

Cisco PIX

Interoperability Guide

Copyright © 2004, F/X Communications. All Rights Reserved. The use and copying of this product is subject to a license agreement. Any other use is strictly prohibited. No part of this publication may be reproduced, transcribed, or translated into any language, in any form by any means without the prior written consent of F/X Communications. Information in this document is subject to change without notice and does not constitute any commitment on the part of F/X Communications.

F/X Communications, Brolaeggerstraede 12, DK-4300 Holbaek, Denmark.

Contents

1. Cisco PIX 5.01	3
1.1. Important notice	3
1.2. Brief step-by-step instructions	3
1.3. Configuring Cisco PIX	3
1.4. Configuring the InJoy side	4
1.5. Connecting to the Cisco PIX side	5

1. Cisco PIX 5.01

1.1. Important notice

The connections in the following tests were conducted over a LAN, using 192.162.x.x IP addresses for the IPSec endpoints. 192.168.x.x addresses were used to illustrate internal networks (behind IPSec endpoints). When modifying these samples for Internet use, replace the 192.162.x.x addresses with the external IP address of the IPSec endpoints.

1.2. Brief step-by-step instructions

To create a VPN using the InJoy IPSec and Cisco PIX, the following steps must be completed:

- 1 Install an InJoy product with IPSec on a PC ("Local Host").
- 2 Install the Pluto IKE server on the InJoy PC.
- 3 Configure the Cisco PIX ("Remote Gateway").
 - 3.1 Define the Cisco PIX setup
 - 3.2 Setup TACACS (RADIUS) sever for Extended Authentication (XAuth)
- 4 Configure the InJoy IPSec side.
- 5 Restart the InJoy IPSec product and the IKE server.
- 6 Force InJoy to establish the SA. (note: any traffic between the IPSec endpoints will force this).

1.3. Configuring Cisco PIX

Below is an example of PIX configuration with extended authentication and inner (Red Node) IP address assignment.

```
PIX Version 5.1(0)210
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
access-list nonat permit ip 172.18.1.0 255.255.255.0 172.18.2.0 255.255.255.0
access-list 106 permit ip 172.18.1.0 255.255.255.0 10.1.1.0 255.255.255.0
enable password 9Femq2iCVqLKfvaV encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
logging timestamp
no logging standby
logging console debugging
no logging monitor
```

```

logging buffered debugging
logging trap debugging
logging history debugging
logging facility 20
logging queue 9048
interface ethernet0 10baset
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 207.35.166.199 255.255.255.224
ip address inside 172.18.1.254 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
ip local pool dealer2 172.18.2.1-172.18.2.150
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 207.35.166.201 netmask 255.255.255.255
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 207.35.166.193 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partner protocol tacacs+
aaa-server partner (inside) host 172.18.1.1 vitacs timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
sysopt ipsec pl-compatible
crypto ipsec transform-set strong-des esp-des esp-md5-hmac
crypto dynamic-map cisco 4 set transform-set strong-des
crypto map partner-map 10 ipsec-isakmp
crypto map partner-map 10 match address 106
crypto map partner-map 10 set peer 207.35.166.194
crypto map partner-map 10 set transform-set strong-des
crypto map partner-map 40 ipsec-isakmp dynamic cisco
crypto map partner-map client configuration address initiate
crypto map partner-map client authentication partner
crypto map partner-map interface outside
isakmp enable outside
isakmp key vitlabtest address 207.35.166.200 netmask 255.255.255.255 no-xauth no
-config-mode
isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local dealer2 outside
isakmp policy 8 authentication pre-share
isakmp policy 8 encryption des
isakmp policy 8 hash md5
isakmp policy 8 group 1
isakmp policy 8 lifetime 1000
telnet timeout 5
terminal width 80
Cryptochecksum:8050066b6428ba7bf43a5cefb7c0dd5

```

1.4. *Configuring the InJoy side*

On the Local Host add the following section to the file ipsec.cnf, to describe the SA to the Cisco PIX:

```

cisco
    Description = "Cisco PIX",

```

```

Mode = Tunnel,
Local-IP = "192.162.5.2",      # local host IP address
Remote-IP = "207.35.166.199", # remote gateway IP address
Remote-Net = "172.18.1.0",
Remote-Mask = "255.255.255.0",
Auth-Type = Client-Xauth,
User-Id = Prompt,             # ask for username for Xauth
AH = No,
ESP = Yes,
Reinit = Yes,
Preshared-Secret = "secret_phrase",

```

Restart the InJoy IPsec and the Pluto IKE server for changes to take effect.

User-Id = Prompt is used to allow entering of the user name and password for the extended authentication.

1.5. *Connecting to the Cisco PIX side*

If extended authentication support is configured, you will be prompted to enter an appropriate user name and password (by the IPsec host product). Any traffic to the Remote Subnet behind the Gateway will force IKE negotiations.

After extended authentication is performed successfully, the Cisco PIX side will assign the Local Host an Inner (Red Node) IP address. This address will be used as the source IP address of tunneled traffic from the Local Host to the Remote Gateway. In other words, the destination IP address of tunneled traffic will be changed from the public IP address, to the internal IP address assigned by the Cisco PIX side.

On the Local Host, the ipsec.log will contain the following lines:

```

Jul 11 03:29:25 : adding to pluto: cisco
Jul 11 03:29:25 : force pluto to initiate: cisco
Jul 11 03:29:37 : ipsec: install sa [cisco]
Jul 11 03:29:37 : SA name = [cisco]
Jul 11 03:29:37 : XA name = [smith]
Jul 11 03:29:37 : Local gateway (host) ip address = [192.162.5.2]
Jul 11 03:29:37 : Inner IP = [172.18.2.3]
Jul 11 03:29:37 : Local net = [172.18.2.3]
Jul 11 03:29:37 : Local net mask = [255.255.255.255]
Jul 11 03:29:37 : Remote gateway (host) ip address = [207.35.166.199]
Jul 11 03:29:37 : Remote net = [172.18.1.0]
Jul 11 03:29:37 : Remote net mask = [255.255.255.0]
Jul 11 03:29:37 : ISAKMP SA lifetime = [1000] seconds
Jul 11 03:29:37 : IPSEC SA lifetime = [28800] seconds
Jul 11 03:29:37 : ESP encr/auth/keylen=[ESP_ALG_CBC_DES/AH_ALG_MD5/24]
Jul 11 03:29:37 : AH method/keylen = [unknown/0]
Jul 11 03:29:37 : Road Warrior = [yes]

```

On the Remote Gateway, extended Authentication will be performed using the TACACS (or RADIUS) user database and an inner IP address will be assigned for the Local Host.

```

crypto_isakmp_process_block: src 154.5.112.130, dest 207.35.166.199
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 0 against priority 8 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA

```

```

ISAKMP: auth pre-share
ISAKMP: unknown DH group 5
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 1 against priority 8 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: auth pre-share
ISAKMP: unknown DH group 5
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 8 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: auth pre-share
ISAKMP: default group 2
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 8 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: auth pre-share
ISAKMP: default group 2
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 8 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: auth pre-share
ISAKMP: unknown DH group 5
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 8 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: auth pre-share
ISAKMP: unknown DH group 5
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 8 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: auth pre-share
ISAKMP: default group 2
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 7 against priority 8 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: auth pre-share
ISAKMP: default group 2
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 8 against priority 8 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: auth pre-share
ISAKMP: default group 1
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 9 against priority 8 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: auth pre-share
ISAKMP: default group 1

```

```

ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 10 against priority 8 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: auth pre-share
ISAKMP: default group 1
ISAKMP: life type in seconds
ISAKMP: life duration (basic) of 1000
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.162.5.2, dest 207.35.166.199
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.162.5.2, dest 207.35.166.199
OAK_QM exchange
ISAKMP (0:0): Need XAUTH
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 192.162.5.2. ID = 234420053 (0xdf8f755)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.162.5.2, dest 207.35.166.199
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 192.162.5.2. message ID =
234420053
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 192.162.5.2. ID = 234420053 (0xdf8f755)
crypto_isakmp_process_block: src 192.162.5.2, dest 207.35.166.199
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 192.162.5.2. message ID =
234420053
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): initiating peer config to 192.162.5.2. ID = -429703294 (0xe6633f82)
return status is IKMP_NO_ERROR109011: Authen Session Start: user 'smith', sid 3
crypto_isakmp_process_block: src 192.162.5.2, dest 207.35.166.199
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 192.162.5.2. message ID = -
429703294
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.162.5.2, dest 207.35.166.199
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = -216311441
ISAKMP : Checking IPsec proposal 0
ISAKMP: transform 0, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part
#1,
(key eng. msg.) dest= 207.35.166.199, src= 192.162.5.2,
dest_proxy= 172.18.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 172.18.2.3/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,

```

```

lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = -216311441
ISAKMP (0): processing ID payload. message ID = -216311441
ISAKMP (0): ID_IPV4_ADDR src 172.18.2.3 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = -216311441
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 172.18.1.0/255.255.255.0 prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xaaccabdb(2865540059) for SA
from 192.162.5.2 to 207.35.166.199 for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.162.5.2, dest 207.35.166.199
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITIPSEC(map_alloc_entry): allocating entry 6
IPSEC(map_alloc_entry): allocating entry 5
ISAKMP (0): Creating IPsec SAs
inbound SA from 192.162.5.2 to 207.35.166.199 (proxy 172.18.2.3 to 172.18.1.0)
has spi -1429427237 and conn_id 6 and flags 4
lifetime of 28800 seconds
outbound SA from 207.35.166.199 to 192.162.5.2 (proxy 172.18.1.0 to 172.18.2.3)
has spi -1495552099 and conn_id 5 and flags 4
lifetime of 28800 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 207.35.166.199, src= 192.162.5.2,
dest_proxy= 172.18.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 172.18.2.3/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 0kb,
spi= 0xaaccabdb(2865540059), conn_id= 6, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 207.35.166.199, dest= 192.162.5.2,
src_proxy= 172.18.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 172.18.2.3/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 0kb,
spi= 0xa6dbaf9d(2799415197), conn_id= 5, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR602301: sa created,
(sa) sa_dest= 207.35.166.199, sa_prot= 50,
sa_spi= 0xaaccabdb(2865540059),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 6
602301: sa created,
(sa) sa_dest= 192.162.5.2, sa_prot= 50,
sa_spi= 0xa6dbaf9d(2799415197),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 5

```