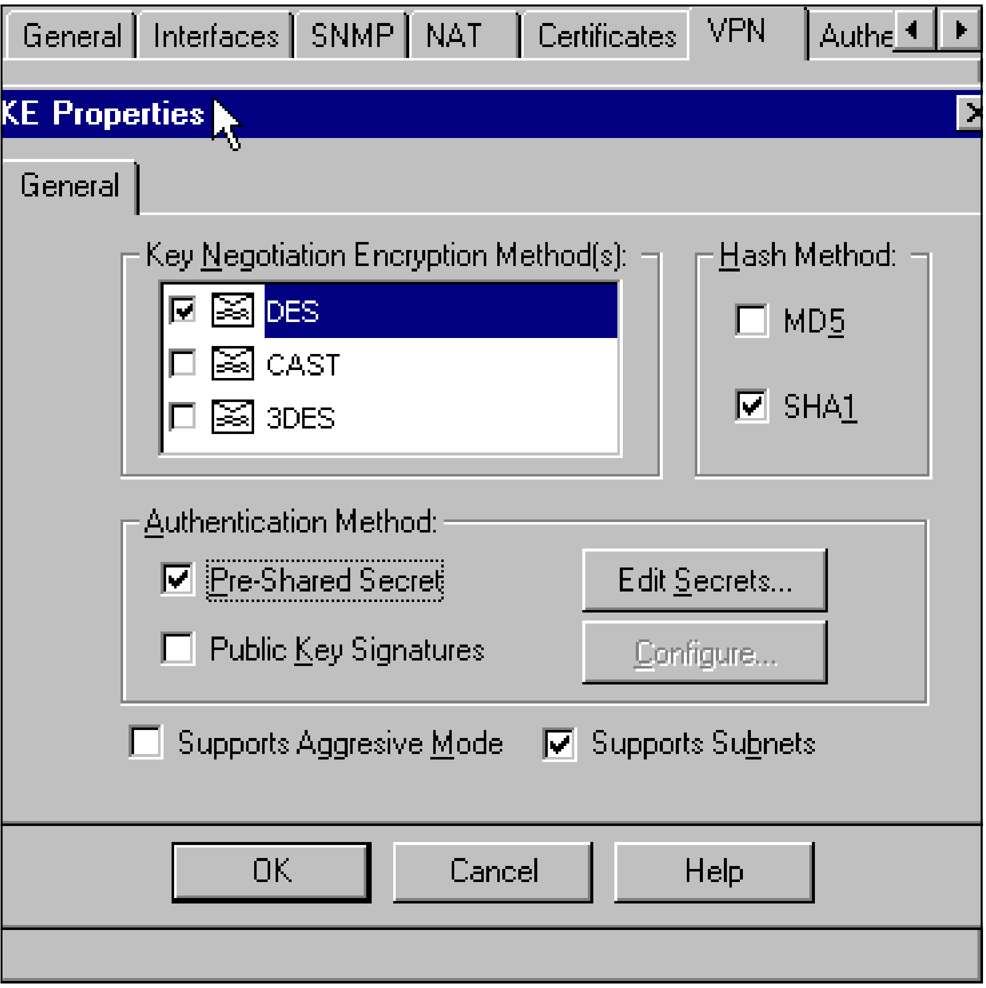
Edit...

Traffic Control Logging

☑ Turn on Traffic Control Logging

OK Cancel Help

7. 更改DES加密的IKE属性以与以下命令一致：**isakmp policy # encryption des**
8. 将IKE属性更改为SHA1散列以与以下命令一致：**isakmp policy # hash sha**更改这些设置：取消选定积极模式。选中支持**子网复**选框。在Authentication Method下，选中**Pre-Shared Secret复选**框。这与以下命令相同：**isakmp policy # authentication pre-**



KE Properties

General

Key Negotiation Encryption Method(s):

☑ DES
☐ CAST
☐ 3DES

Hash Method:

☐ MD5
☑ SHA1

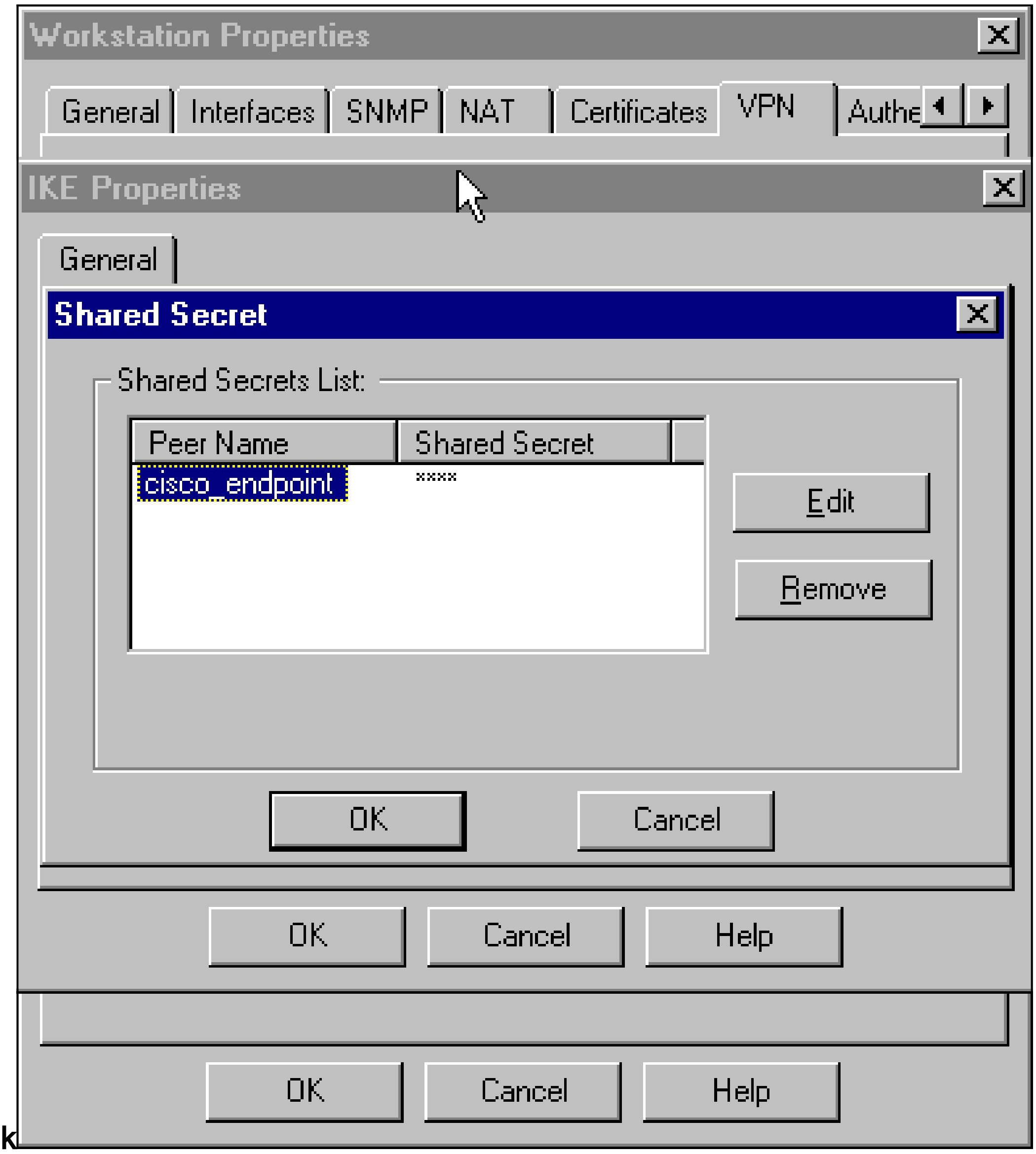
Authentication Method:

☑ Pre-Shared Secret
☐ Public Key Signatures

☐ Supports Aggresive Mode ☑ Supports Subnets

share

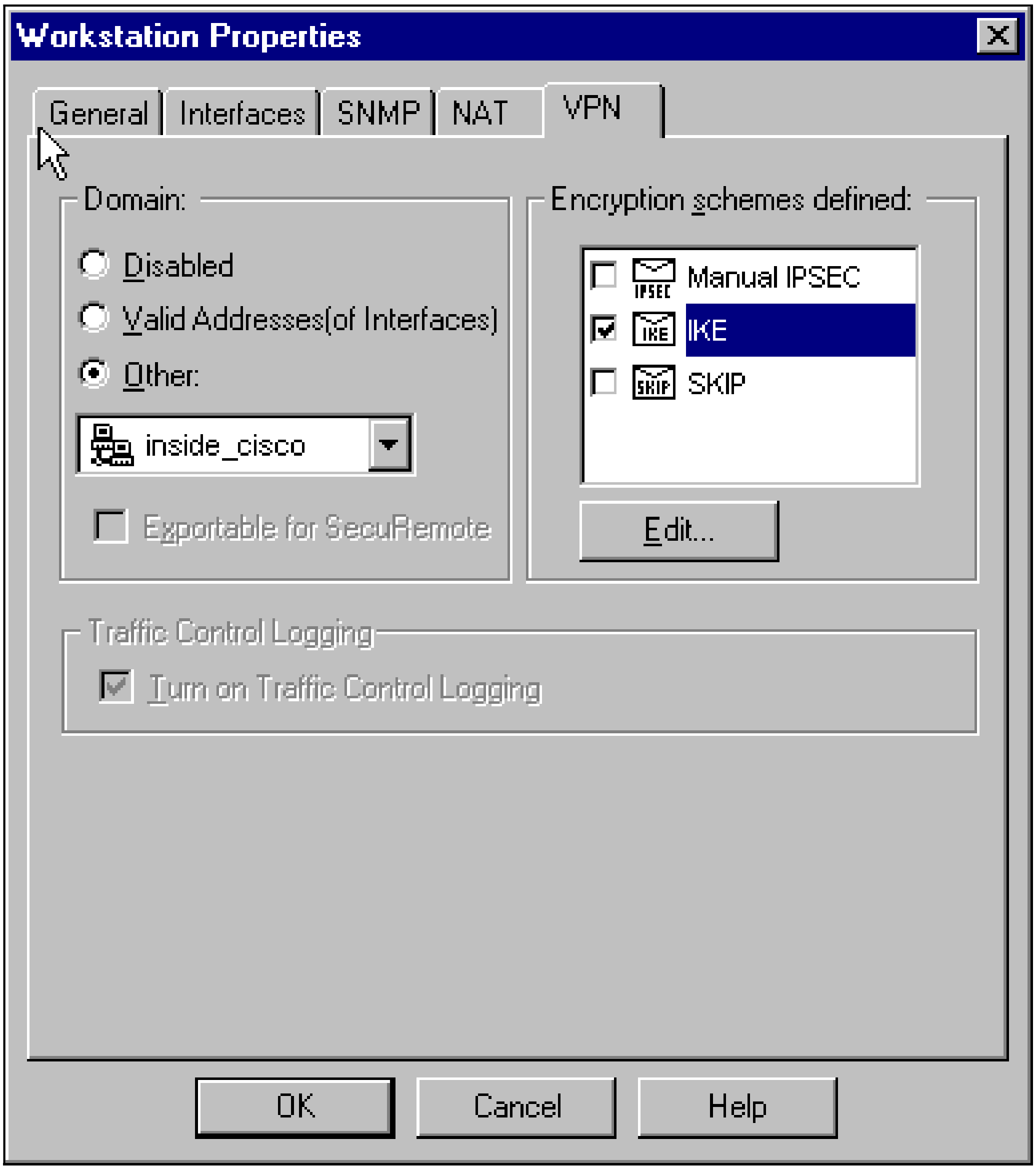
9. 单击**Edit Secrets**，将预共享密钥设置为与PIX命令一致：**isakmp key key address address**



Peer Name	Shared Secret
cisco_endpoint	****

netmask netmask

10. 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PIX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**。



Workstation Properties

General Interfaces SNMP NAT VPN

Domain:

○ Disabled

○ Valid Addresses(of Interfaces)

● Other: inside_cisco

□ Exportable for SecuRemote

Encryption schemes defined:

□ Manual IPSEC

☑ IKE

□ SKIP

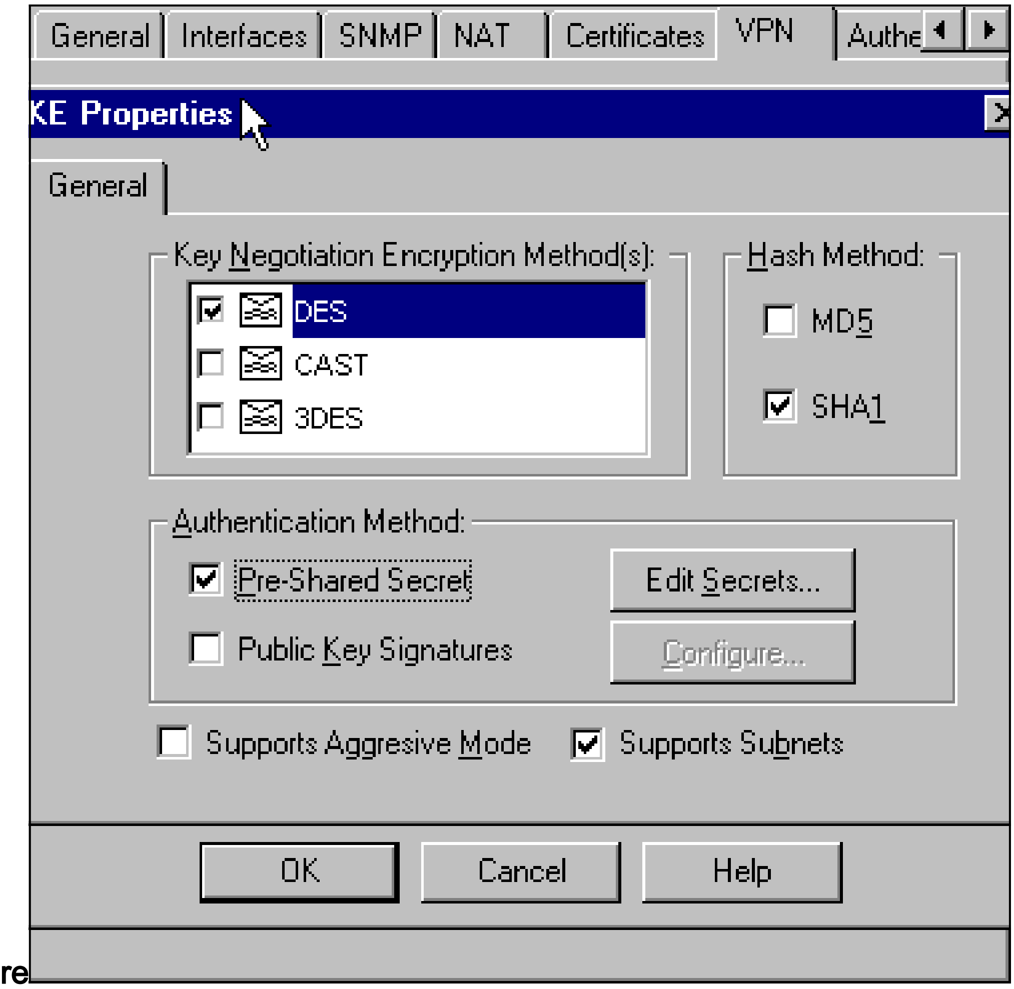
Edit...

Traffic Control Logging

☑ Turn on Traffic Control Logging

OK Cancel Help

11. 更改IKE属性DES加密以与以下命令一致：**isakmp policy # encryption des**
12. 将IKE属性更改为SHA1散列以与以下命令一致：**crypto isakmp policy # hash sha**更改这些设置：取消选定积极模式。选中支持**子网复**选框。在Authentication Method下，选中**Pre-Shared Secret复**选框。此操作与以下命令一致：**isakmp policy # authentication pre-**



KE Properties

General

Key Negotiation Encryption Method(s):

☑ DES
☐ CAST
☐ 3DES

Hash Method:

☐ MD5
☑ SHA1

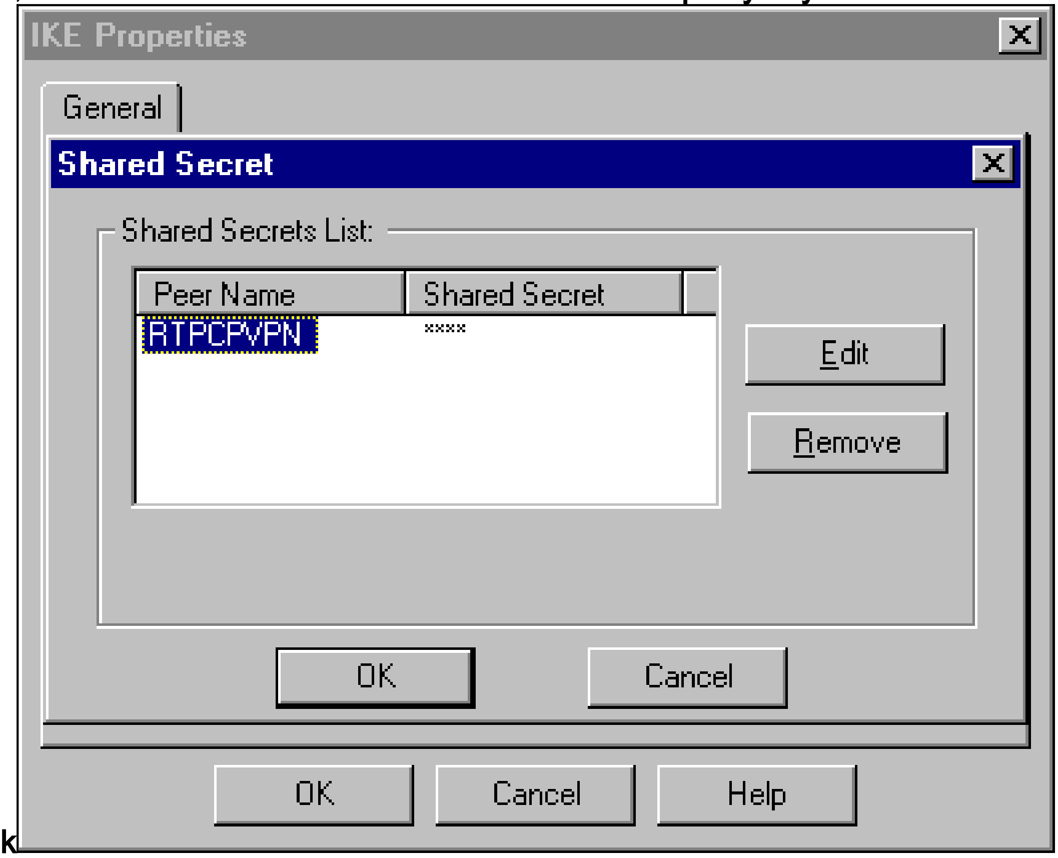
Authentication Method:

☑ Pre-Shared Secret
☐ Public Key Signatures

☐ Supports Aggresive Mode ☑ Supports Subnets

share

13. 单击**Edit Secrets**，将预共享密钥设置为与此PIX命令一致：**isakmp key key address address netmask netmask**



IKE Properties

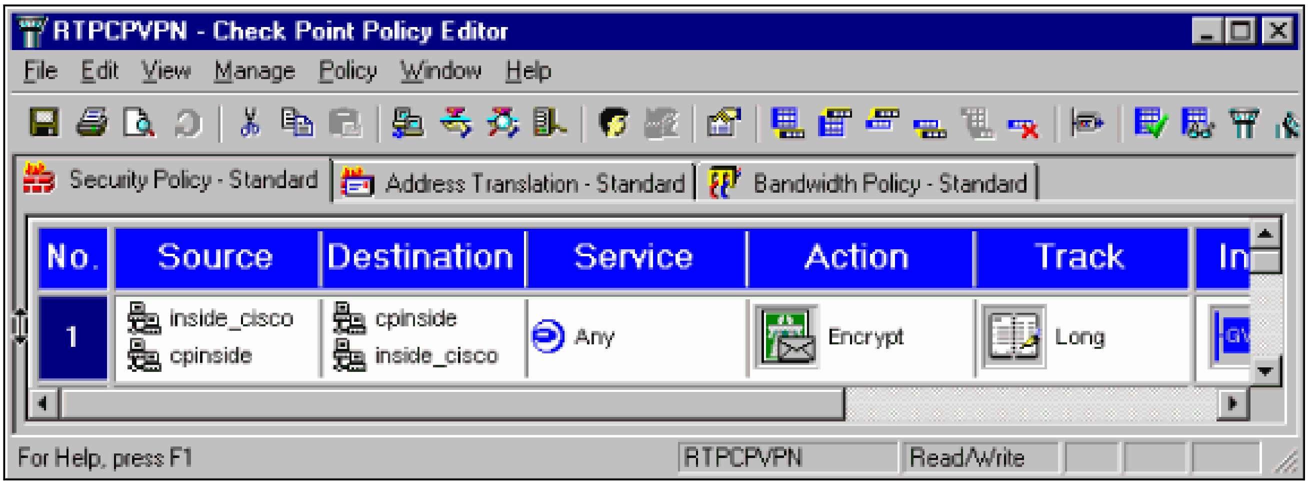
General

Shared Secret

Shared Secrets List:

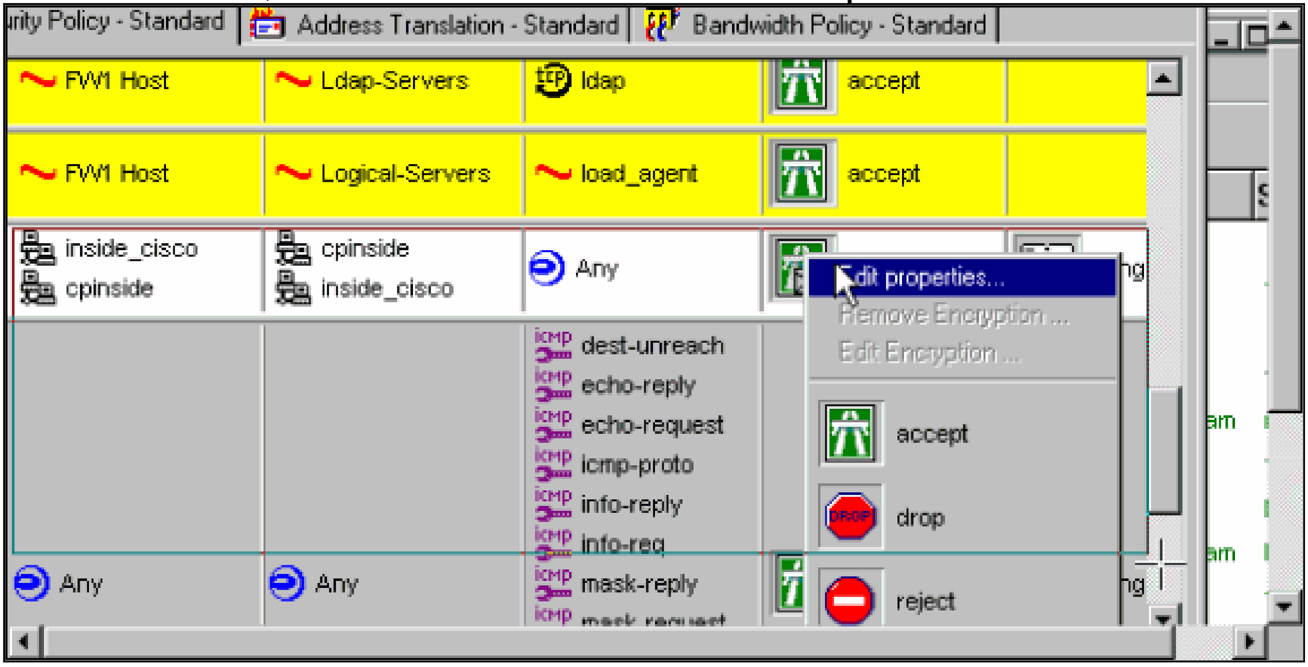
Peer Name	Shared Secret
RTPCPVPN	****

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**。


RTPCPVPN - Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - Standard
Address Translation - Standard
Bandwidth Policy - Standard
For Help, press F1
RTPCPVPN
Read/Write

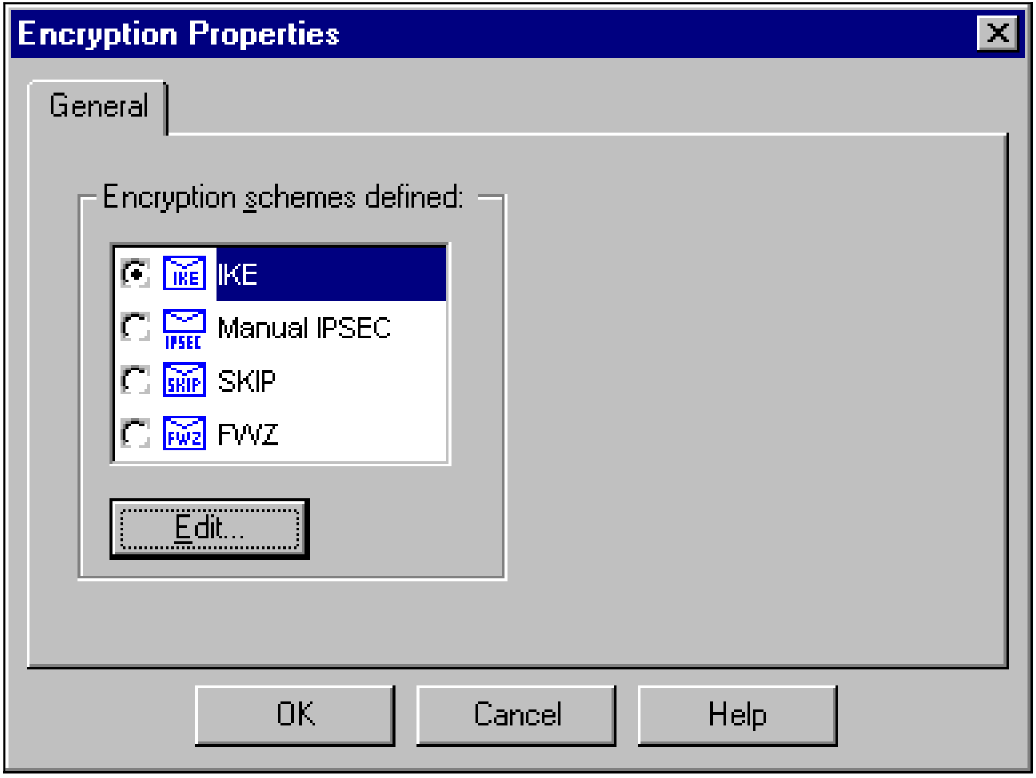
No.	Source	Destination	Service	Action	Track	In
1	inside_cisco cpinside	cpinside inside_cisco	Any	Encrypt	Long	GW

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。**



FW1 Host	Ldap-Servers	ldap	accept
FW1 Host	Logical-Servers	load_agent	accept
inside_cisco cpinside	cpinside inside_cisco	Any	
		dest-unreach echo-reply echo-request icmp-proto info-reply info-req	
Any	Any	mask-reply mask-request	

16. 选择 **IKE**，然后单击 **Edit**。

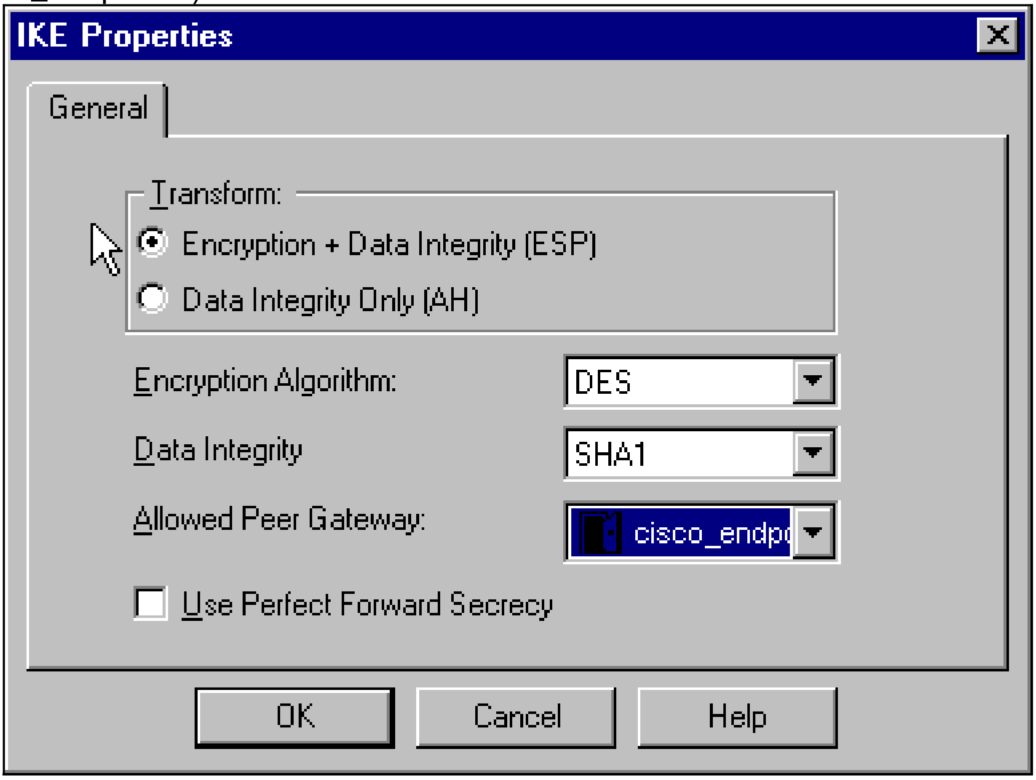


Encryption schemes defined:

- ● IKE
- ○ Manual IPSEC
- ○ SKIP
- ○ FWZ

17. 在IKE属性屏幕上，更改这些属性以与此命令中的PIX IPSec转换一致：**crypto ipsec**

transform-set myset esp-des esp-sha-hmac下面请变换，选择**加密+数据完整性(ESP)**。 加密算法必须**是DES**，数据完整性必须是**SHA1**，允许的对等网关必须是外部PIX网关（称为“cisco_endpoint”）。 Click



IKE Properties

General

Transform:

● Encryption + Data Integrity (ESP)

○ Data Integrity Only (AH)

Encryption Algorithm: DES

Data Integrity: SHA1

Allowed Peer Gateway: cisco_endp

□ Use Perfect Forward Secrecy

OK.

18. 配置Checkpoint后，在Checkpoint菜单上选择**Policy** > **Install**以使更改生效。

debug、show和clear命令

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

在发出 **debug 命令之前，请参阅**有关 debug 命令的重要信息。

Cisco PIX 防火墙

- **debug crypto engine** — 显示有关执行加密和解密的加密引擎的调试消息。
- **debug crypto isakmp** — 显示有关IKE事件的消息。
- **debug crypto ipsec** — 显示IPSec事件。
- **show crypto isakmp sa - 查看对等体上的所有当前 IKE 安全关联 (SA)。**
- **show crypto ipsec sa** — 查看当前安全关联使用的设置。
- **clear crypto isakmp sa** — （从配置模式）清除所有活动IKE连接。
- **clear crypto ipsec sa** — （从配置模式）删除所有IPSec安全关联。

检查点：

由于在步骤14中显示的“策略编辑器”窗口中为“长”设置了“跟踪”，因此，在日志查看器中，已拒绝的流量以红色显示。输入以下命令可获得更详细的调试：

```
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
```

注意：这是Microsoft Windows NT安装。

您可以使用以下命令清除检查点上的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"你**确**定吗"回答是？提示。

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

当检查点的加密域中配置了多个相邻内部网络时，设备可以根据相关流量自动汇总这些网络。如果PIX上的加密ACL未配置为匹配，隧道可能会失败。例如，如果将内部网络10.0.0.0 /24和10.0.1.0 /24配置为包含在隧道中，则可将其总结为10.0.0.0 /23。

PIX 的调试输出示例

```
cisco_endpoint# show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
        tx      Off
        rx      Off
        open    Off
        cable   Off
        txdmp   Off
        rxdmp   Off
        ifc     Off
        rxip    Off
        txip    Off
        get     Off
        put     Off
        verify  Off
        switch  Off
        fail    Off
        fmsg    Off
```

```
cisco_endpoint# term mon
cisco_endpoint#
ISAKMP (0): beginning Quick Mode exchange,
M-ID of 2112882468:7df00724IPSEC(key_engine):
 got a queue event...
IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA
        from  172.18.124.157 to   172.18.124.35 for prot 3
70
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.35
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2112882468

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-SHA
ISAKMP (0): atts are acceptable.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

ISAKMP (0): processing NONCE payload. message ID = 2112882468

ISAKMP (0): processing ID payload. message ID = 2112882468
ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (0): Creating IPSec SAs
        inbound SA from  172.18.124.157 to   172.18.124.35 (proxy
      10.32.50.0 to 192.168.1.0)
        has spi 2641490588 and conn_id 3 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.18.124.35 to  172.18.124.157 (proxy
     192.168.1.0 to 10.32.50.0)
        has spi 3955804195 and conn_id 4 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
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= 28800s and 4608000kb,
    spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
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= 28800s and 4608000kb,
    spi= 0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR2303: 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= 28800s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0,
flags= 0x4004

602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi=
0x9d71f29c(2641490588),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3

602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi=
0xebc8c823(3955804195),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4

cisco_endpoint# sho cry ips sa

interface: outside
    Crypto map tag: rtpmap, 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): (0.0.0.0/0.0.0.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0 #send errors 0, #recv errors 0

     local crypto endpt.: 172.18.124.35,
     remote crypto endpt.: 172.18.124.157
     path mtu 1500, ipsec overhead 0, media mtu 1500
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   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: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #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, ipsec overhead 56, media mtu 1500
     current outbound spi: ebc8c823
     inbound esp sas:
      spi: 0x9d71f29c(2641490588)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3, crypto map: rtpmap
        sa timing: remaining key lifetime (k/sec): (4607999/28777)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xebc8c823(3955804195)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 4, crypto map: rtpmap
        sa timing: remaining key lifetime (k/sec): (4607999/28777)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

cisco_endpoint# sho cry is sa
        dst            src         state     pending    created
  172.18.124.157   172.18.124.35    QM_IDLE        0           2
```

相关信息

- PIX 支持页
- PIX 命令参考
- 请求注解 (RFC)
- 配置 IPSec 网络安全
- 配置 Internet 密钥交换安全协议
- PIX 5.2 ：配置 IPSec
- PIX 5.3 ：配置 IPSec
- IPSec 支持页面
- 技术支持 - Cisco Systems