Configurando um túnel IPSec - Cisco Secure PIX Firewall para o Checkpoint 4.1 Firewall

Contents

Introduction

Esta configuração de exemplo demonstra como formar um túnel IPSec com chaves pré-compartilhadas para unir duas redes privadas. Em nosso exemplo, as redes associadas são a rede privada 192.168.1.X dentro do Cisco Secure Pix Firewall (PIX) e a rede privada 10.32.50.X dentro do Ponto de Controle. Supõe-se que o tráfego de dentro do PIX e de dentro do Checkpoint 4.1 Firewall para a Internet (representado aqui pelas redes 172.18.124.X) flui antes de iniciar essa configuração.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software PIX versão 5.3.1
- Checkpoint 4.1 Firewall

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

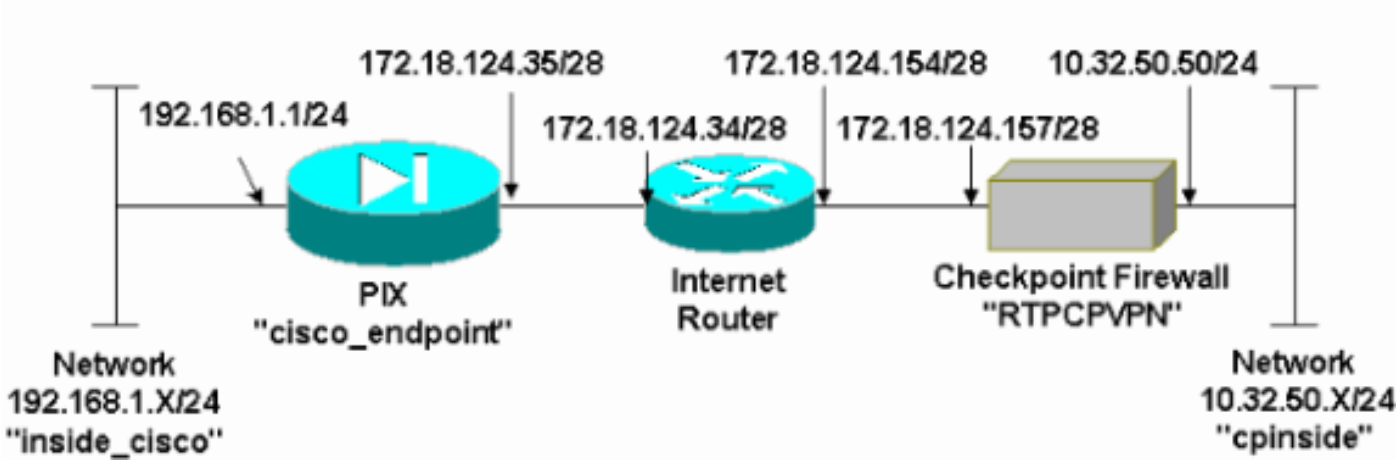
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta Command Lookup Tool (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama:



Configurações

Este documento usa as configurações mostradas nesta seção.

Configuração de PIX

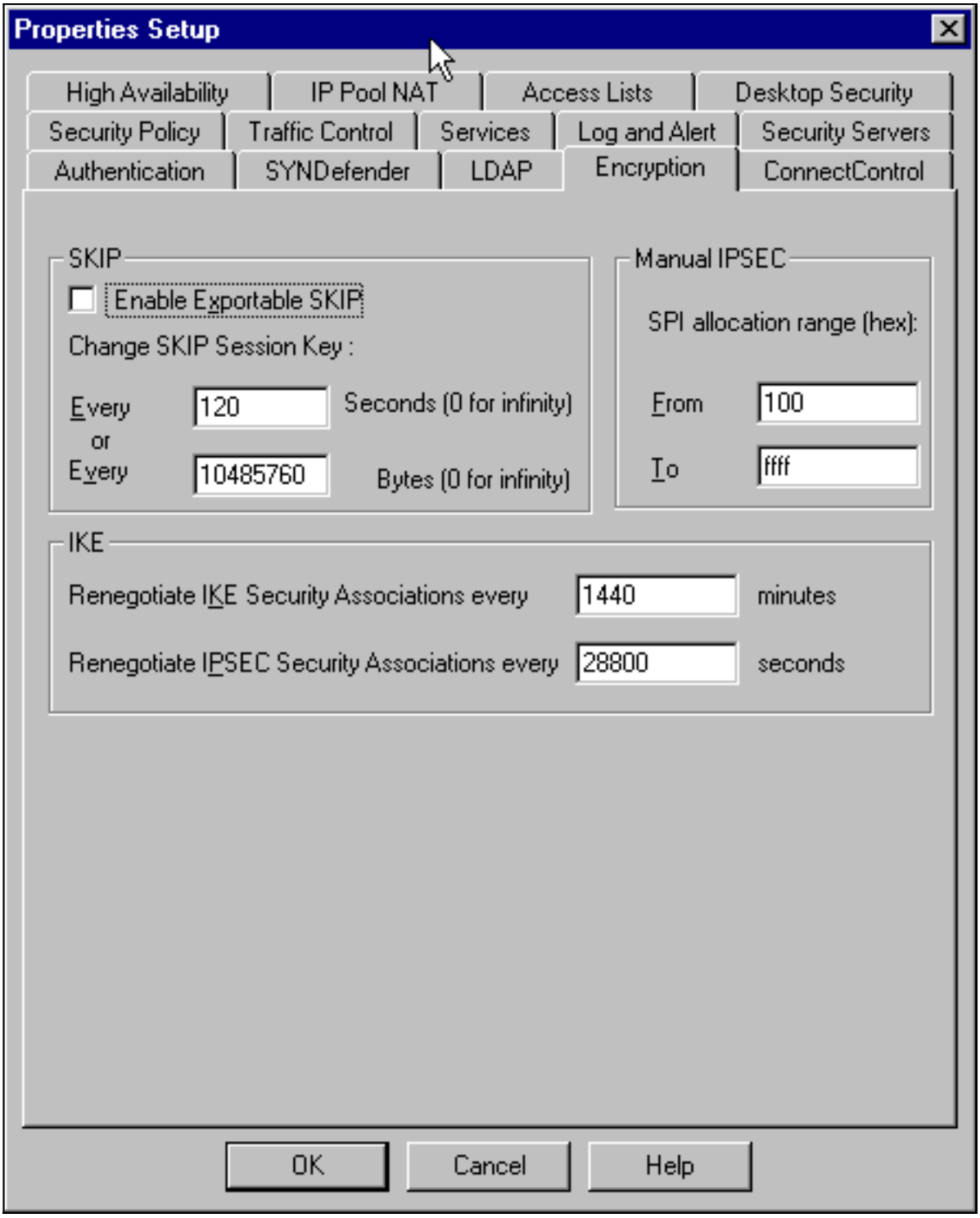
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
```

```
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
```

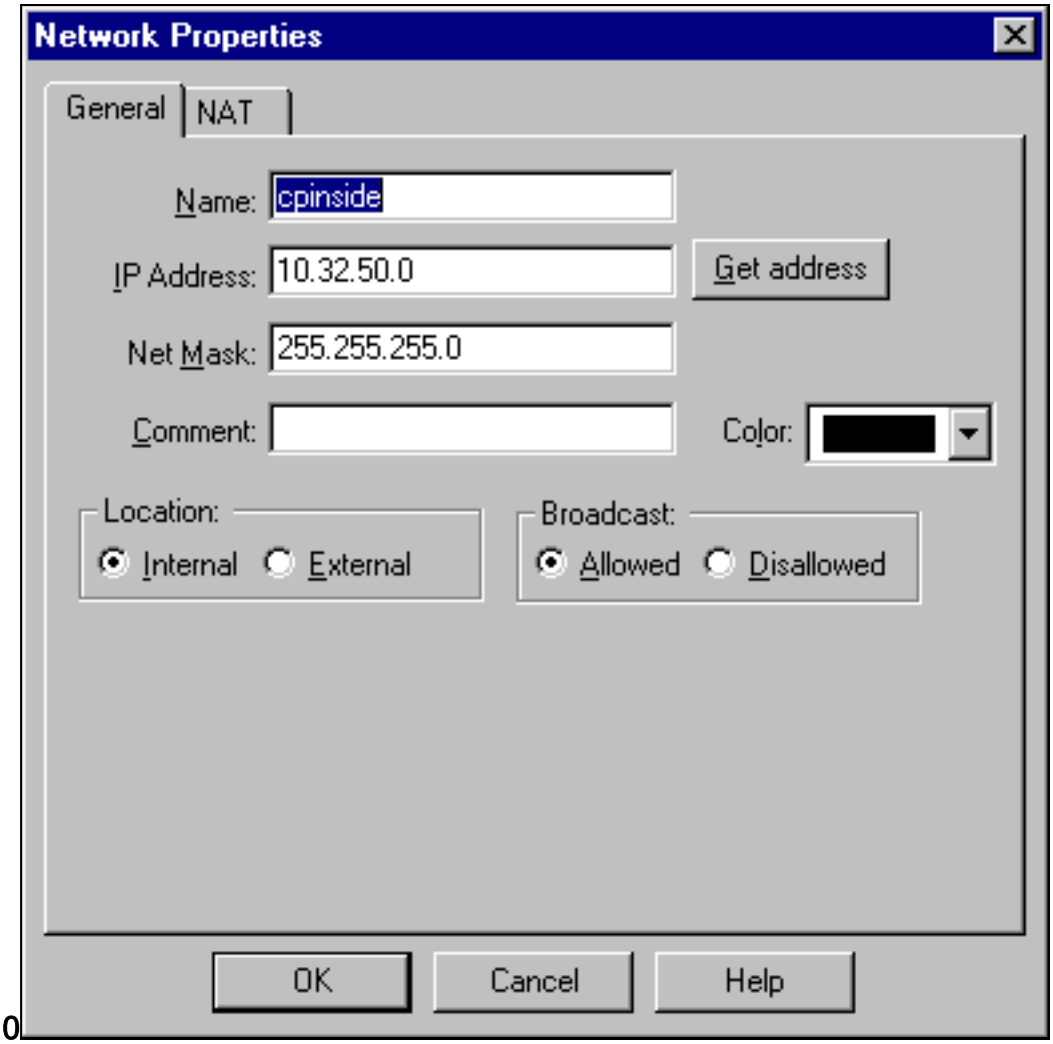
```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

Firewall de ponto de controle

1. Como a duração padrão do IPSec e do IKE difere entre os fornecedores, selecione Properties (Propriedades) > Encryption (Criptografia) para definir a duração de Checkpoint de acordo com os padrões do PIX.O tempo de vida do IKE padrão do PIX é de 86400 segundos (=1440 minutos), modificável por este comando: **isakmp policy # lifetime 86400**O tempo de vida do PIX IKE pode ser configurado entre 60 e 86400 segundos.O tempo de vida do IPSec padrão do PIX é de 28800 segundos, modificável por este comando: **crypto ipsec security-association lifetime seconds #**Você pode configurar uma duração de PIX IPSec entre 120 e 86400
   segundos.

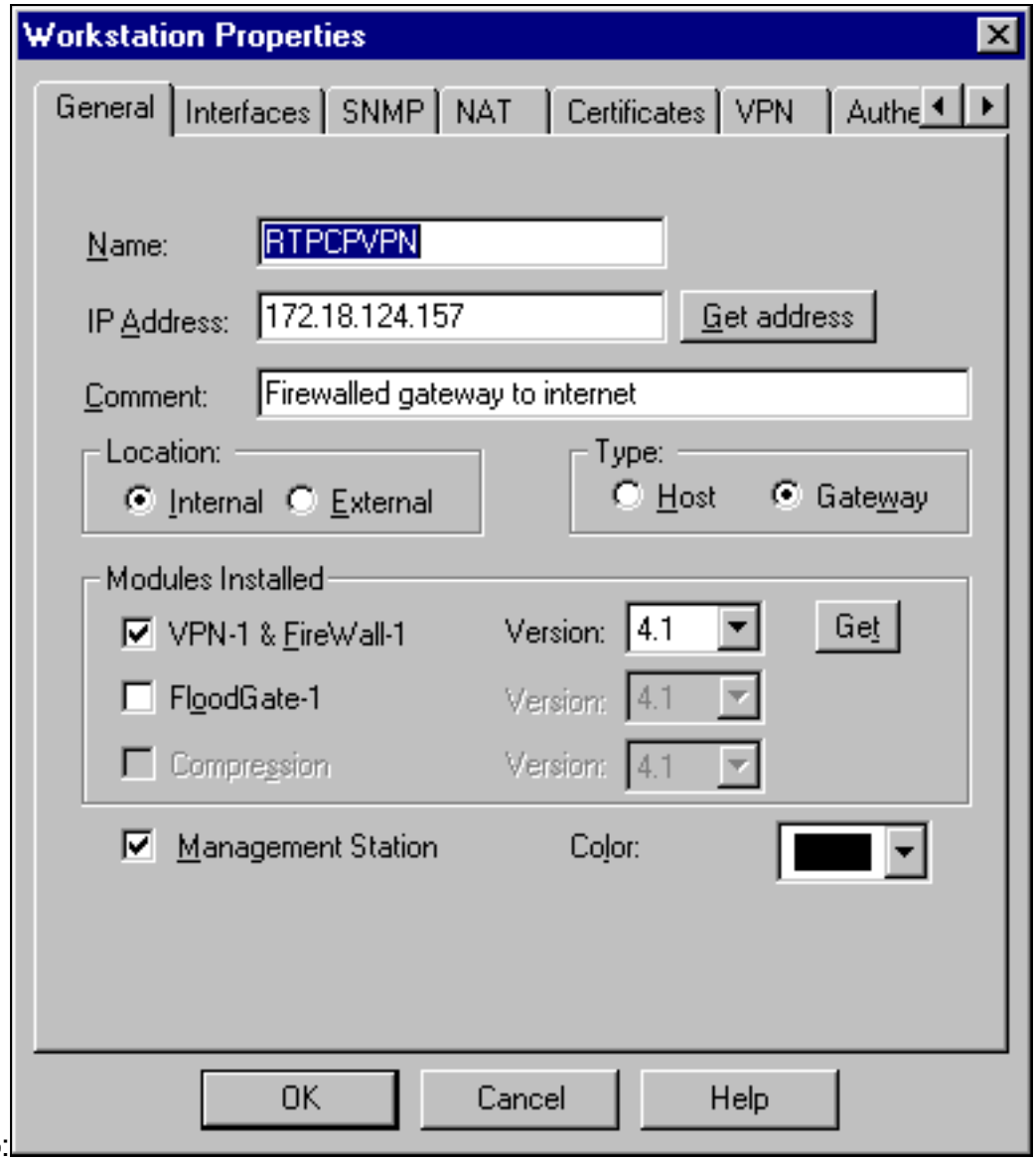


2. Selecione Gerenciar > Objetos de rede > Novo (ou Editar) > Rede para configurar o objeto para a rede interna ("cpinside") por trás do ponto de controle.Isso deve concordar com a rede de destino (segunda) neste comando PIX: **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**



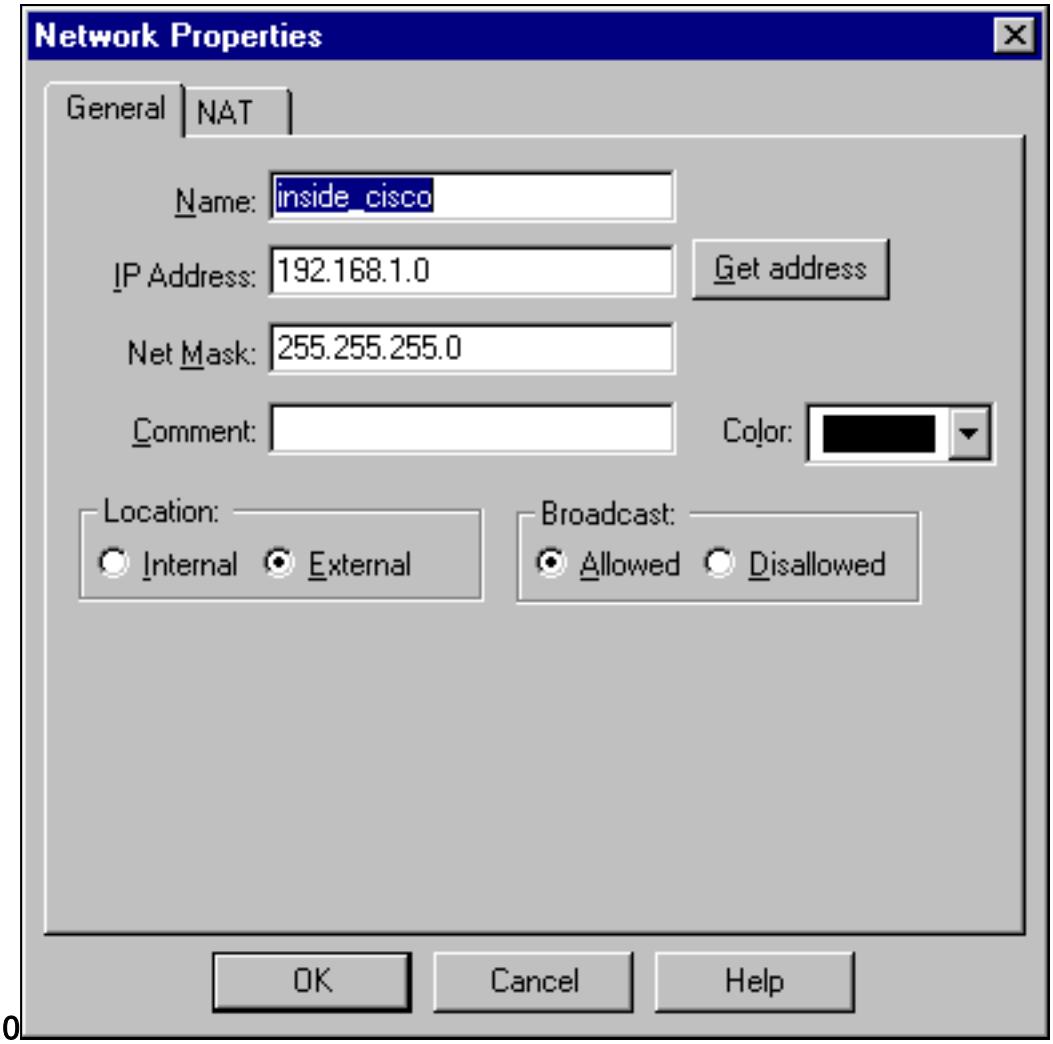
255.255.255.0

3. Selecione **Gerenciar > Objetos de rede > Editar** para editar o objeto para o ponto de extremidade do gateway ("RTPCPVPN" Checkpoint) que o PIX aponta para neste comando: **crypto map name # set peer ip_address**Em Local, selecione Interno. Para Tipo, selecione Gateway. Em Módulos instalados, marque a caixa de seleção **VPN-1 e FireWall-1** e também selecione a caixa de seleção **Estação de**



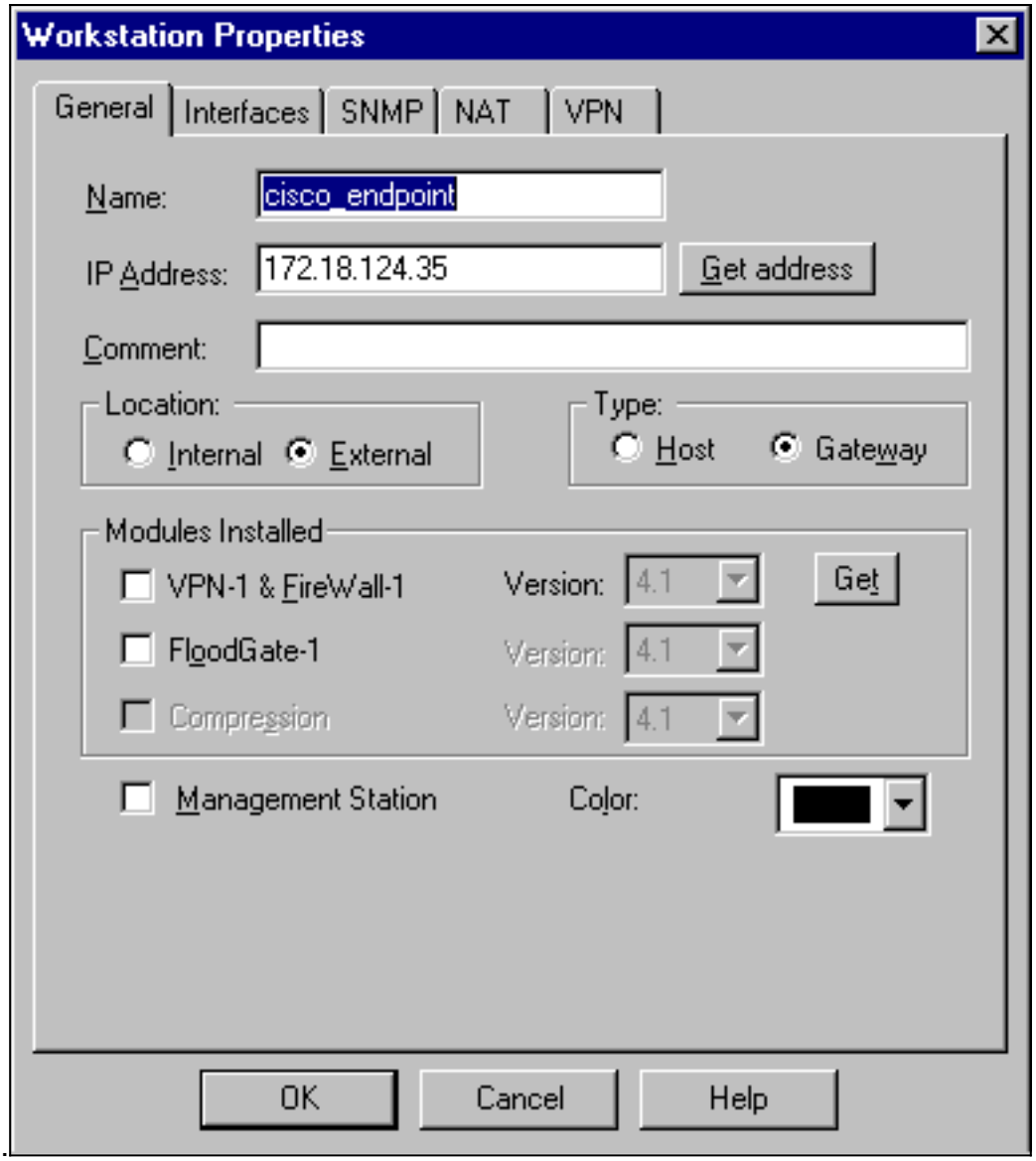
gerenciamento:

4. Selecione **Gerenciar > Objetos de rede > Novo > Rede** para configurar o objeto para a rede externa ("inside_cisco") atrás do PIX.Isso deve concordar com a rede de origem (primeira) neste comando PIX: **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**

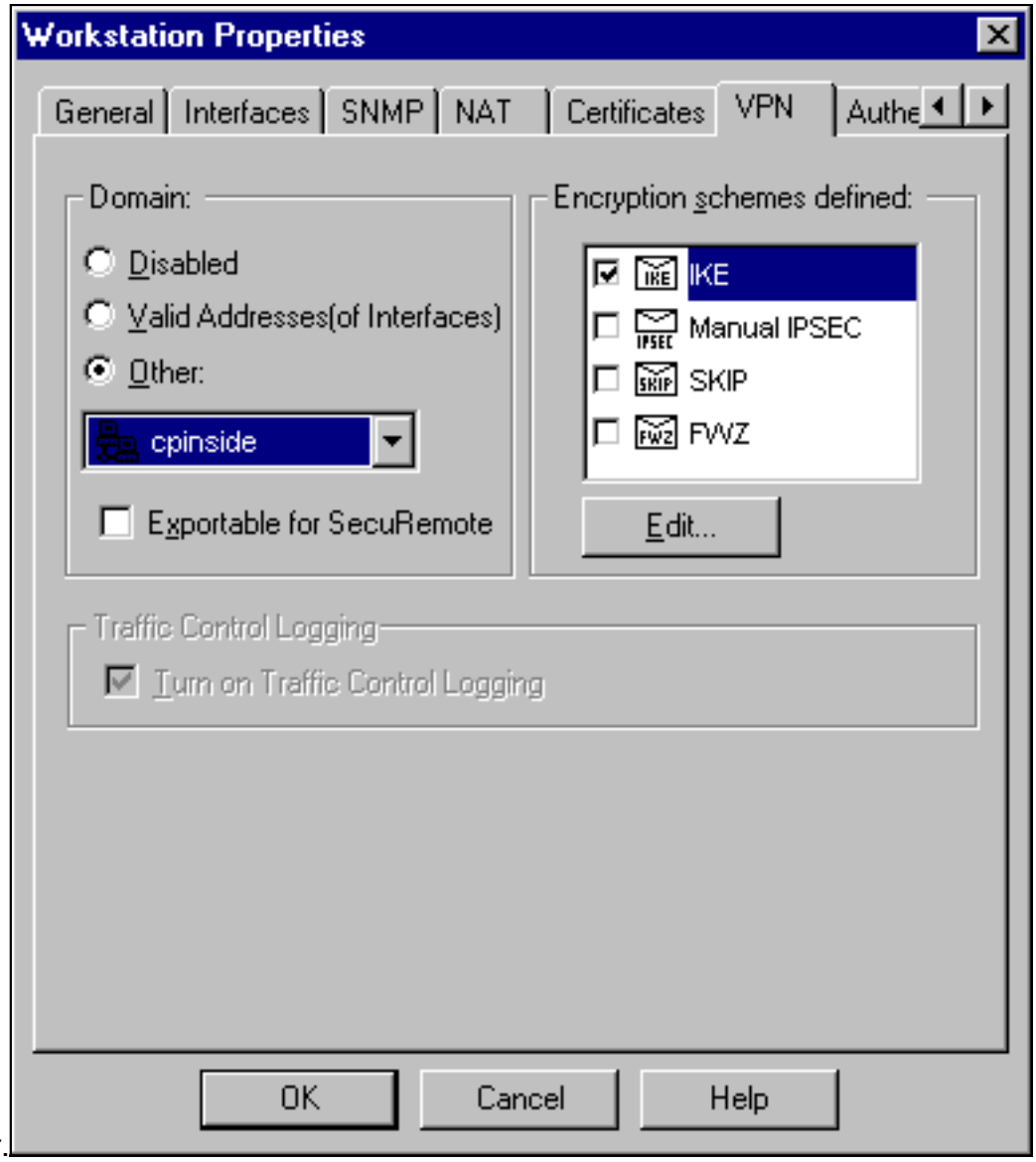


255.255.255.0

5. Selecione Manage (Gerenciar) > Network objects (Objetos de rede) > New (Novo) > Workstation (Estação de Trabalho) para adicionar um objeto referente ao gateway de PIX interno ("cisco_endpoint") . Esta é a interface PIX à qual este comando é aplicado: **crypto map *name* interface externa**Em Local, selecione Externo. Para Tipo, selecione Gateway.**Observação:** não marque a caixa de seleção VPN-1/FireWall-

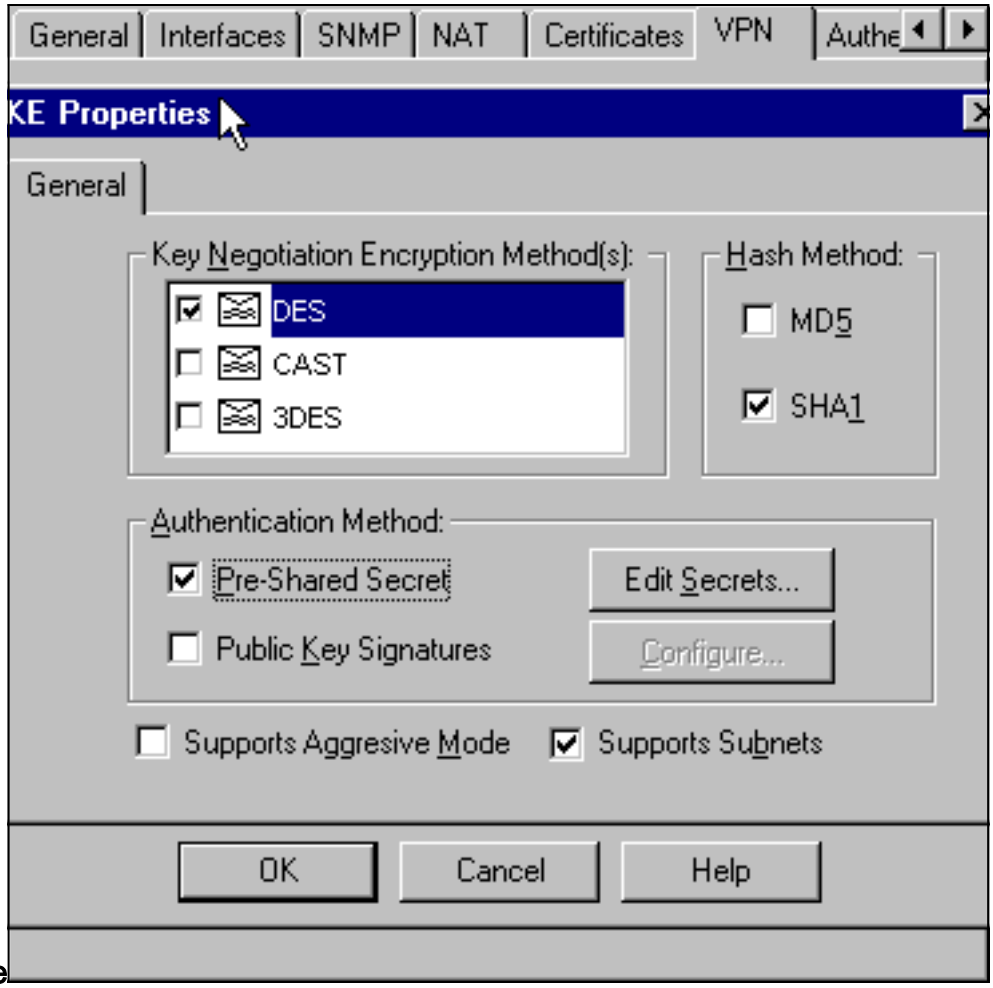
1. 

6. Selecionar Manage > Network objetct > Edit para editar o ponto final do gateway do ponto de controle (chamado "RTPCPVPN") na guia VPN. Em Domain, selecione Other e, em seguida, selecione o lado interno da rede de ponto de controle (chamado “cpinside”) a partir da lista suspensa. Sob esquemas de criptografia definidos, selecione IKE e clique em



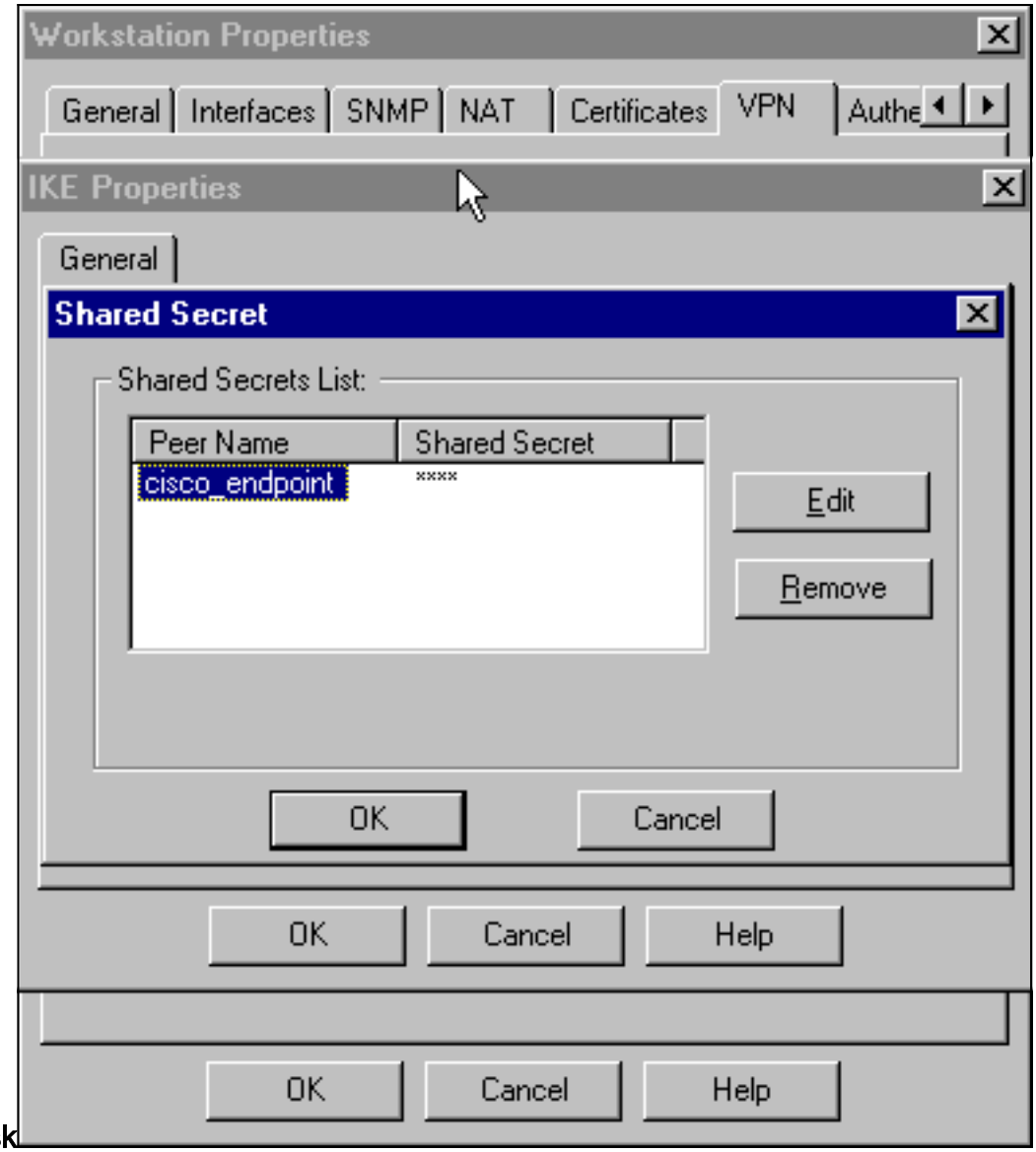
Editar.

7. Altere as propriedades IKE da criptografia DES para concordar com este comando:**isakmp policy # encryption des**
8. Altere as propriedades de IKE para hashing SHA1 para concordar com este comando:**isakmp policy # hash sha**Altere estas configurações:Desative o Modo assertivo.Marque a caixa de seleção **Suporta Sub-Redes**.Em Authentication Method (Método de autenticação), marque a caixa de seleção **Pre-Shared Secret**. Isso concorda com este comando:**isakmp policy # authentication pre-**



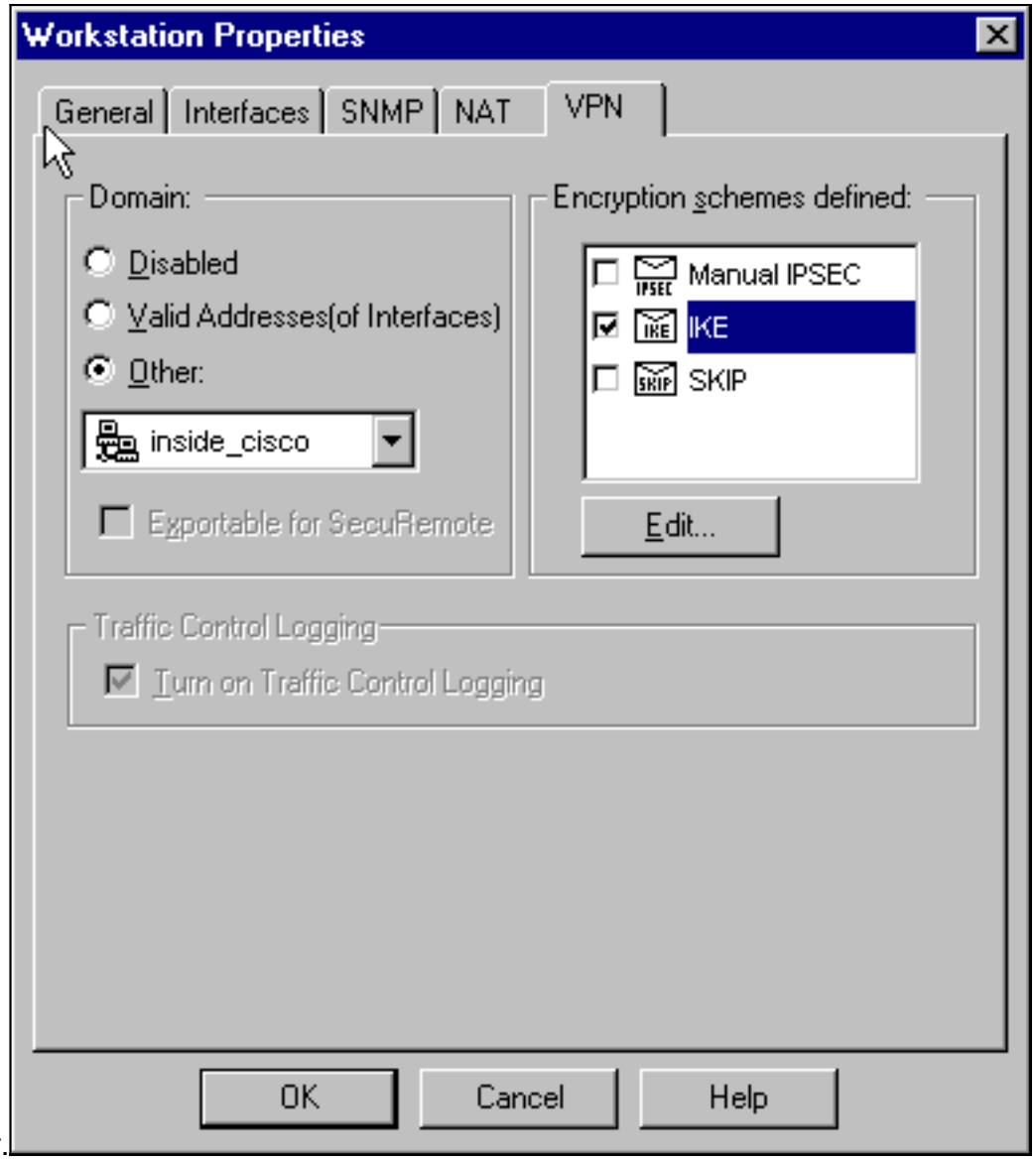
share

9. Clique em **Editar segredos** para definir a chave pré-compartilhada para concordar com o comando PIX:**isakmp key key address address netmask**



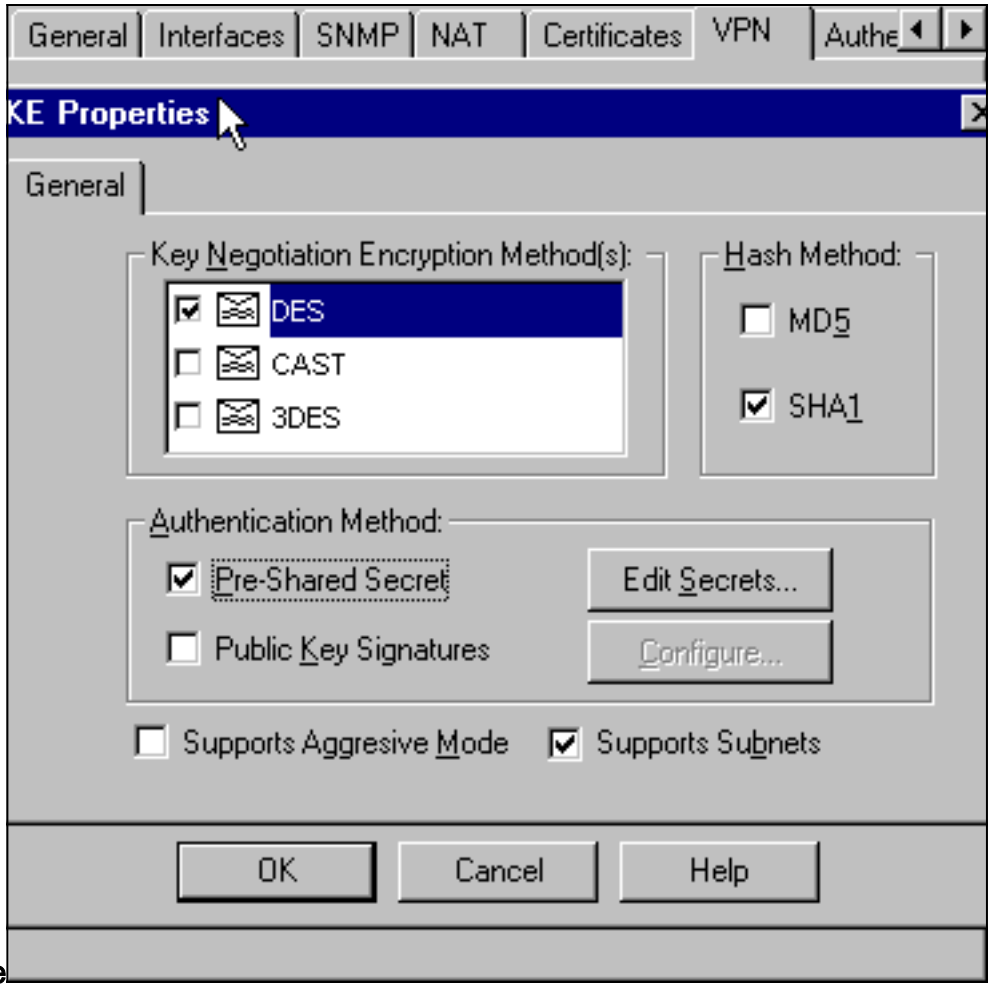
netmask

10. Selecione Gerenciar > Objetos de rede > Editar para editar a guia VPN “cisco_endpoint”. Em Domain (Domínio), selecione Other (Outro) e escolha a parte inteira da rede PIX (chamado de "inside_cisco"). Sob esquemas de criptografia definidos, selecione IKE e



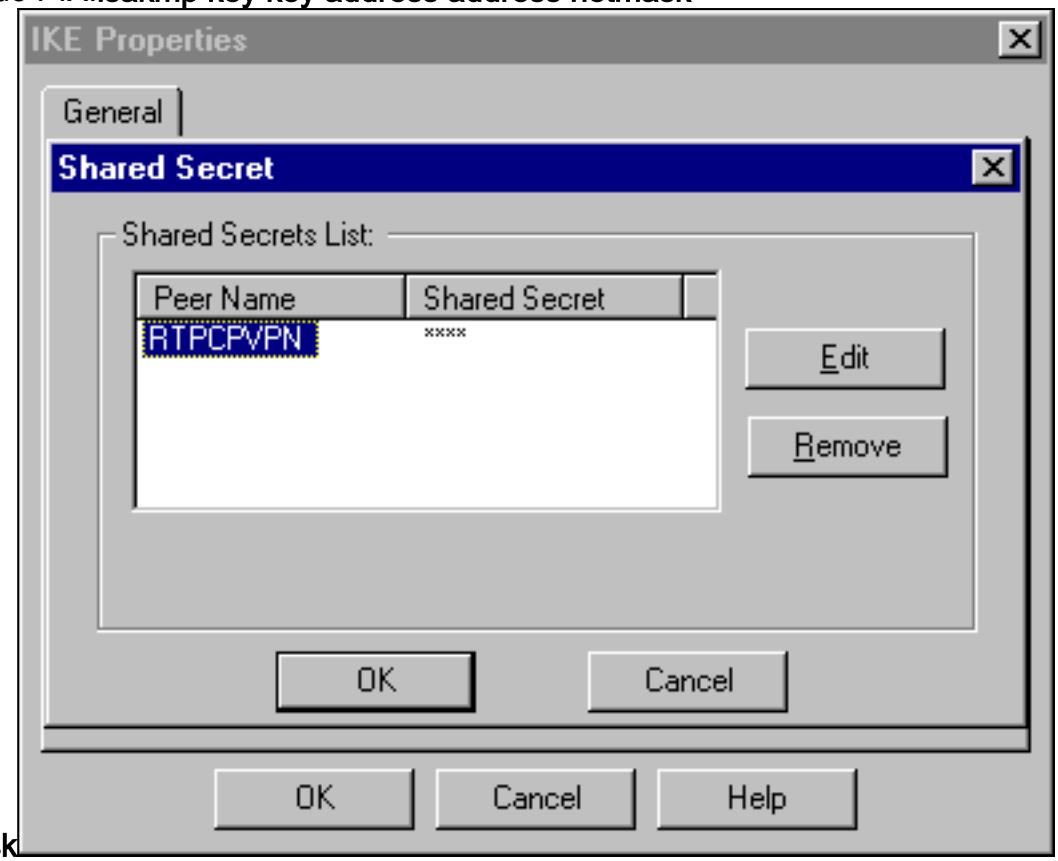
clique em Editar.

11. Altere a criptografia DES das propriedades IKE para concordar com este comando:**isakmp policy # encryption des**
12. Altere as propriedades de IKE para hashing SHA1 para concordar com este comando:**crypto isakmp policy # hash sha**Altere estas configurações:Desative o Modo assertivo.Marque a caixa de seleção **Suporta Sub-Redes**.Em Authentication Method, marque a caixa de seleção **Pre-Shared Secret**. Esta ação concorda com este comando:**isakmp policy # authentication pre-**



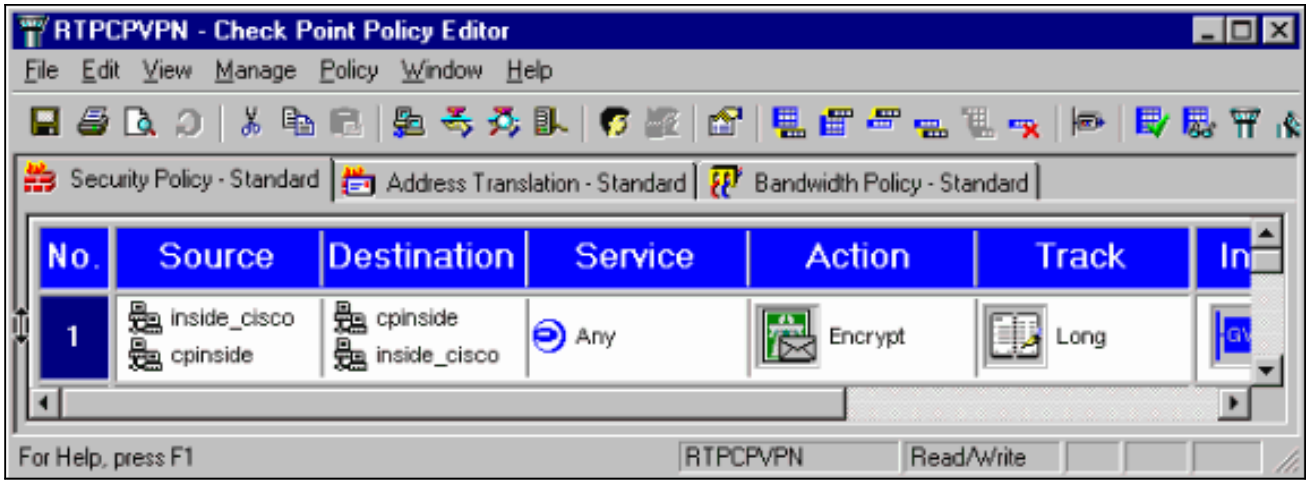
share

13. Clique em **Editar segredos** para definir a chave pré-compartilhada para concordar com este comando PIX:**isakmp key key address address netmask**

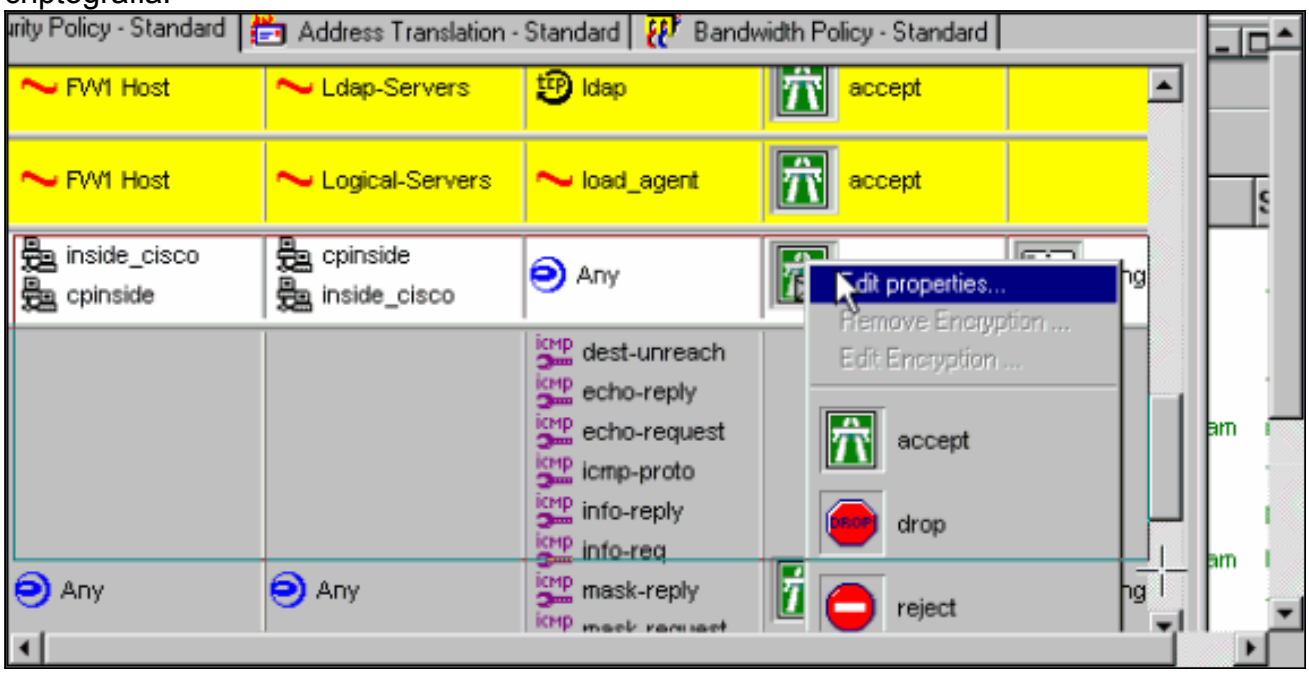


netmask

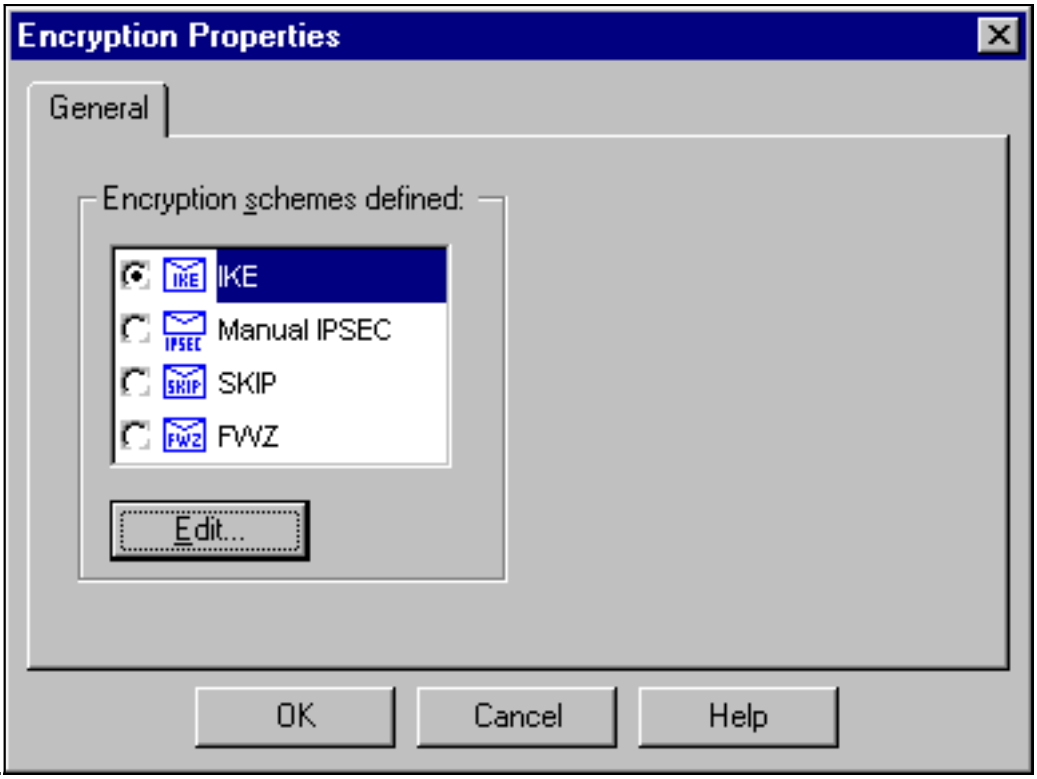
14. Na janela Policy Editor, insira uma regra com Source e Destination como "inside_cisco" e "cpinside" (bidirecional). Ajustar Serviço=Qualquer, Ação=Criptografar e Rastreio=Longo.



15. No título Ação, clique no ícone **Criptografar** verde e selecione **Editar propriedades** para configurar políticas de criptografia.

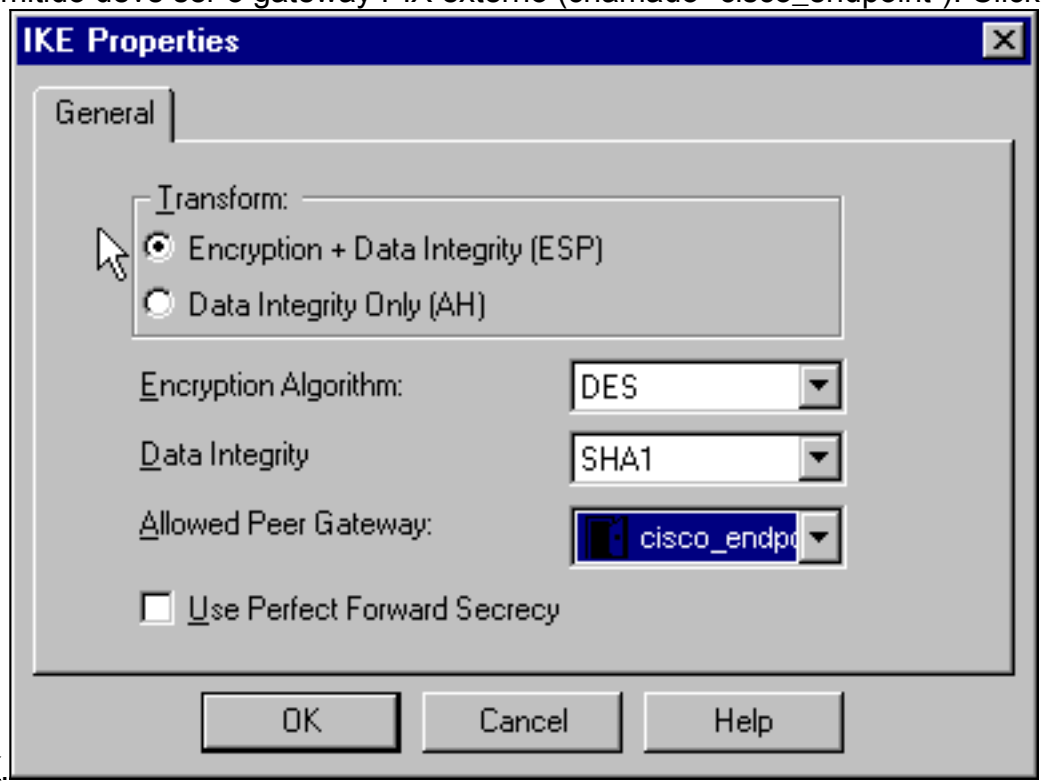


16. Selecione IKE e, em seguida, clique em



Editar.

17. Na tela Propriedades de IKE, altere essas propriedades para concordar com as transformações de PIX IPSec neste comando:**crypto ipsec transform-set myset esp-des esp-sha-hmac**Em Transform, selecione Encryption + Data Integrity (ESP). O algoritmo de criptografia deve ser **DES**, a integridade dos dados deve ser **SHA1**, e o gateway de peer permitido deve ser o gateway PIX externo (chamado "cisco_endpoint"). Click



OK.

18. Depois que o ponto de verificação estiver configurado, selecione **Policy** > **Install** no menu Checkpoint para que as alterações entrem em vigor.

Comandos show, debug e clear

Esta seção fornece informações que você pode usar para confirmar se sua configuração está

funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Antes de emitir comandos de depuração, consulte Informações importantes sobre Comandos de Depuração.

Cisco PIX Firewall

- **debug crypto engine** —Exibe mensagens de depuração sobre mecanismos de criptografia, que executam criptografia e descriptografia.
- **debug crypto isakmp** — Exibe mensagens sobre eventos IKE.
- **debug crypto ipsec—Exibe eventos IPSec.**
- **show crypto isakmp sa** — Exibir todas as associações de segurança (SAs) IKE atuais em um peer.
- **show crypto ipsec sa** — Exibir as configurações usadas pelas associações de segurança atuais.
- **clear crypto isakmp sa** —(do modo de configuração) Apague todas as conexões IKE ativas.
- **clear crypto ipsec sa** —(do modo de configuração) Exclua todas as associações de segurança IPSec.

Ponto de controle:

Como o Rastreamento foi definido como Longo na janela Editor de políticas mostrada na etapa 14, o tráfego negado aparece em vermelho no Visualizador de registros. Uma depuração mais detalhada pode ser obtida inserindo:

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

e em outra janela:

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

Observação: esta foi uma instalação do Microsoft Windows NT.

Você pode limpar SAs no ponto de verificação com estes comandos:

```
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
```

e respondendo **sim** na janela Tem certeza? prompt.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Sumarização de rede

Quando várias redes internas adjacentes são configuradas no domínio de criptografia no ponto de verificação, o dispositivo pode resumi-las automaticamente em relação ao tráfego interessante. Se a ACL de criptografia no PIX não estiver configurada para corresponder, o túnel provavelmente falhará. Por exemplo, se as redes internas de 10.0.0.0 /24 e 10.0.1.0 /24 estiverem configuradas para serem incluídas no túnel, elas podem ser resumidas em 10.0.0.0 /23.

Exemplo de saída de depuração do PIX

```
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
```

Informações Relacionadas

- Página de suporte do PIX
- Referências de comando PIX
- Solicitações de Comentários (RFCs)
- Configuração da segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- PIX 5.2: Configurando IPSec
- PIX 5.3: Configurando IPSec
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems