IPSec トンネル設定 - Cisco Secure PIX Firewall を Checkpoint 4.1 へ

内容

概要

この設定例は、事前共有キーを使用する IPSec トンネルを 2 つのプライベート ネットワークに参加するように構成する方法を示しています。この例で参加するネットワークは、Cisco Secure Pix Firewall（PIX）内部の 192.168.1.X プライベート ネットワークと Checkpoint 内部の 10.32.50.X プライベート ネットワークです。ここでは、この設定を始める前に、PIX 内部および Checkpoint 4.1 Firewall 内部からインターネットへのトラフィック（ここでは 172.18.124.X ネットワークと表現しています）が流れていると仮定しています。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- PIX ソフトウェア リリース 5.3.1
- Checkpoint 4.1 Firewall

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

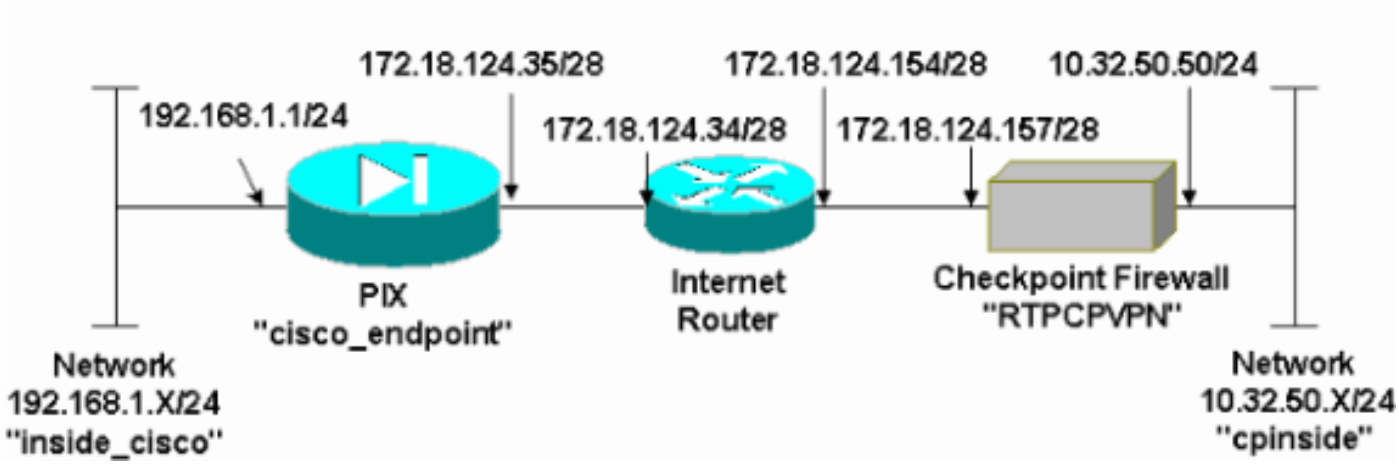
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

ネットワーク図

このドキュメントでは、次の図に示すネットワーク設定を使用します。



設定

このドキュメントでは、このセクションで示す設定を使用しています。

PIX の設定

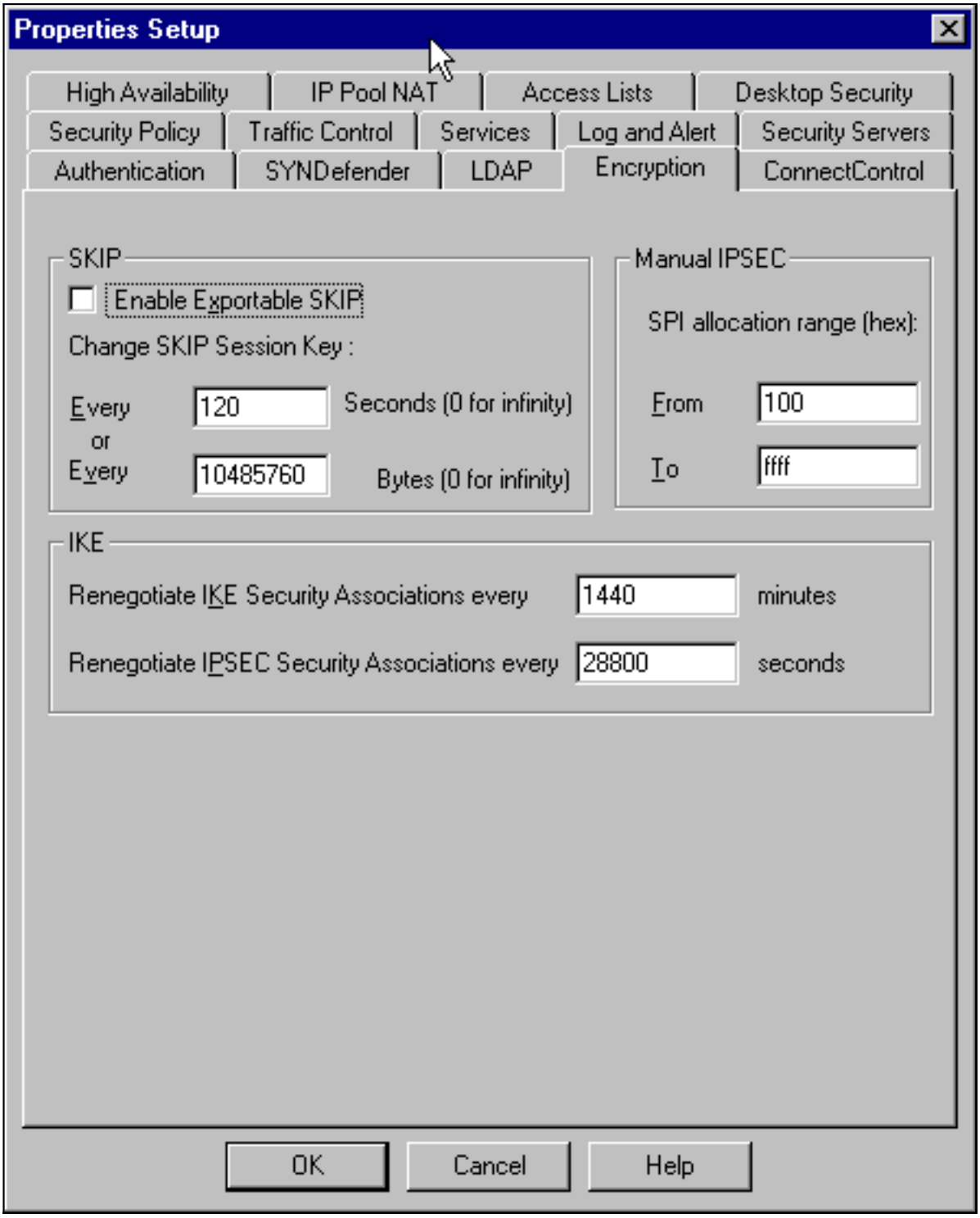
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
```

```
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
```

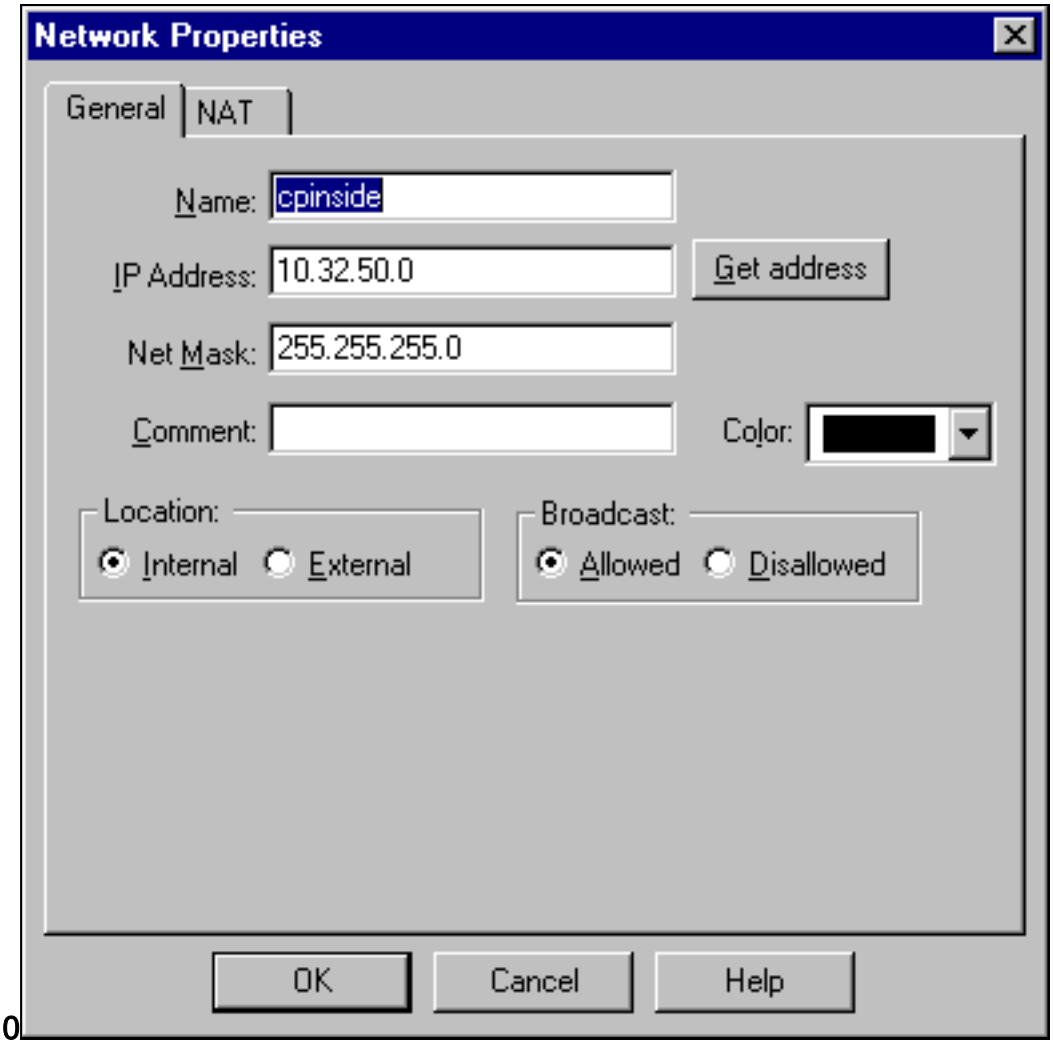
```
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

Checkpoint Firewall

1. IKE と IPSec のデフォルトのライフタイムは各ベンダーによって異なるため、 Properties > Encryption を選択して、Checkpoint のライフタイムを PIX のデフォルトと一致するように設定します。PIXのデフォルトのIKEライフタイムは86400秒（1440分）ですが、次のコマンドで変更できます。**isakmp policy # lifetime 86400**PIX IKEライフタイムは60 ~ 86400秒の間で設定できます。PIXのデフォルトのIPSecライフタイムは28800秒ですが、次のコマンドで変更できます。**crypto ipsec security-association lifetime seconds #**PIX IPSecライフタイムは120 ~ 86400秒の間で設定できます。

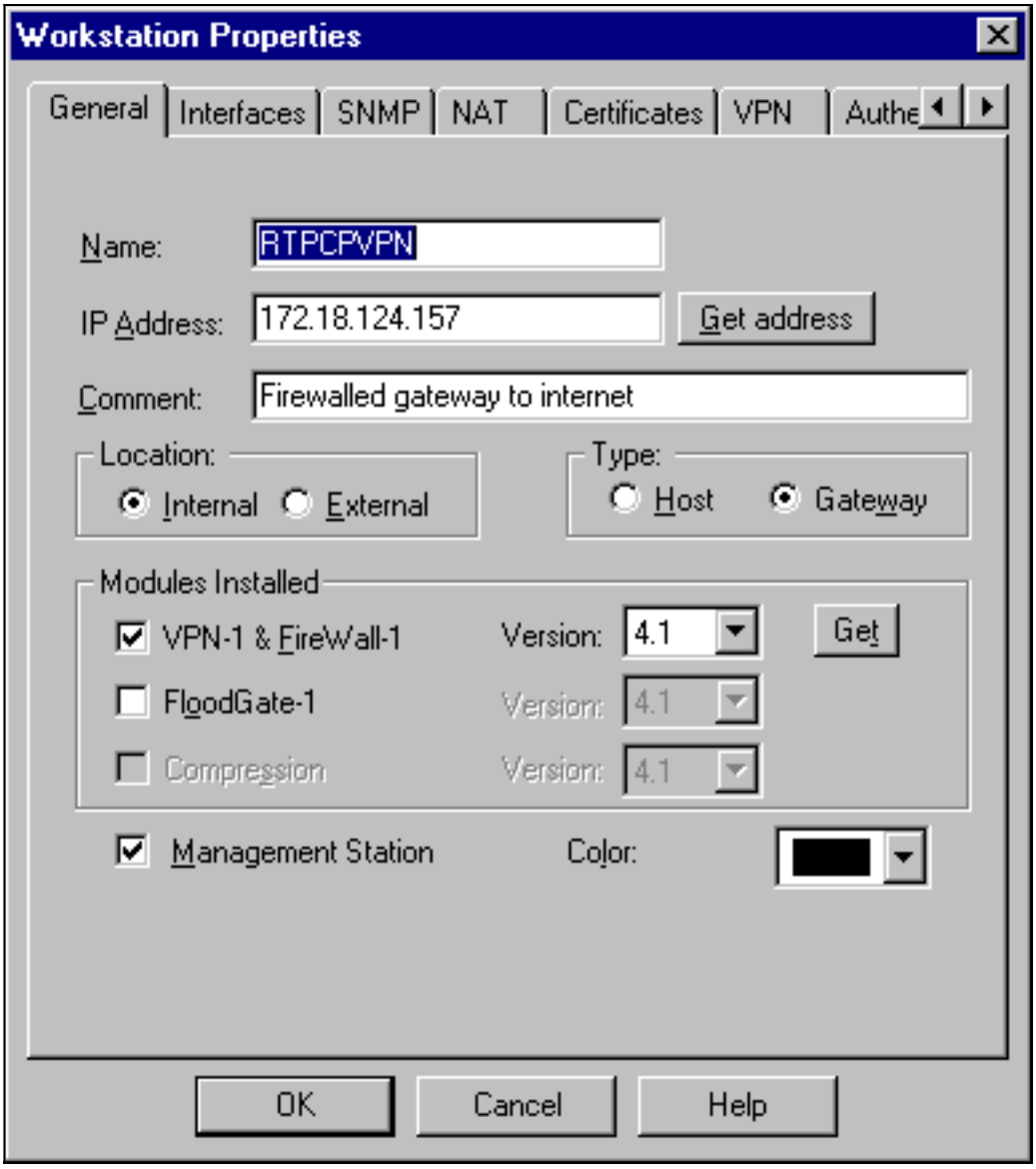


2. [Manage] > [Network objects] > [New]（または [Edit]）> [Network] の順に選択し、Checkpoint の背後にある内部（「cpinside」）ネットワークのオブジェクトを設定します。これは、このPIXコマンドの宛先（2番目の）ネットワークと一致している必要があります。
access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0

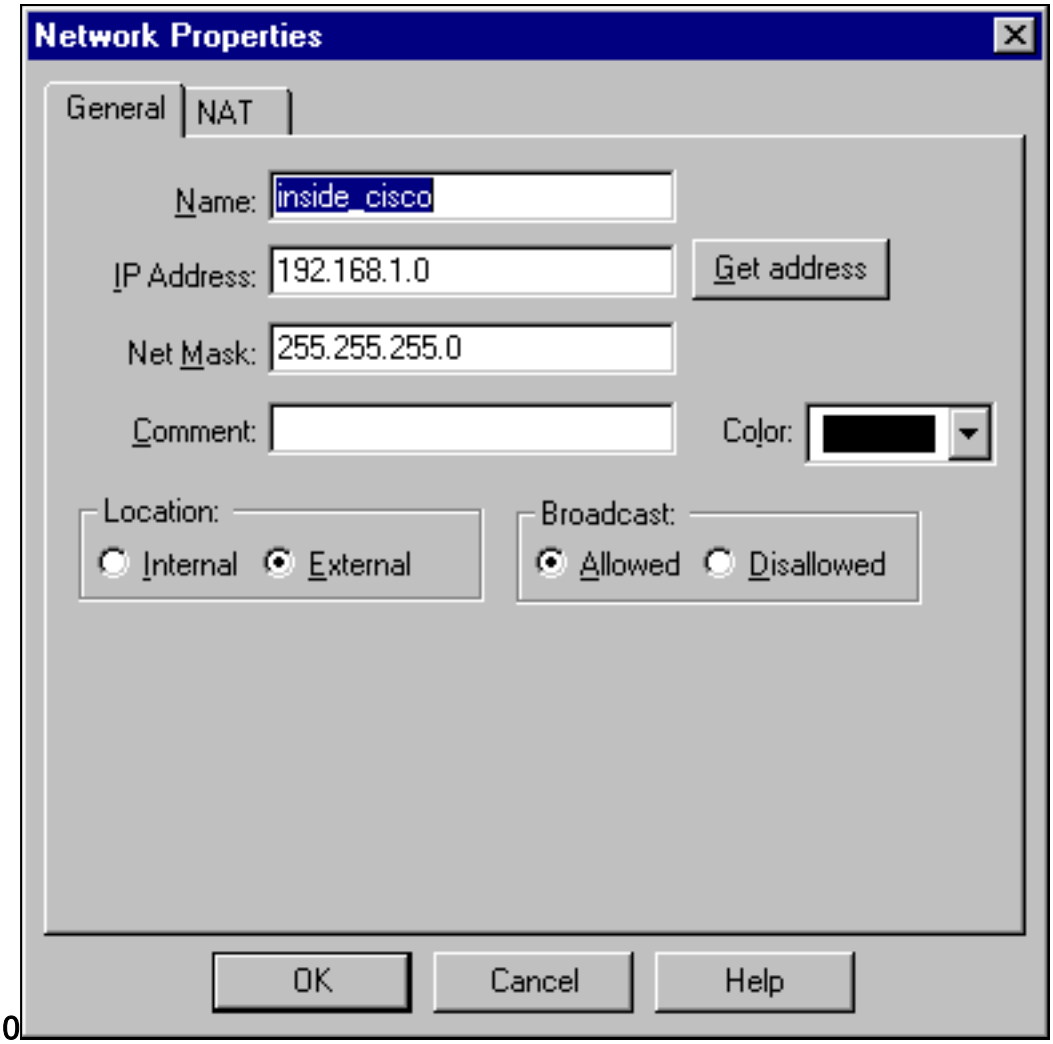


255.255.255.0

3. [Manage] > [Network objects] > [Edit] を選択し、PIXがこのコマンドでポイントしているゲートウェイ（「RTPCPVPN」チェックポイント）エンドポイントのオブジェクトを編集します。**crypto map name # set peer ip_address**Location の下で Internal を選択します。Type で Gateway を選択します。[Modules Installed]で、[**VPN-1 & FireWall-1**]チェックボ**ックスを選択**し、[**Management Station**]チェックボックス**をオン**にします。

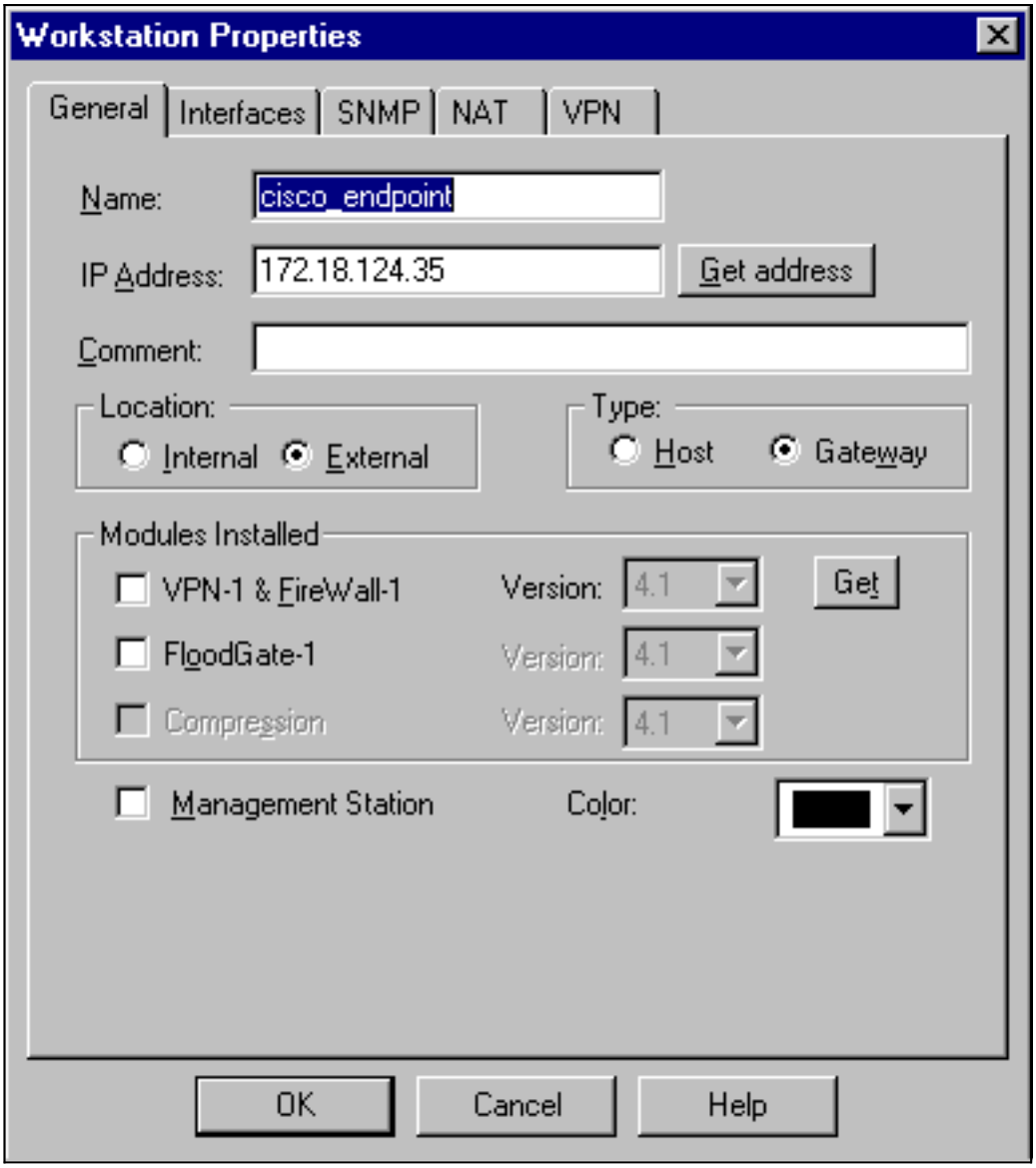


4. Manage > Network objects > New > Network の順に選択し、PIX の背後にある外部（「inside_cisco」）ネットワークのオブジェクトを設定します。これは、このPIXコマンドの送信元（最初）ネットワークと一致している必要があります。**access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**

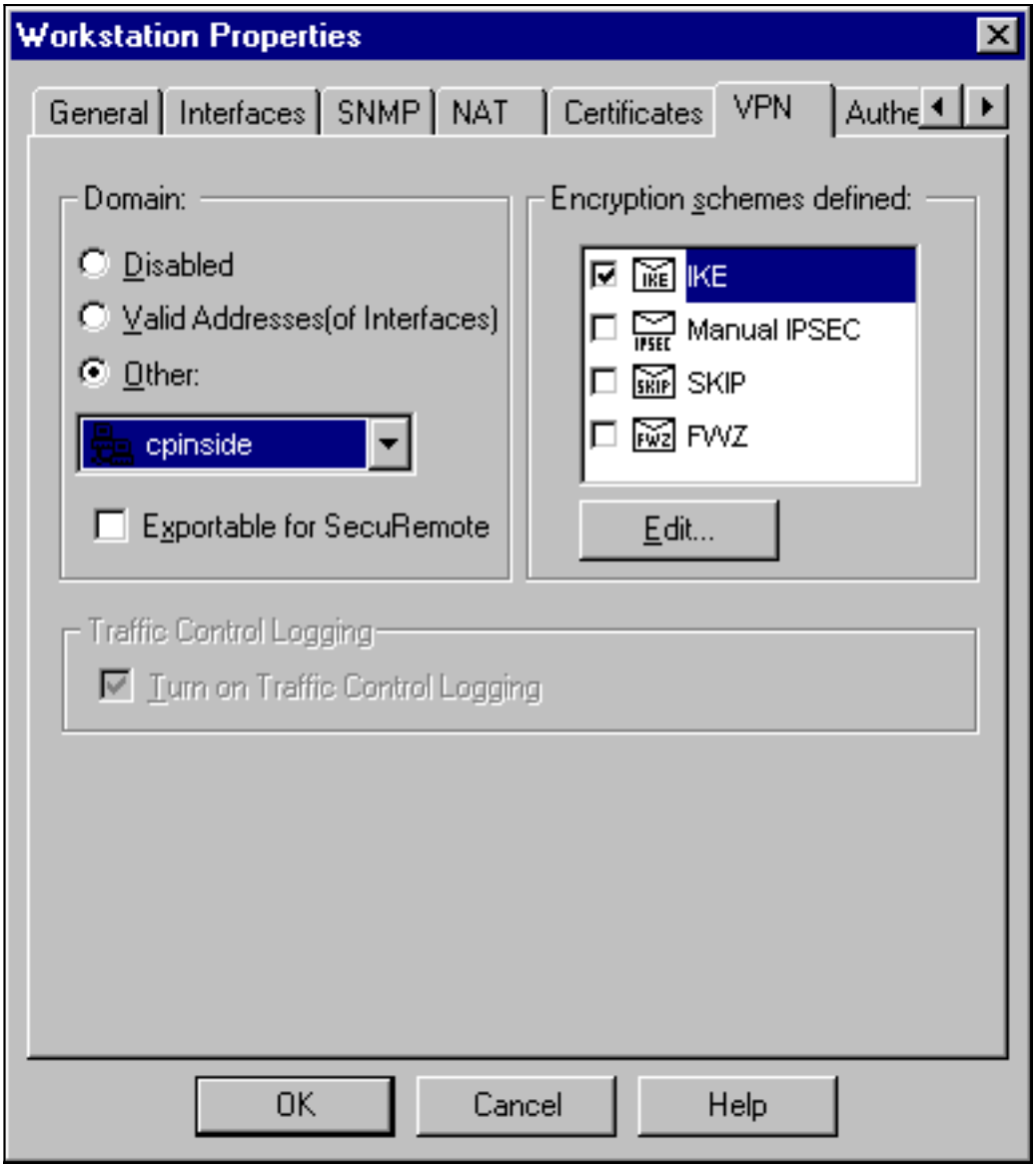


255.255.255.0

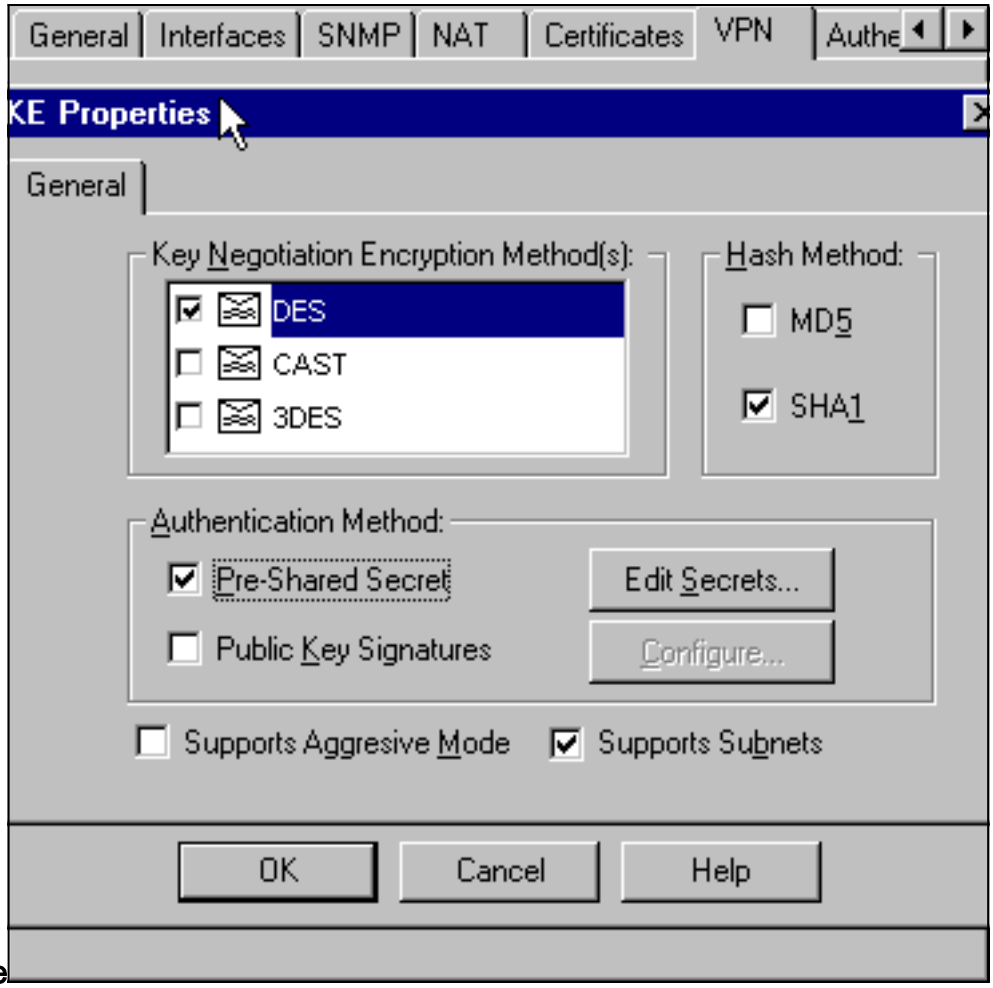
5. Manage > Network objects > New > Workstation の順に選択し、外部 (「cisco_endpoint」) PIX ゲートウェイのオブジェクトを追加します。このコマンドが適用されるPIXインターフェイスを次に示します。**crypto map name interface outside**Location の下で External を選択します。Type で Gateway を選択します。**注：**[VPN-1/FireWall-1]チェックボックスは選択しないでください。



6. [Manage] > [Network objects] > [Edit] の順に選択し、Checkpoint ゲートウェイ エンドポイント（「RTPCPVPN」という名前）の [VPN] タブを編集します。[Domain] の下で、[Other] を選択してから、Checkpoint ネットワークの内側（「cpinside」という名前）をドロップダウン リストから選択します。[Encryption schemes defined] の下で、[IKE] を選択してから [Edit] をクリックします。

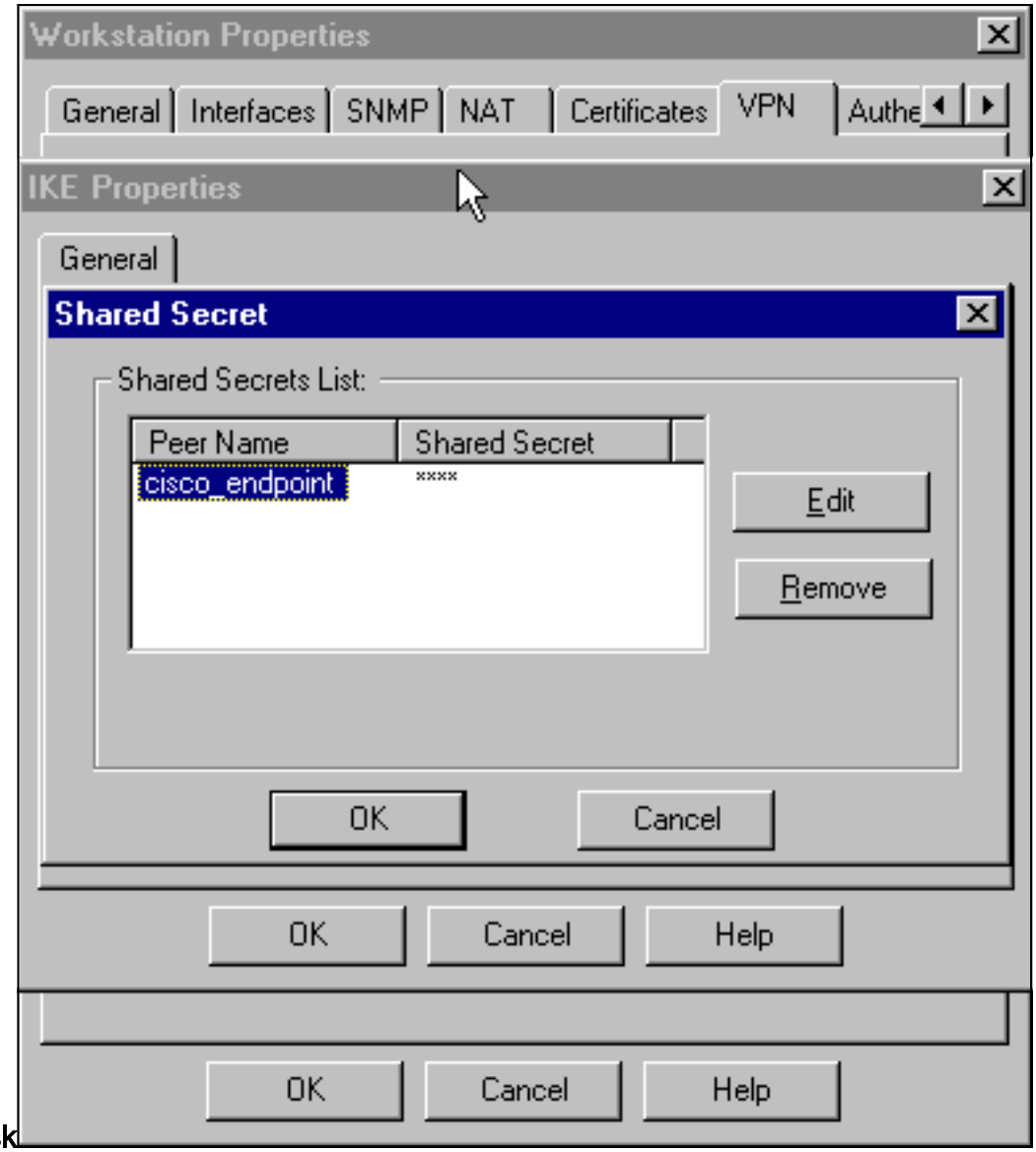


7. DES暗号化のIKEプロパティを次のコマンドに一致するように変更します。**isakmp policy # encryption des**
8. 次のコマンドに一致するように、IKEプロパティをSHA1ハッシュに変更します。**isakmp policy # hash sha**次の設定を変更します。[Aggressive Mode] をオフにします。[サブネットをサポート]チェックボックスをオンにします。[Authentication Method]で、[Pre-Shared Secret]チェックボックスをオンにします。これは、次のコマンドと一致します。**isakmp policy # authentication pre-**



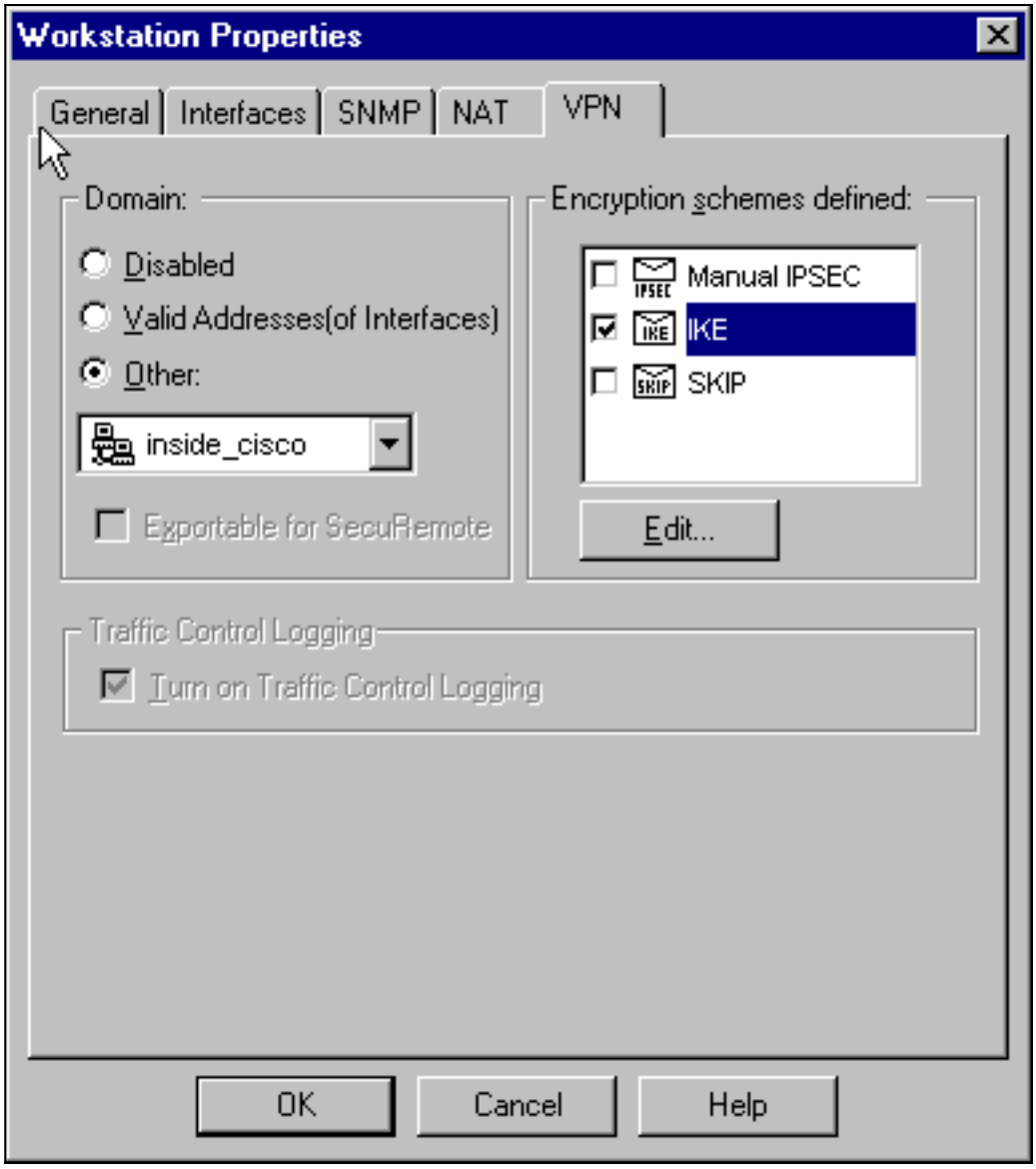
share

9. [Edit Secrets] をクリックして、事前共有キーをPIXコマンドと一致するように設定します。**isakmp key key address address netmask**

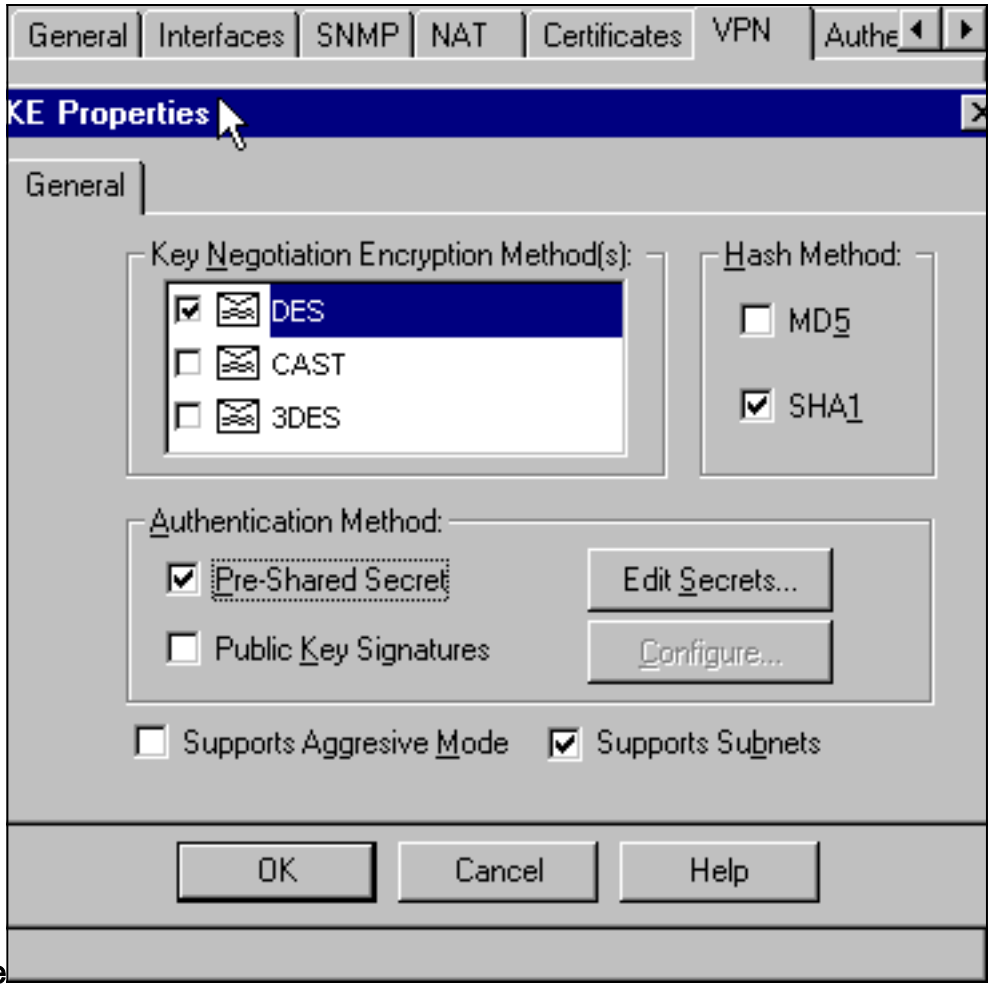


netmask

10. [Manage] > [Network objects] > [Edit] の順に選択し、「cisco_endpoint」の [VPN] タブを編集します。Domain の下で、Other を選択してから PIX ネットワークの内側（「inside_cisco」という名前）を選択します。 [Encryption schemes defined] の下で、[IKE] を選択してから [Edit] をクリックします。

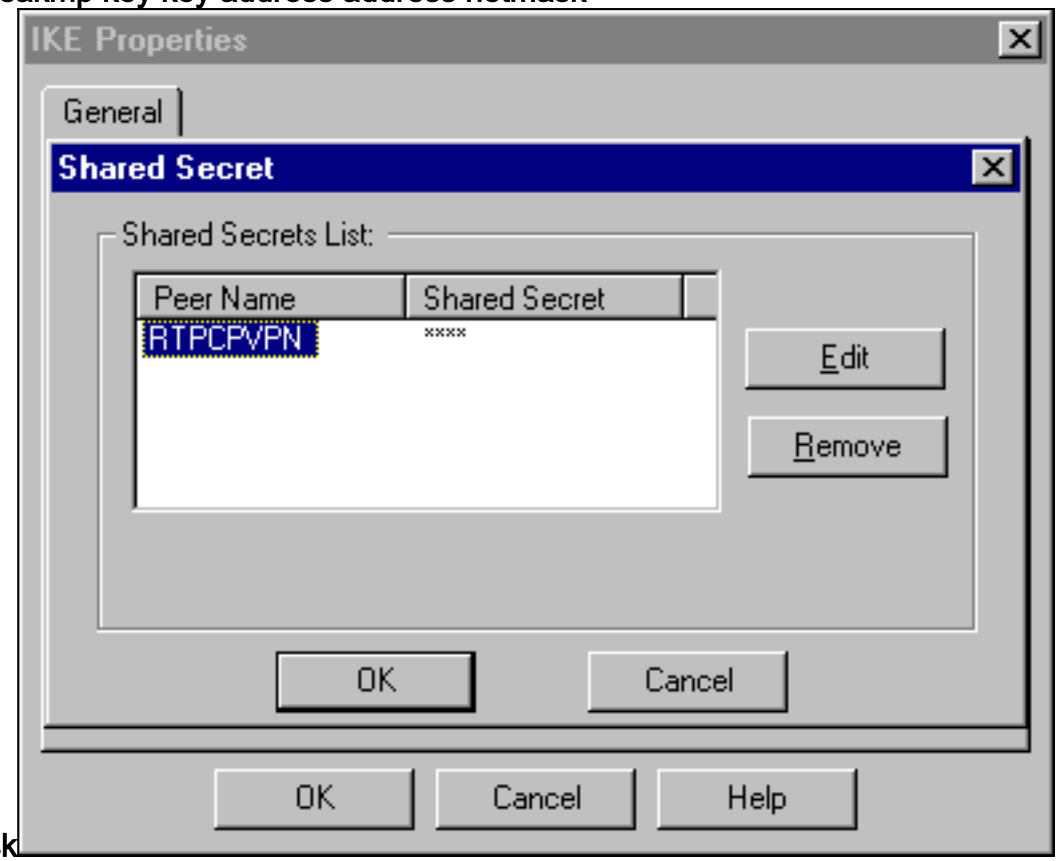


11. IKEプロパティDES暗号化を次のコマンドと一致するように変更します。**isakmp policy # encryption des**
12. 次のコマンドに一致するように、IKEプロパティをSHA1ハッシュに変更します。**crypto isakmp policy # hash sha**次の設定を変更します。[Aggressive Mode] をオフにします。[サブネットをサポート]チェックボックスをオンにします。[Authentication Method]で、[Pre-Shared Secret]チェックボックスをオンにします。この操作は、次のコマンドと一致します。**isakmp policy # authentication pre-**



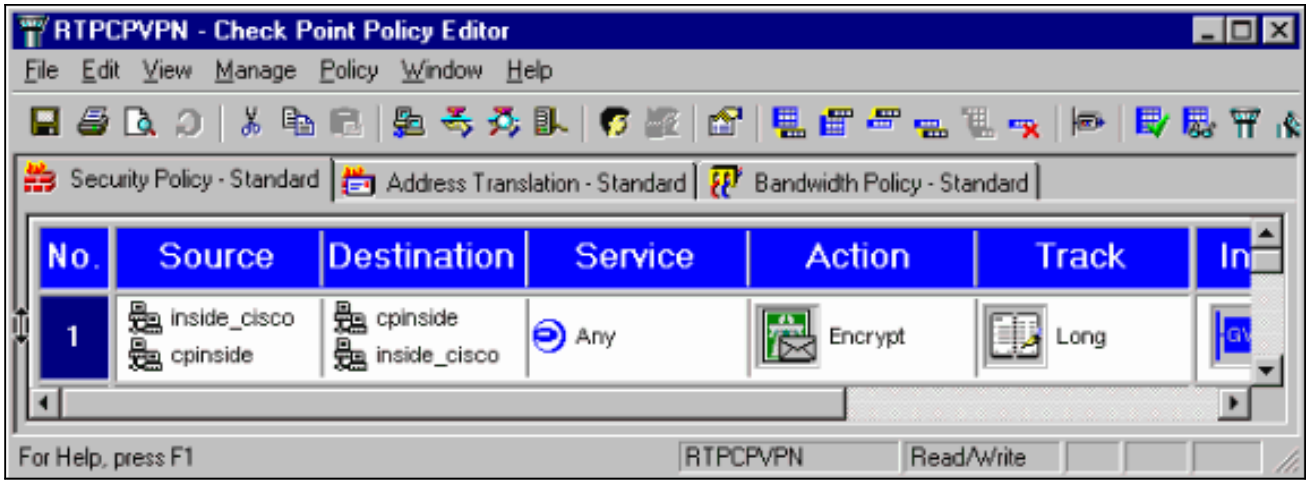
share

13. [Edit Secrets] をクリックして、事前共有キーを次のPIXコマンドと一致するように設定します。**isakmp key key address address netmask**

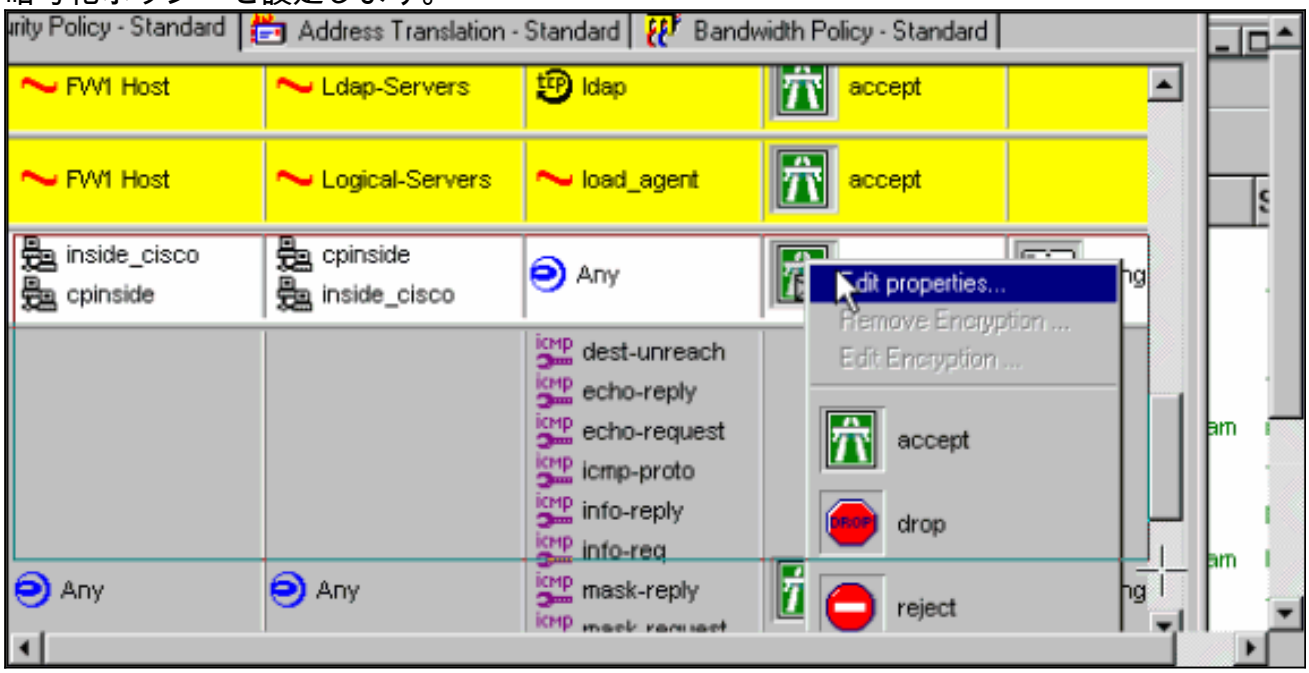


netmask

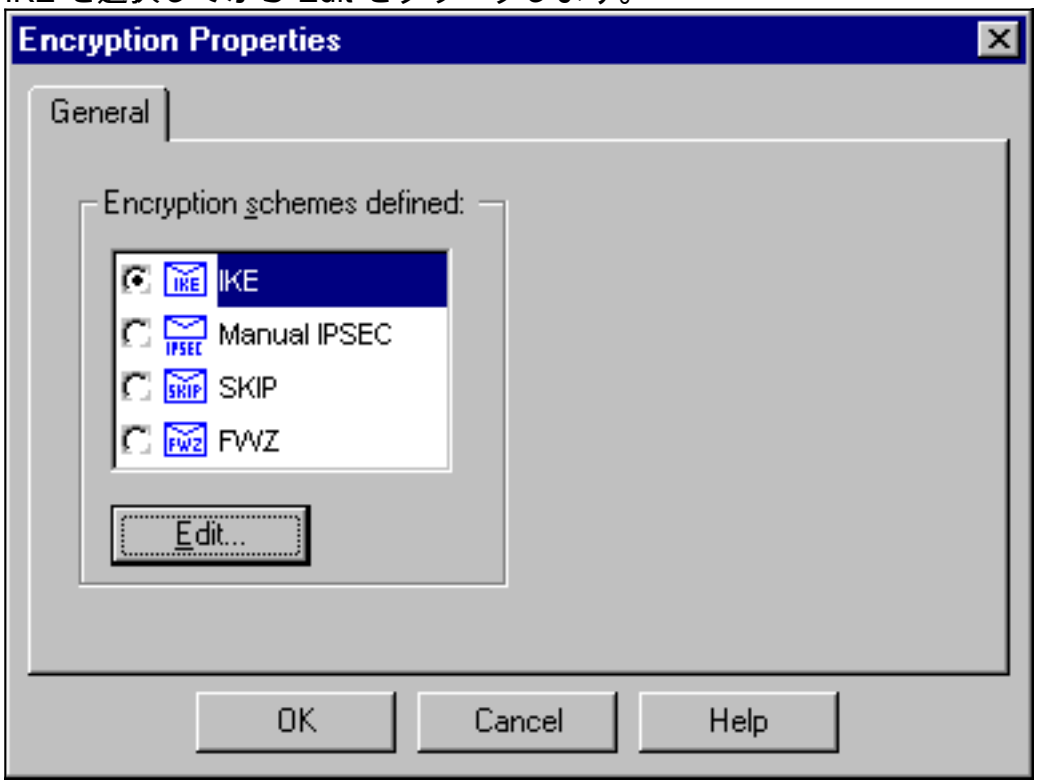
14. [Policy Editor] ウィンドウで、Source と Destination の両方に「inside_cisco」と「cpinside」（双方向）を設定したルールを挿入します。 **Service=Any**、**Action=Encrypt**、および **Track=Long** を設定します。



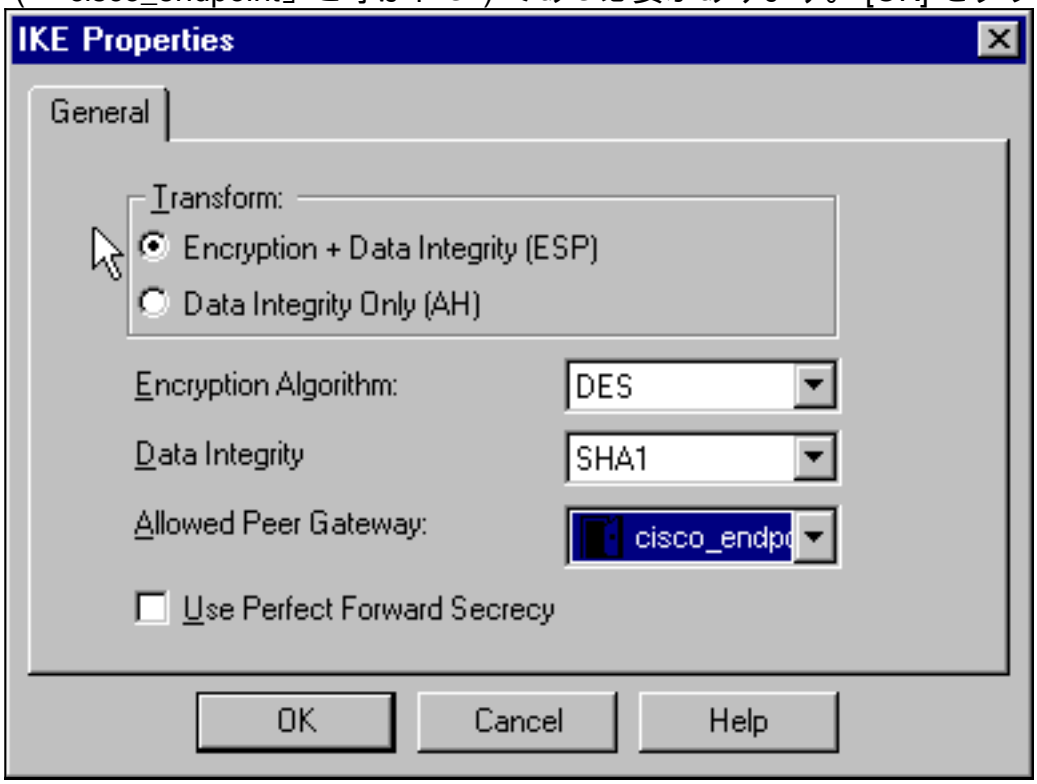
15. [Action] 見出しの下で、緑の [Encrypt] アイコンをクリックし、[Edit properties] を選択して暗号化ポリシーを設定します。



16. IKE を選択してから Edit をクリックします。



17. [IKE Properties]画面で、次のコマンドのPIX IPSecトランスフォームと一致するように、これらのプロパティを変更します。**crypto ipsec transform-set myset esp-des esp-sha-hmac**[Transform] の [Encryption + Data Integrity (ESP)] を選択します。 暗号化アルゴリズムは**DES**、データ整合性は**SHA1**、許可されたピアゲートウェイは外部PIXゲートウェイ（「cisco_endpoint」と呼ばれる）である必要があります。 [OK] をクリックします。



18. Checkpointを設定した後、変更を有効にするには、Checkpointメニューで**Policy > Install**の順に選択します。

debug、show、および clear コマンド

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

Cisco PIX ファイアウォール

- **debug crypto engine**：暗号化と復号化を実行する暗号化エンジンに関するデバッグメッセージを表示します。
- **debug crypto isakmp**:IKEイベントに関するメッセージを表示します。
- **debug crypto ipsec**:IPSecイベントを表示します。
- **show crypto isakmp sa**：ピアにおける現在のIKE Security Association（SA；セキュリティアソシエーション）をすべて表示します。
- **show crypto ipsec sa**：現在のセキュリティアソシエーションで使用されている設定を表示します。
- **clear crypto isakmp sa**:（コンフィギュレーションモードから）アクティブなIKE接続をすべ

てクリアします。
- **clear crypto ipsec sa**:（コンフィギュレーションモードから）すべてのIPSecセキュリティアソシエーションを削除します。

Checkpoint：

ステップ14に示す[Policy Editor]ウィンドウで[Tracking]が[Long]に設定されているため、拒否されたトラフィックはログビューアに赤色で表示されます。次のように入力すると、より詳細なデバッグを取得できます。

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

さらに、別のウィンドウで次のコマンドを実行します。

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

注：これは Microsoft Windows NTのインストールです。

次のコマンドを使用して、チェックポイント上のSAをクリアできます。

```
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
```

「はい」と答えて間違いありませんか。プロンプトで表示されない場合があります。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ネットワーク集約

複数の隣接する内部ネットワークがチェックポイントの暗号化ドメインに設定されている場合、デバイスは対象トラフィックに関して自動的にそれらを集約できます。PIXの暗号ACLが一致するように設定されていない場合、トンネルは失敗する可能性があります。たとえば、10.0.0.0 /24と10.0.1.0 /24の内部ネットワークがトンネルに含まれるように設定されている場合、それらを10.0.0.0 /23に集約できます。

PIX からの debug の出力例

```
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
```

関連情報

- PIX に関するサポート ページ
- PIX コマンド リファレンス
- Requests for Comments (RFCs)
- IPSec ネットワーク セキュリティの設定
- Internet Key Exchange セキュリティ プロトコルの設定
- PIX 5.2：IPSec の設定
- PIX 5.3：IPSec の設定
- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems