

[Solutions](#) | [Products](#) | [Ordering](#) | [Support](#) | [Partners](#) | [Training](#) | [Corporate](#)
 Sample Configurations

Configuring an IPSec Tunnel - Cisco Secure PIX Firewall to Checkpoint 4.1 Firewall

Contents

[Introduction](#)

[Hardware and Software Versions](#)

[Network Diagram](#)

[Configurations](#)

[Cisco Secure PIX Firewall](#)

[Checkpoint Firewall](#)

[debug and show and clear Commands](#)

[Sample Debug Output](#)

[Related Information](#)

Introduction

This sample configuration demonstrates how to form an IPSec tunnel with pre-shared keys to join 2 private networks. In our example, the joined networks are the 192.168.1.X private network inside the Cisco Secure Pix Firewall (PIX) and the 10.32.50.X private network inside the Checkpoint. We assume that traffic from inside the PIX and inside the Checkpoint 4.1 Firewall to the Internet (represented here by the 172.18.124.X networks) is flowing prior to beginning this configuration.

Hardware and Software Versions

This configuration was developed and tested using the software and hardware versions below.

- PIX Software version 5.3.1
- Checkpoint 4.1 Firewall

Network Diagram

Help us help you.

Please rate this
 et:

- Excellent
 Good
 Average
 Fair
 Poor

his et
 reete:a :ase:

- Yes
 No

estis r
 ireet:

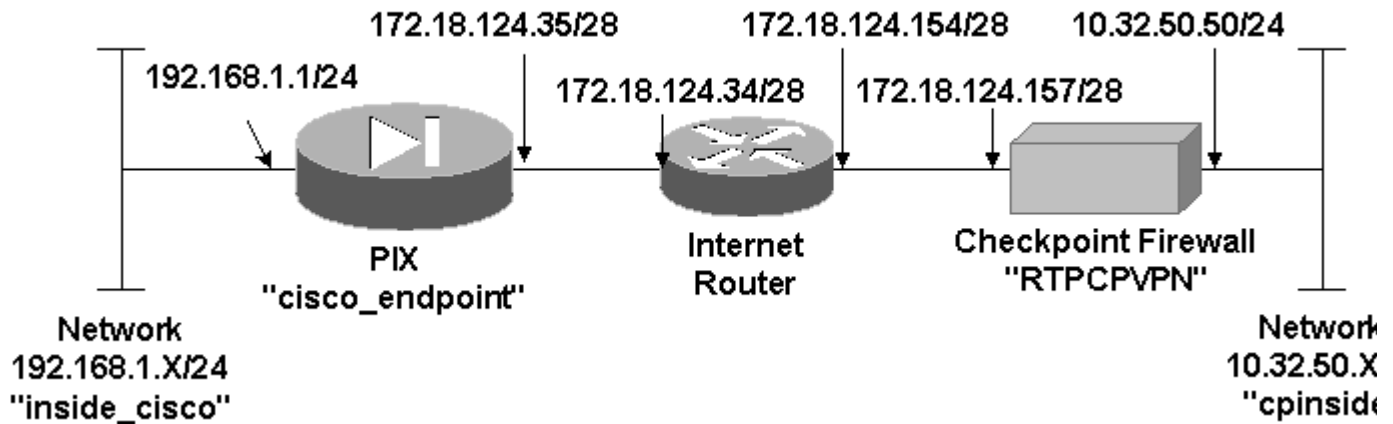
(256 character limit)

tial tat
 irati:

Name:

Email:

Send



Configurations

PIX Configuration

```

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 0:3
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. Since the IKE and IPsec default lifetimes differ between vendors, select **Properties > Encryption** to set the Checkpoint lifetimes to agree with the PIX defaults.

The PIX default IKE lifetime is 86400 seconds (=1440 minutes), modifiable by the following command:

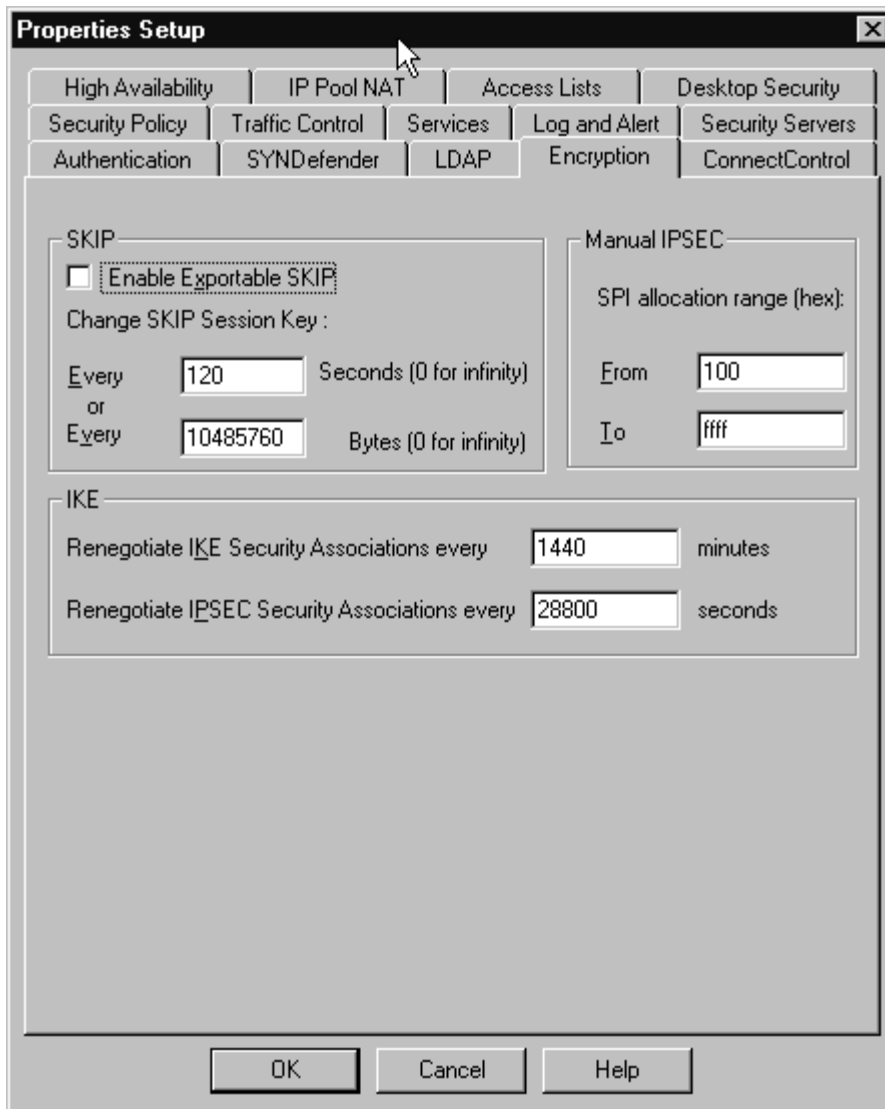
```
isakmp policy # lifetime 86400
```

You can configure a PIX IKE lifetime between 60-86400 seconds.

The PIX default IPsec lifetime is 28800 seconds, modifiable by the following command:

```
crypto ipsec security-association lifetime seconds #
```

You can configure a PIX IPsec lifetime between 120-86400 seconds.



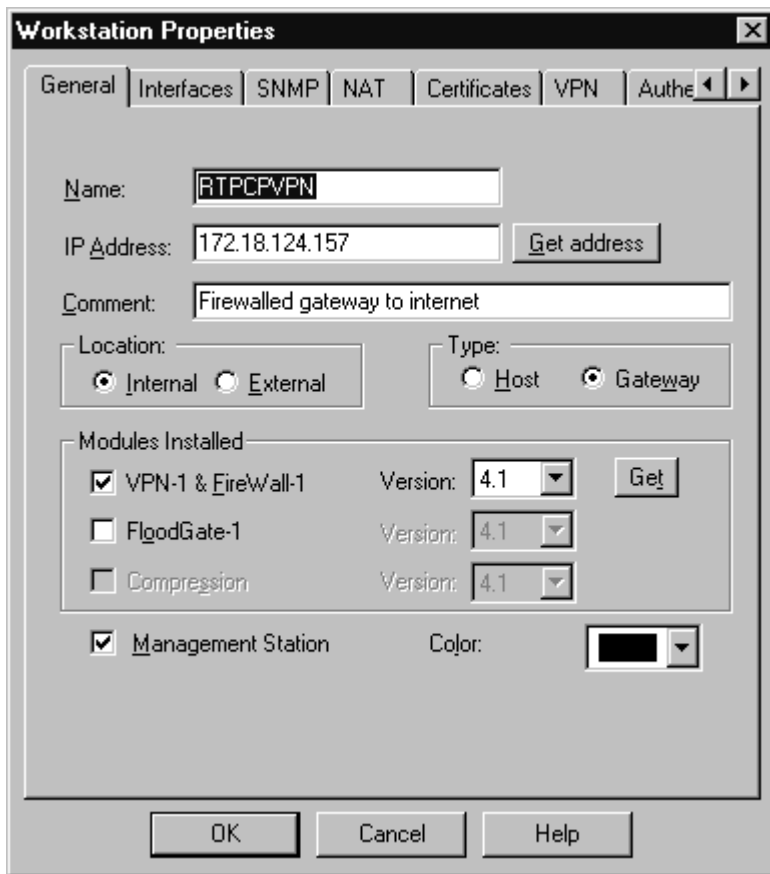
2. Select **Manage > Network objects > New (or Edit) > Network** to configure the object for the internal ("cpinside") network behind the Checkpoint.

This should agree with the destination (second) network in the PIX command:
access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0 255.255.255.0

The screenshot shows a 'Network Properties' dialog box with a 'NAT' tab selected. The 'Name' field contains 'cpinside'. The 'IP Address' field contains '10.32.50.0' and has a 'Get address' button next to it. The 'Net Mask' field contains '255.255.255.0'. There is an empty 'Comment' field and a 'Color' dropdown menu set to black. Below these fields are two groups of radio buttons: 'Location' with 'Internal' selected and 'External' unselected; and 'Broadcast' with 'Allowed' selected and 'Disallowed' unselected. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

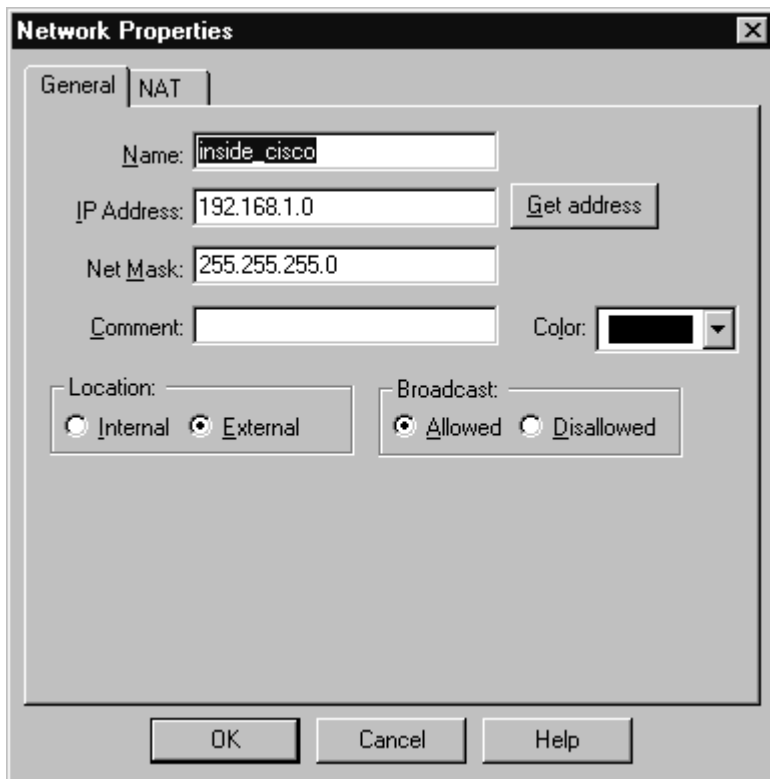
3. Select **Manage > Network objects > Edit** to edit the object for the gateway ("RTPCPVPN" Checkpoint) endpoint that the PIX points to in the following command:
crypto map *name* # set peer *ip_address*

Under Location, select **Internal**. For Type, select **Gateway**. Under Modules Installed, select the **VPN-1 & FireWall-1** check box, and also select the **Management Station** check box:



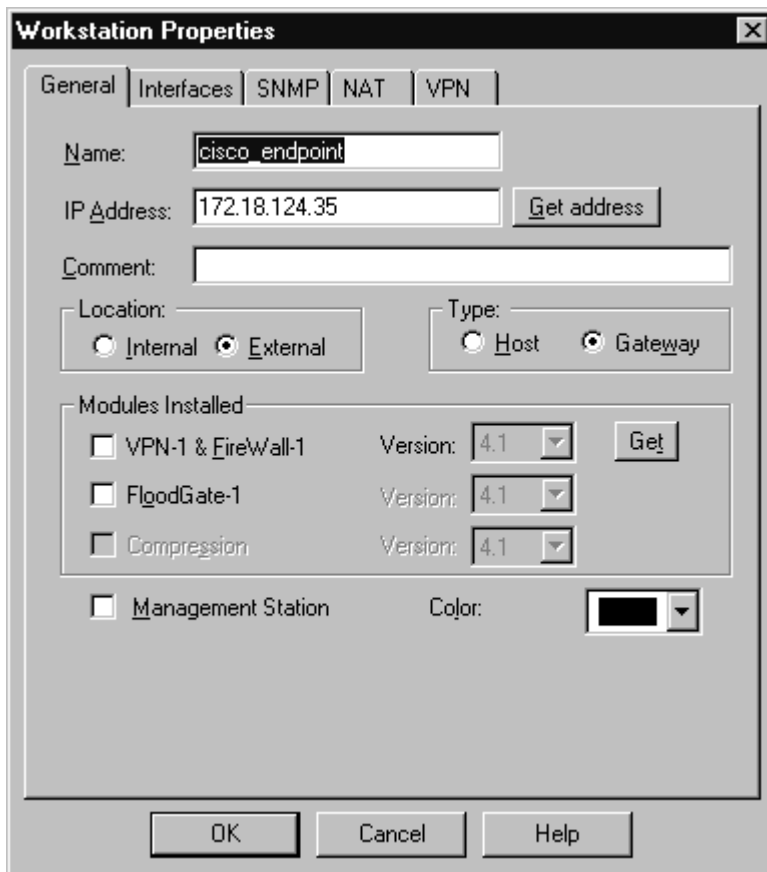
4. Select **Manage > Network objects > New > Network** to configure the object for the external ("inside_cisco") network behind the PIX.

This should agree with the source (first) network in the following PIX command:
access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0 255.255.255.0

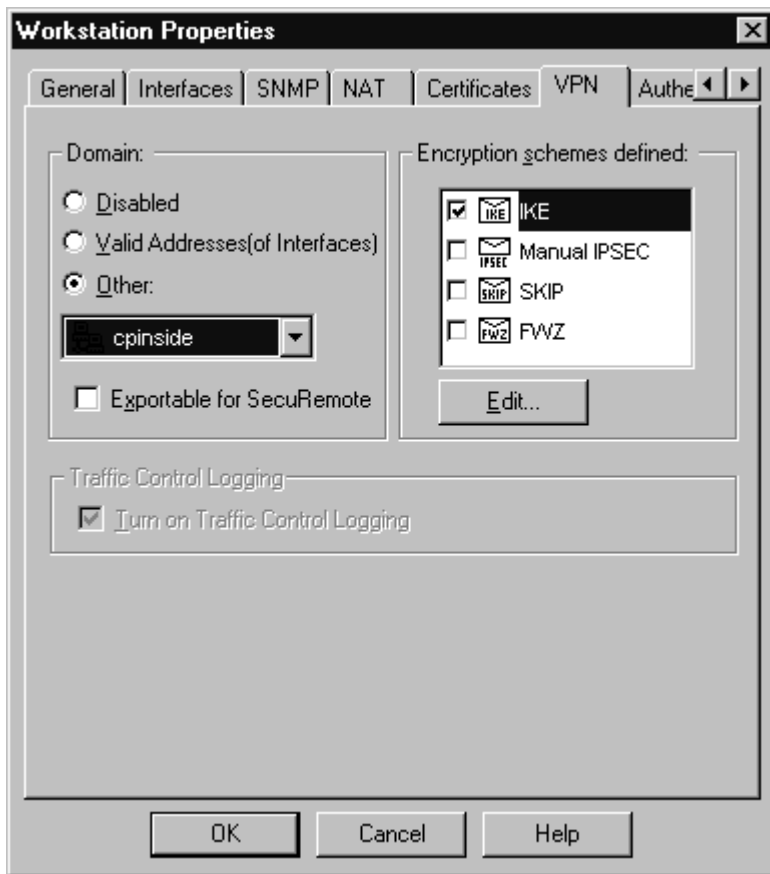


5. Select **Manage > Network objects > New > Workstation** to add an object for the external ("cisco_endpoint") PIX gateway. This is the PIX interface to which the following command is applied:
crypto map *name* interface outside

Under Location, select **External**. For Type, select **Gateway**.
Note: Do not select the VPN-1/FireWall-1 check box.



6. Select **Manage > Network objects > Edit** to edit the Checkpoint gateway endpoint (called "RTPCPVPN") VPN tab. Under Domain, select **Other** and then select the inside of the Checkpoint network (called "cpinside") from the drop-down list. Under Encryption schemes defined, select **IKE**, and then click **Edit**.



7. Change the IKE properties for DES encryption to agree with the commands:

isakmp policy # encryption des

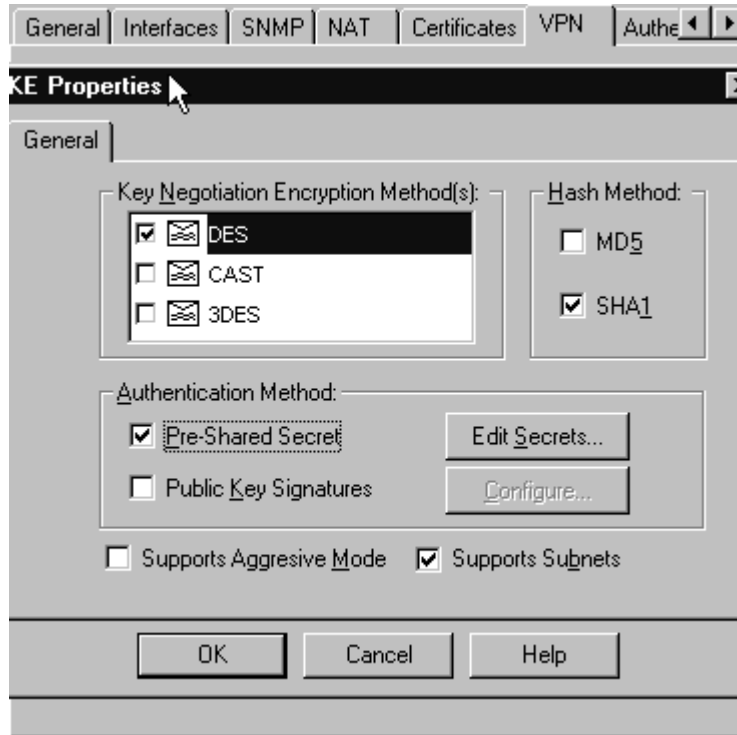
8. Change the IKE properties to SHA1 hashing to agree with the commands:

isakmp policy # hash sha

Change the following settings:

- A. De-select **Aggressive Mode**.
- B. Select the **Supports Subnets** check box.
- C. Under Authentication Method, select the **Pre-Shared Secret** check box. This agrees with the following commands:

isakmp policy # authentication pre-share

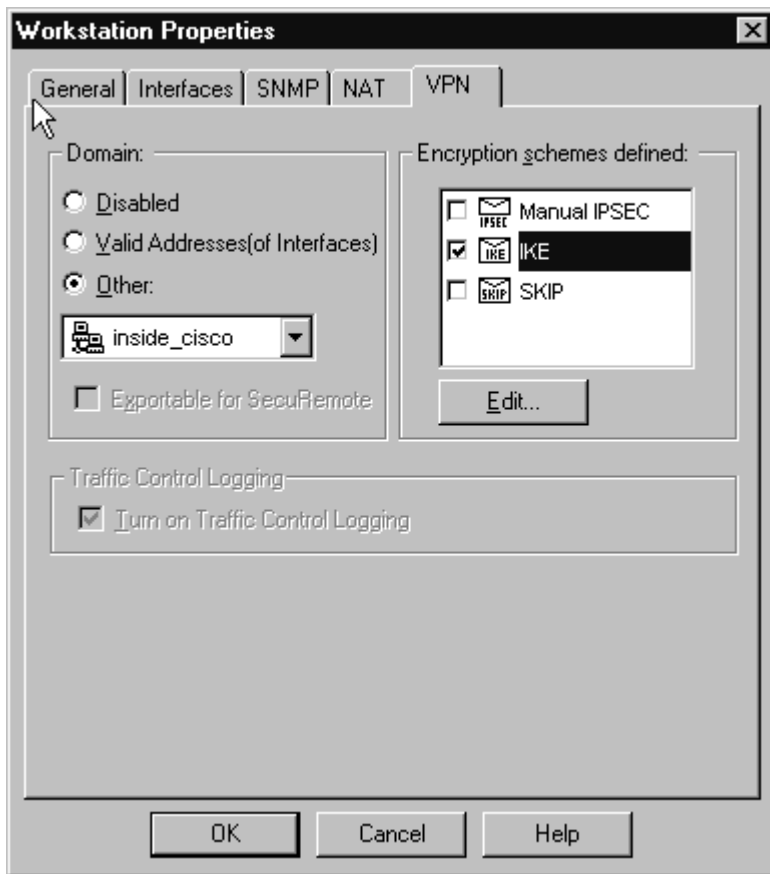


9. Then click **Edit Secrets** to set the pre-shared key to agree with the PIX command:

isakmp key key address address netmask netmask



10. Select **Manage > Network objects > Edit** to edit the "cisco_endpoint" VPN tab. Under Domain, select **Other**, and then select the inside of the PIX network (called "inside_cisco"). Under Encryption schemes defined, select **IKE**, and then click **Edit**.



11. Change the IKE properties DES encryption to agree with the following commands:

isakmp policy # encryption des

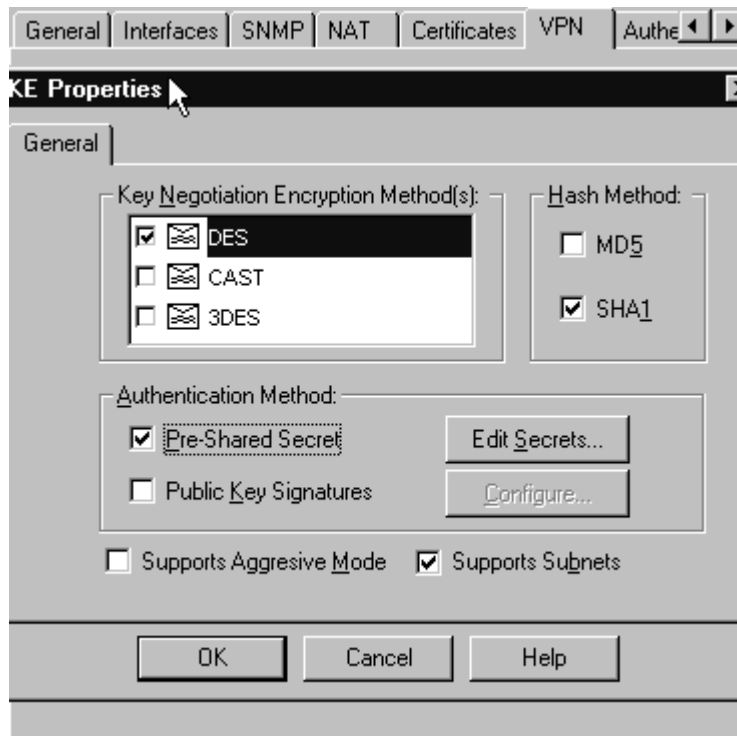
12. Change the IKE properties to SHA1 hashing to agree with the following commands:

crypto isakmp policy # hash sha

Change the following settings:

- A. De-select **Aggressive Mode**.
- B. Select the **Supports Subnets** check box.
- C. Under Authentication Method, select the **Pre-Shared Secret** check box. This agrees with the following commands:

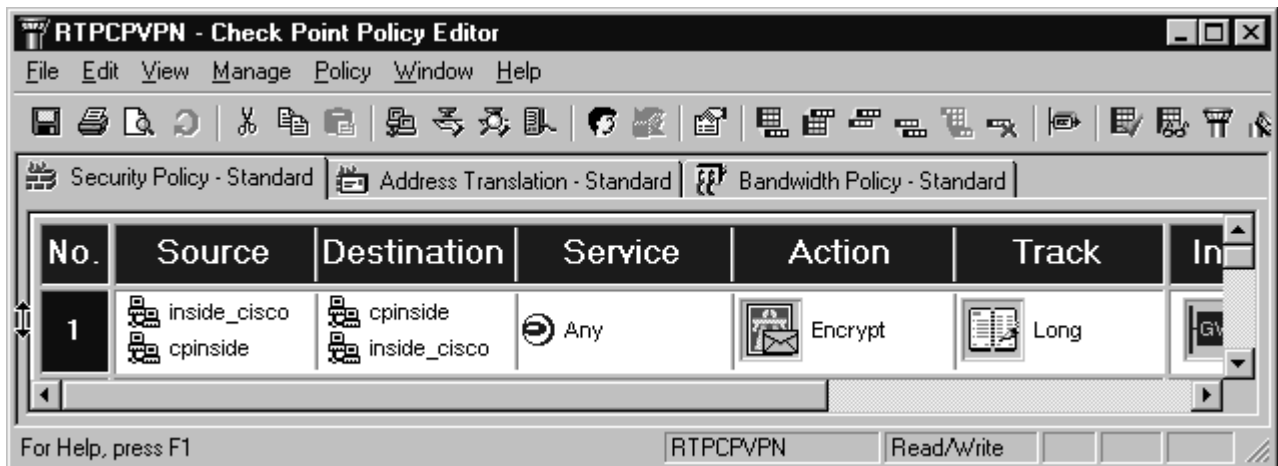
isakmp policy # authentication pre-share



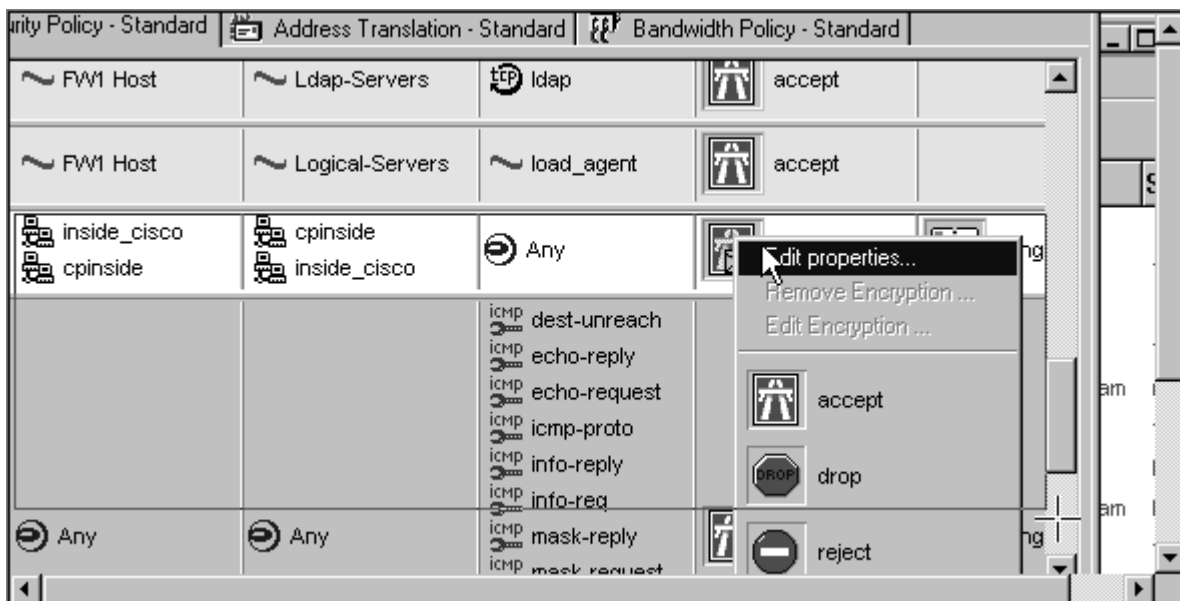
13. Then click **Edit Secrets** to set the pre-shared key to agree with the following PIX command:
isakmp key key address address netmask netmask



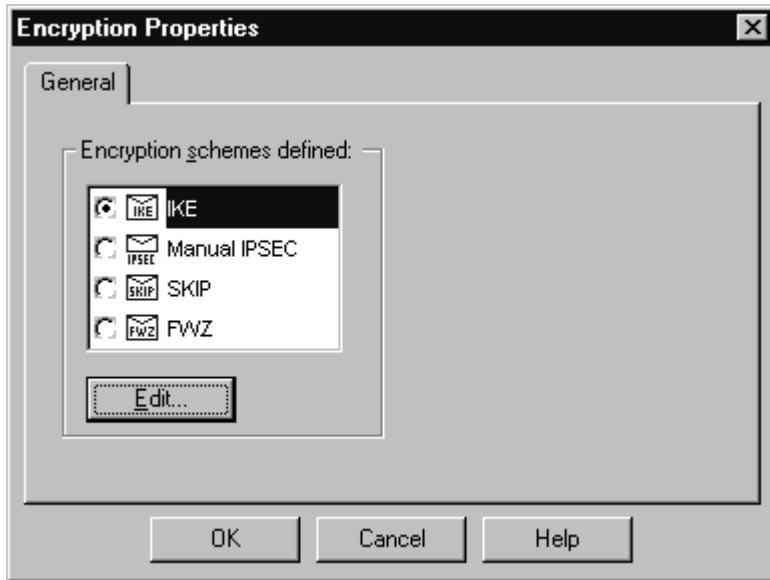
14. In the Policy Editor window, insert a rule with both Source and Destination as "inside_cisco" and "cpinside" (bidirectional). Set **Service=Any**, **Action=Encrypt**, and **Track=Long**.



- Then, under the Action heading, click the green **Encrypt** icon and select **Edit properties** to configure encryption policies.



- Select **IKE**, and then click **Edit**.



17. On the IKE Properties screen, change these properties to agree with the PIX IPSec transforms in the following command:

crypto ipsec transform-set myset esp-des esp-sha-hmac

Under Transform, select **Encryption + Data Integrity (ESP)**. The Encryption Algorithm should be **DES**, Data Integrity should be **SHA1**, and the Allowed Peer Gateway should be the external PIX gateway (called "cisco_endpoint"). Click **OK**.



18. After configuring the Checkpoint, select **Policy > Install** on the Checkpoint menu to have the changes take effect.

debug, show and clear Commands

Before issuing **debug** commands, please see [Important Information on Debug Commands](#).

Cisco PIX Firewall

- **debug crypto engine** - Display debug messages about crypto engines, which perform encryption and decryption.
- **debug crypto isakmp** - Display messages about IKE events.
- **debug crypto ipsec** - Display IPSec events.
- **show crypto isakmp sa** - View all current IKE security associations (SAs) at a peer.
- **show crypto ipsec sa** - View the settings used by current security associations.
- **clear crypto isakmp** - (from configuration mode) Clear all active IKE connections.
- **clear crypto sa** - (from configuration mode) Delete all IPSec security associations.

Checkpoint:

Because the Tracking was set for Long in the Policy Editor window, denied traffic should appear in red in the Log Viewer. More verbose debug can be obtained by doing:

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

and in another window:

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

Note: This was a Microsoft Windows NT installation.

Clearing SAs on the Checkpoint can be done by issuing the following commands:

```
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
```

and answering **yes** at the Are you sure? prompt.

Sample Debug Output from the 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
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
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
  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
  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, de
602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi= 0x9d71f29c(26414
602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi= 0xebc8c823(3955
```

```
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
```

Related Information

- [More IPSec Technical Tips](#)
- [IPSec Support Pages](#)
- [Configuring IPSec Network Security](#)
- [Configuring Internet Key Exchange Security Protocol](#)
- [PIX Top Issues](#)
- [PIX Support Pages](#)
- [PIX 5.1: Configuring IPSec](#)
- [PIX 5.2: Configuring IPSec](#)
- [PIX 5.3: Configuring IPSec](#)

Home	What's New	How to Buy	Login	Register	Feedback	Search	Map/Help
----------------------	----------------------------	----------------------------	-----------------------	--------------------------	--------------------------	------------------------	--------------------------

All contents are Copyright © 1992--2001 Cisco Systems Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).