



CHECK POINT™
Software Technologies Ltd.

Check Point VPN-1 and Cisco PIX Gateway to Gateway IKE VPN Using Pre-shared Secrets

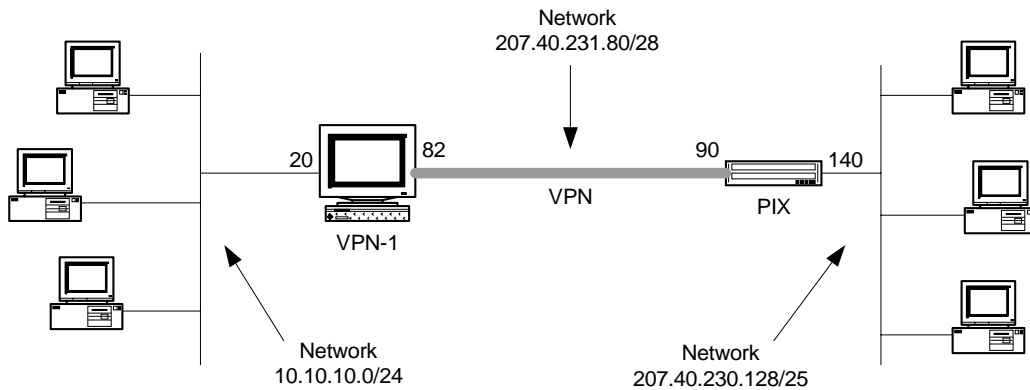
Authored By: David Dietrich
Date: May19, 2000
Purpose: To describe and document how to configure IKE VPN's with Cisco PIX
Version: 1.0

Table of Contents

Overview.....	2
Configuring VPN-1 objects and rules.....	2
PIX Configuration.....	8
Other PIX Configuration Scenarios.....	10
Scenario 1 – PIX needs to NAT outbound, but not the in IKE tunnel.....	10
Scenario 2 – PIX needs to NAT outbound, including the in IKE tunnel.....	10
Tips and Troubleshooting.....	12
Reference information.....	13
Complete PIX config file for the simple gateway to gateway VPN example.....	13
Output from fwd -d during successful VPN traverse (quite verbose):.....	14
Output from PIX debug crypto ipsec/isakmp commands.....	21

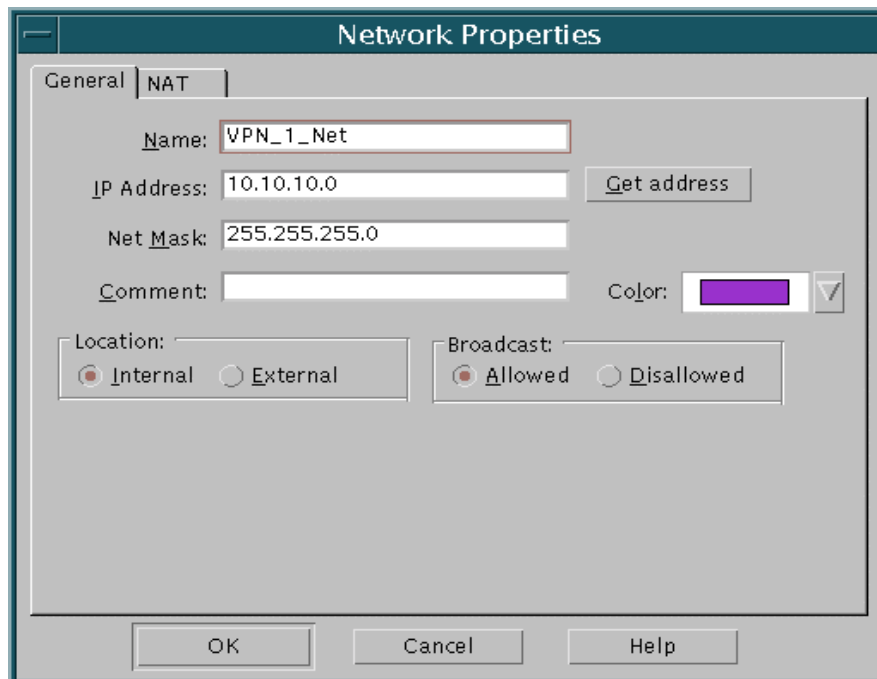
Overview

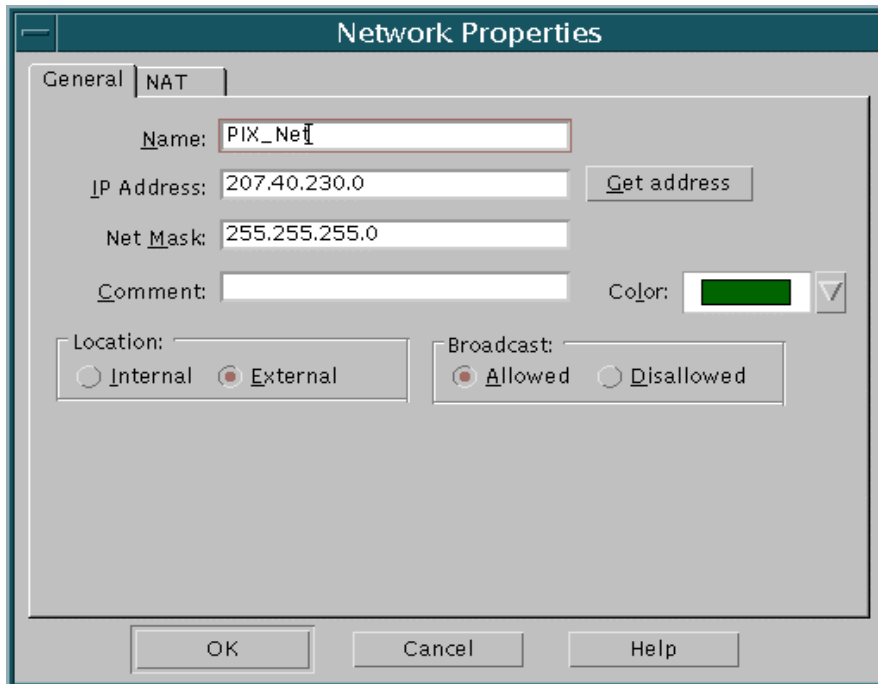
This document describes a simple IPSEC vpn configuration between a VPN-1 gateway, version 4.1 SP1 and a Cisco PIX version 5.x. The authentication method used will be shared secrets. This configuration will describe a simple vpn per the following network diagram:



Configuring VPN-1 objects and rules

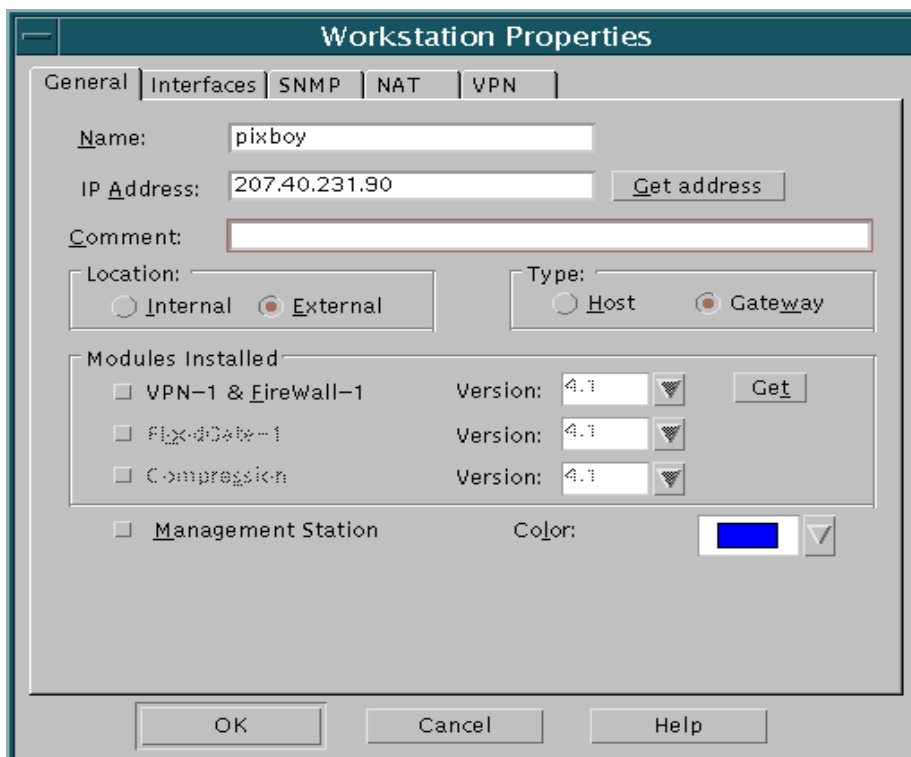
Create network objects to represent the traffic that the VPN-1 gateway and the PIX will encrypt. In this example, this will be the two networks behind the VPN-1 gateway and the PIX.



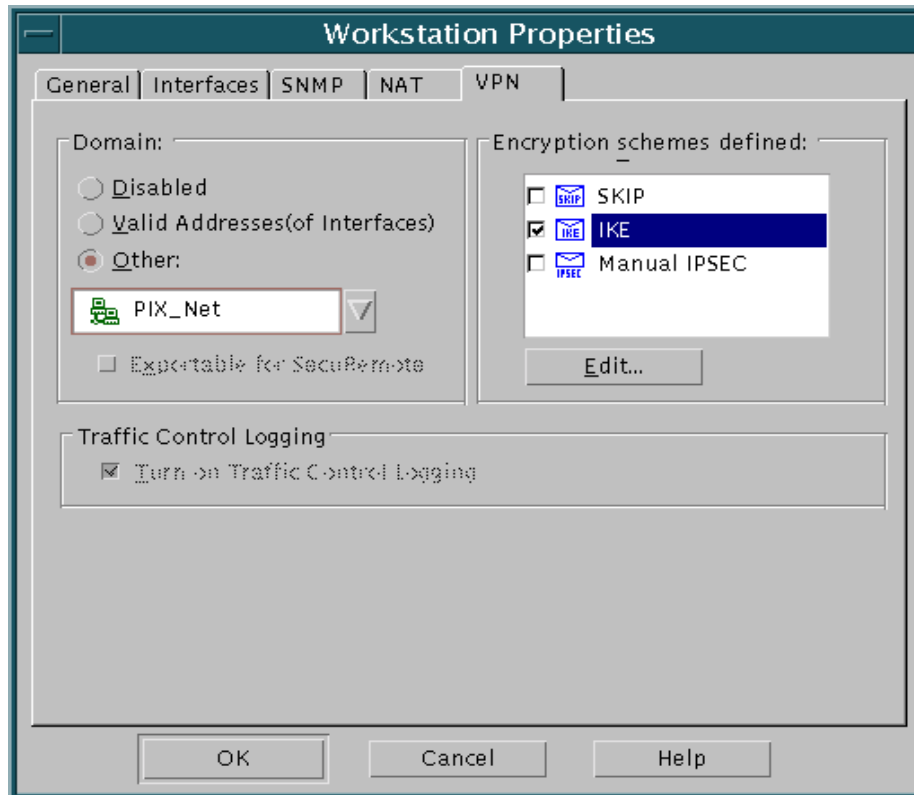


Create a workstation object for the PIX

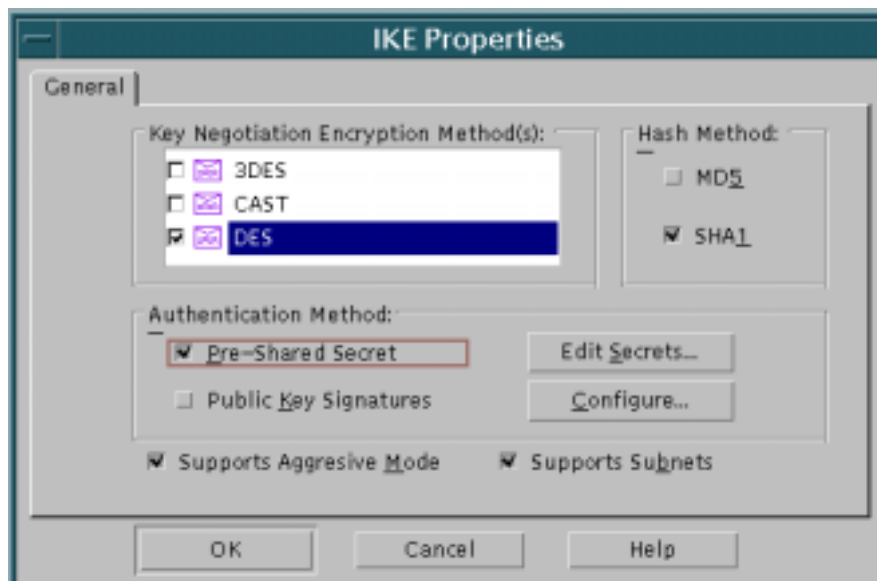
In the general tab, select location External and type Gateway



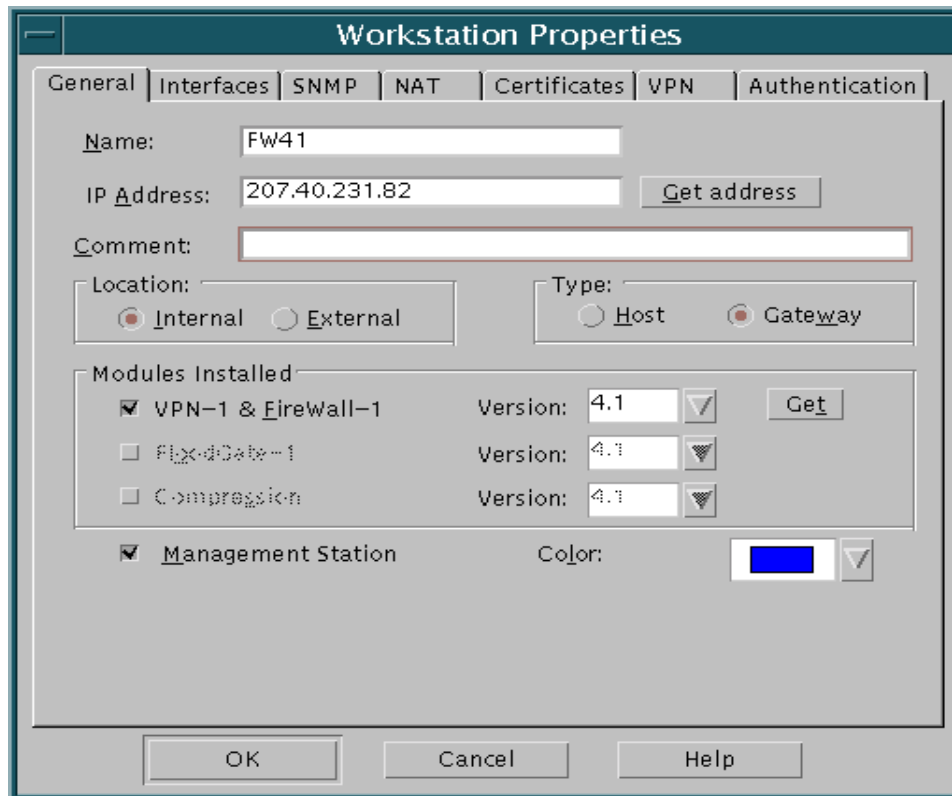
In the VPN tab identify the PIX_Net network object as the encryption Domain, on the left. On the right, select IKE as the scheme. After selecting IKE, select the Edit button...



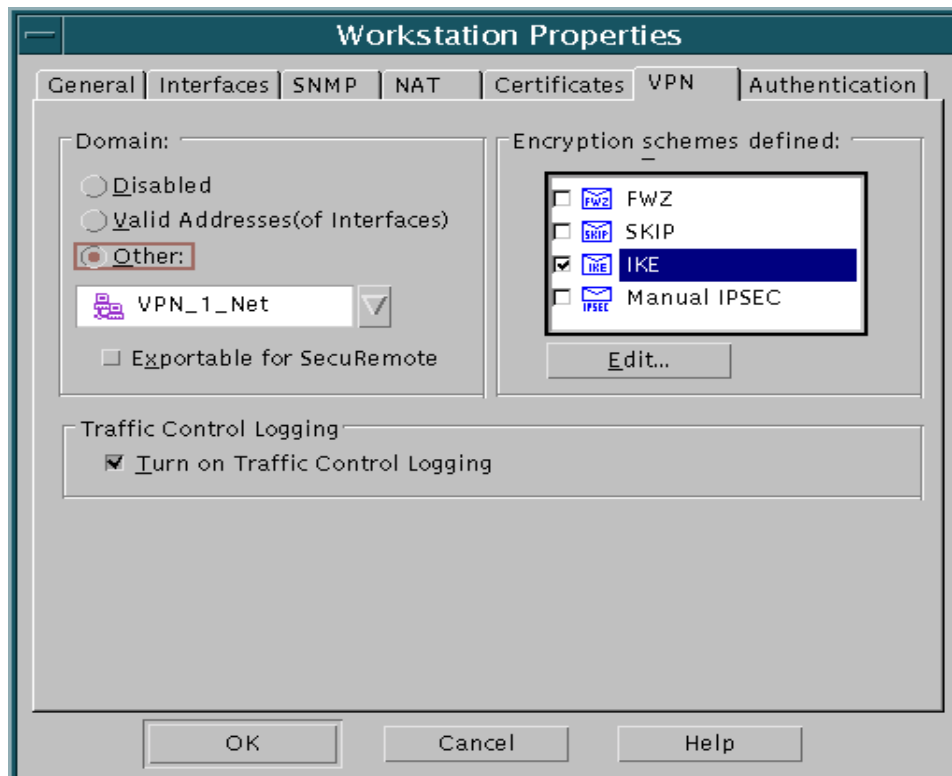
In the IKE Properties, select the methods you intend to use for IKE security association negotiations. In this example we'll use DES encryption and SHA hash algorithm. Check Aggressive Mode and Subnet support as well. Note: 3DES is a better encryption method, of course. The lab PIX unit we had was only enabled with DES.



Create a workstation object for the VPN-1 gateway



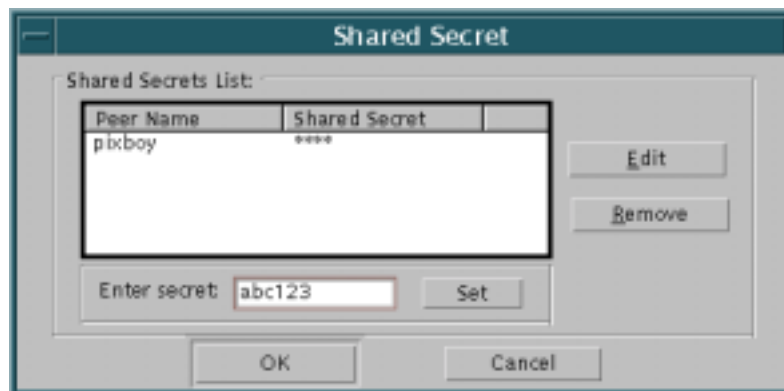
In the VPN tab identify the VPN_1_Net network object as the encryption Domain, on the left. On the right, select IKE as the scheme. After selecting IKE, select the Edit button...



In the IKE Properties, select the methods you intend to use for IKE security association negotiations. In this example we'll use DES encryption and SHA hash algorithm. Multiple selections may be made if the firewall needs to support other VPN's with different parameters. Check Aggressive Mode and Subnet support as well. Select Pre-share Secret and continue....

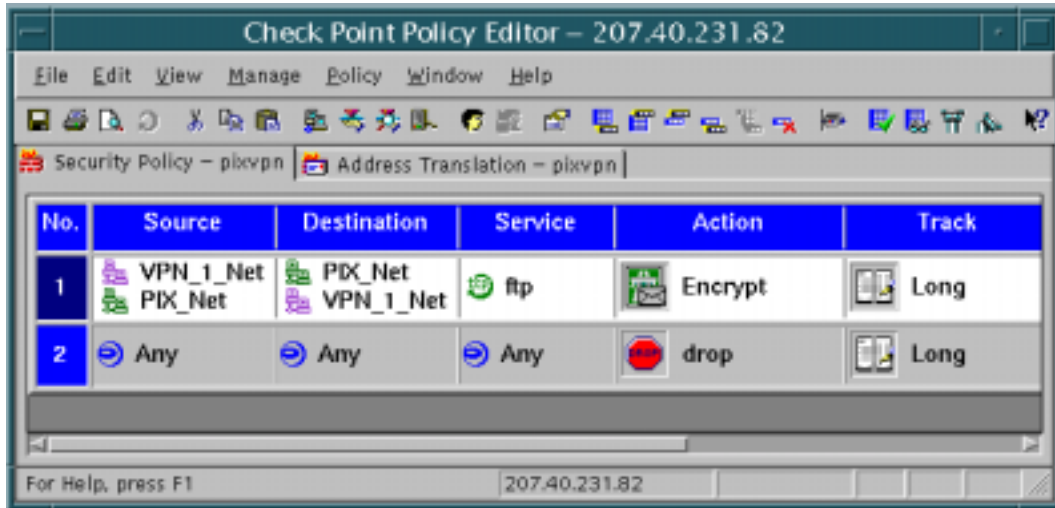


Select the object defined for the peer and enter a shared secret value.

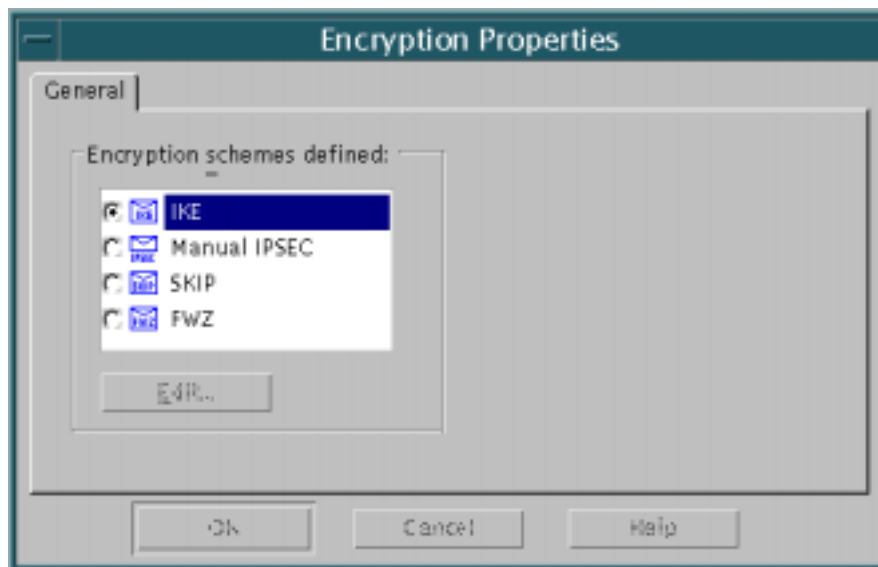


Create the encryption rule in the VPN-1 Policy editor

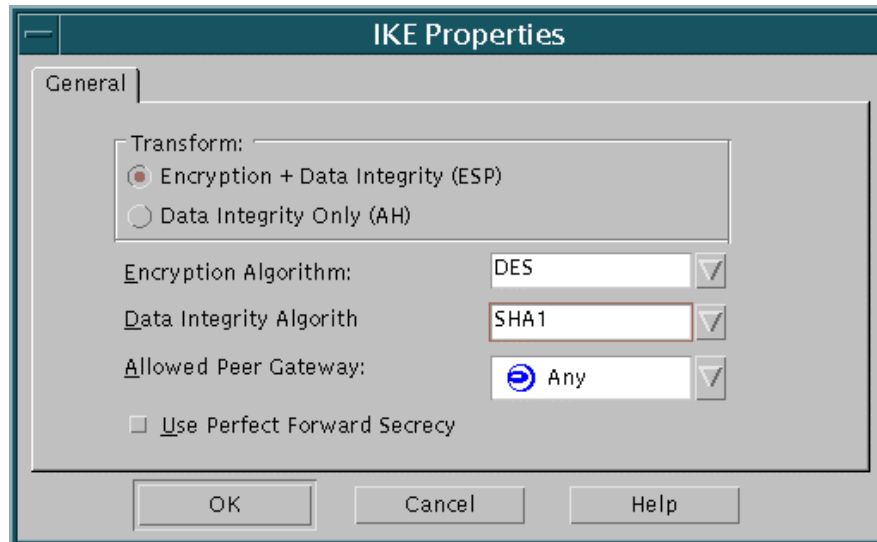
In this example, we've allowed ftp traffic between the protected networks. Right click on the Encrypt Action and edit Encryption Properties....



Select IKE. Then select Edit and continue...



Select the appropriate properties. The selected algorithms will match the transform defined later in the PIX. These properties pertain to Phase 2 negotiation establishing IPSEC security association. In this example, Perfect Forward Secrecy is not used. The peer gateway could have been limited to the PIX object.



PIX Configuration

The following is a simple configuration of an IPSEC vpn using pre-shared secrets. The actual config commands are shown in **dark red**. This is a minimal configuration; some of the commands shown are default values.

The PIX will define the inside and outside interfaces automatically. These definitions appear as follows:

```
nameif ethernet0 outside security0  
nameif ethernet1 inside security100
```

Assign addresses and netmasks to the interfaces

```
ip address outside 207.40.231.90 255.255.255.240  
ip address inside 207.40.230.140 255.255.255.128
```

Define an access list for the traffic to be encrypted between the internal networks. This access list will be used in a crypto map (a set of encryption instructions). When access lists are used for crypto map association, permit means encrypt. On the PIX access lists can be used for encryption (crypto map association) and for packet filtering (interface access group association).

```
access-list 101 permit ip 207.40.230.0 255.255.255.0 10.10.10.0 255.255.255.0  
access-list 101 permit ip 10.10.10.0 255.255.255.0 207.40.230.0 255.255.255.0
```

Define another access list to specify allowed inbound traffic. The list we used above specifies what to encrypt, since it will be bound to a crypto map. But it will only work in conjunction with allowed traffic flows. There are several ways to address and/or override this. We'll use an access list.

```
access-list 102 permit ip 10.10.10.0 255.255.255.0 207.40.230.0 255.255.255.0
```

Allow outbound connections. No address translation in this example.

```
nat (inside) 0 0 0
```

Allow inbound traffic to be encrypted by binding the second access list to the outside interface.

```
access-group 102 in interface outside
```

Transform Sets - A transform set represents a certain combination of security protocols and algorithms. During the IPsec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. You can specify multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry will be used in the IPsec security association negotiation to protect the data flows specified by that crypto map entry's access list. During IPsec security association negotiations with IKE, the peers search for a transform set that is the same at both peers.

```
crypto ipsec transform-set pixset esp-des esp-sha-hmac
```

Crypto Maps - Crypto maps specify IPsec policy. Crypto map entries created for IPsec pull together the various parts used to set up IPsec security associations, including the following:

- Which traffic should be protected by IPsec (per a crypto access list)
- Where IPsec-protected traffic should be sent (who the peer is)
- What IPsec security should be applied to this traffic (selecting from a list of one or more transform sets)
- Whether security associations are manually established or are established via IKE
- Other parameters that might be necessary to define an IPsec SA

```
crypto map testmap 10 ipsec-isakmp
crypto map testmap 10 match address 101
crypto map testmap 10 set peer 207.40.231.82
crypto map testmap 10 set transform-set pixset
```

You need to apply a crypto map set to each interface through which IPsec traffic will flow. Applying the crypto map set to an interface instructs the PIX Firewall to evaluate all the interface's traffic against the crypto map set and to use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto IPsec.

```
crypto map testmap interface outside
Enable isakmp on the outside interface
```

```
isakmp enable outside
```

Define the peer (the VPN-1 gateway) and the shared secret

```
isakmp key abc123 address 207.40.231.82 netmask 255.255.255.255
```

We can use IP addresses or hostnames during negotiations between the encrypting peers. In this example we'll use IP address.

```
isakmp identity address
```

IKE Policies – a policy stating which parameters are used in during IKE negotiation to establish the IKE security association (Phase 1)

For this example, use pre-shared secrets, des encryption, sha hash algorithm.

```
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash sha
```

Set the Diffie-Hellman group identifier to 1024 bit (1=768 bit, 2=1024 bit)

```
isakmp policy 20 group 2
```

Set the security association in seconds. 86,400 seconds is one day, the default value.

```
isakmp policy 20 lifetime 86400
```

Now test the VPN. Initiate traffic from one network to the other. Encrypt and Decrypt log entries should appear in the VPN-1 log viewer. If the VPN is not functional, use the info in the tips and troubleshooting section.

Other PIX Configuration Scenarios

Use the following changes and additions with the prior simple VPN example.

Scenario 1 – PIX needs to NAT outbound, but not the in IKE tunnel

The PIX will have some configuration to translate addresses outbound. The global command may be used to define a range of addresses to use on outbound connections. The following global and nat statements assign outbound connections source IP's from a range.

```
global (outside) 1 207.40.231.85-207.40.231.89
nat (inside) 1 0 0
```

Add an additional nat statement to exempt the tunnel traffic (crypto access list) from translation as follows:

```
nat (inside) 0 access-list 101
```

Scenario 2 – PIX needs to NAT outbound, including the in IKE tunnel

Define the outbound global address range as in scenario 1.

```
global (outside) 1 207.40.231.85-207.40.231.89
nat (inside) 1 0 0
```

If necessary, add a static global to local address mapping (static NAT). The only way to allow an inbound connection with NAT is with a static mapping. This will allow traffic to initiate from the other side of the tunnel if needed. The static global address must not overlap the range used in the global range. The order of the IP args is global then local, i.e. 207.40.231.84 is the public address in this example:

```
static (inside, outside) 207.40.231.84 207.40.230.198 netmask 255.255.255.255
```

Change the interface and crypto access lists to refer to the global addresses instead of the inside network.

```
access-list 101 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.85
access-list 101 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.86
```

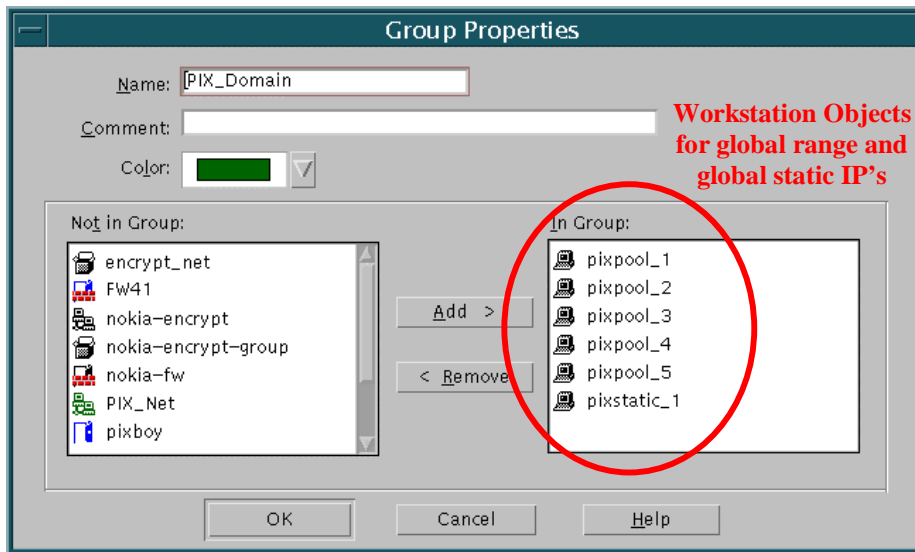
```

access-list 101 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.87
access-list 101 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.88
access-list 101 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.89
access-list 101 permit ip host 207.40.231.85 10.10.10.0 255.255.255.0
access-list 101 permit ip host 207.40.231.86 10.10.10.0 255.255.255.0
access-list 101 permit ip host 207.40.231.87 10.10.10.0 255.255.255.0
access-list 101 permit ip host 207.40.231.88 10.10.10.0 255.255.255.0
access-list 101 permit ip host 207.40.231.89 10.10.10.0 255.255.255.0
access-list 102 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.85
access-list 102 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.86
access-list 102 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.87
access-list 102 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.88
access-list 102 permit ip 10.10.10.0 255.255.255.0 host 207.40.231.89

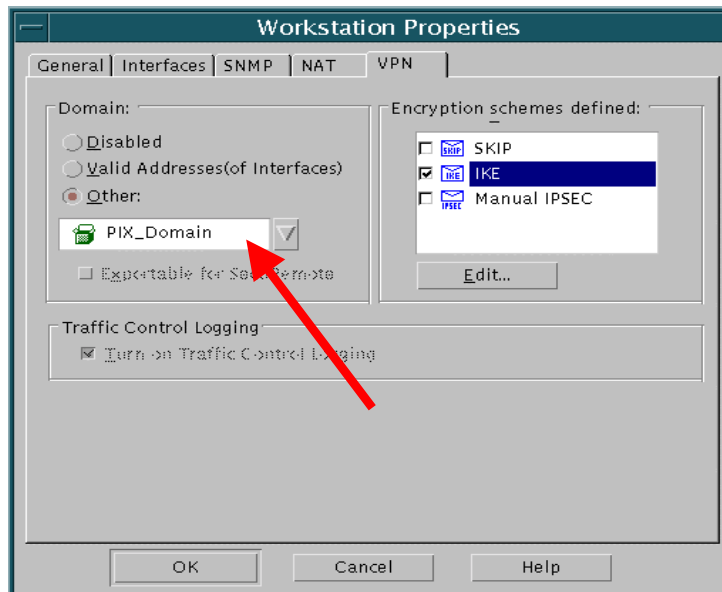
```

Now change the encryption domain for the PIX object on the VPN-1 gateway to include the global (public) addresses rather than the PIX inside net.

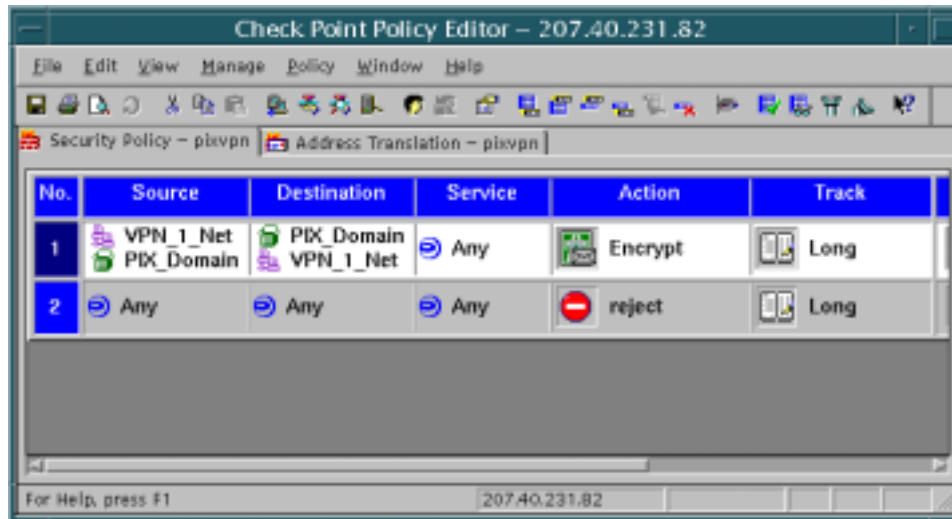
In the VPN-1 gui, create an object for each global range address and each static global address, then put these into a group to be used as the PIX encryption domain.



PIX workstation object will use the group as the encryption domain, rather than the inside network object :



Use the PIX encryption domain group object in the encryption Rule



Tips and Troubleshooting

If more than one attempt is made at trying the VPN, clear out IKE and IPSEC security association on both the PIX and the VPN-1 gateway before trying again.

PIX:

```
clear crypto isakmp sa  
clear crypto ipsec sa
```

VPN-1:

The following commands can be put in a batch of script file for convenience

```
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
```

In addition, watching the debug output of VPN-1 and of the PIX during the negotiations can be useful.

PIX:

```
debug crypto ipsec  
debug crypto isakmp
```

VPN-1:

Run fwd in debug mode:

On a management-only machine, run: fwd -d -n (fw d -d -n on Windows NT).

On a standalone machine, run fwd -d (fw d -d on Windows NT).

On a module-only machine, run fwd -d MASTER (fw d -d MASTER on Windows NT), where MASTER is the name (or IP address) of the management station to which this module should send its logs. If there are several masters, specify them in the same order as in the \$FWDIR/conf/MASTERS file, separated by blanks (or run "fwd -d `cat \$FWDIR/conf/MASTERS`" on UNIX).

Before running the above commands, you need to run 'fwstop'. Once fwd is running, leave it running, and from another window run 'fwstart'.

Reference information

Complete PIX config file for the simple gateway to gateway VPN example

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
access-list 101 permit ip 207.40.230.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list 101 permit ip 10.10.10.0 255.255.255.0 207.40.230.0 255.255.255.0
access-list 102 permit ip 10.10.10.0 255.255.255.0 207.40.230.0 255.255.255.0
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixl
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
no logging timestamp
no logging standby
no logging console
logging monitor errors
logging buffered debugging
logging trap errors
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 207.40.231.90 255.255.255.240
ip address inside 207.40.230.140 255.255.255.128
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
access-group 102 in interface outside
route outside 0.0.0.0 0.0.0.0 207.40.231.82 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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
```

```

floodguard enable
crypto ipsec transform-set pixset esp-des esp-sha-hmac
crypto map testmap 10 ipsec-isakmp
crypto map testmap 10 match address 101
crypto map testmap 10 set peer 207.40.231.82
crypto map testmap 10 set transform-set pixset
crypto map testmap interface outside
isakmp enable outside
isakmp key abc123 address 207.40.231.82 netmask 255.255.255.255
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
telnet timeout 5
terminal width 80

```

Output from fwd -d during successful VPN traverse (quite verbose):

```

# fwd -d
[fwd@fw41] lvfile_init: updating account logtrack
[fwd@fw41] lvtrack_parse:(0) scanned only 2 arguments
[fwd@fw41] lvfile_init: updating normal logtrack
[fwd@fw41] lvtrack_parse:(0) scanned only 2 arguments
[fwd@fw41] in log initfile finished open
[fwd@fw41] fw_read_file: file /opt/CPfw1-41/state/local.lg read 8866 bytes
[fwd@fw41] log_new: sending info
[fwd@fw41] fw_read_file: file /opt/CPfw1-41/state/local.lg read 8866 bytes
[fwd@fw41] log_formats_read: g_fwid = 0x8b4ca8,fw_fid=0xa2
[fwd@fw41] fwusr_init: creating user commands authentication table
[fwd@fw41] fwusr_init: authentication table created
fwd: FireWall-1 server is running
[fwd@fw41] actlog_active called

[fwd@fw41] in fwd_reload_database do_database = 1
[fwd@fw41] fwa_db_init: called
[fwd@fw41] log keepalive t.o. is 18000000 ms
[fwd@fw41] fwauthd_conf - starting
[fwd@fw41] fw_listen_queue = 200
[fwd@fw41] fw_getiflist: 3 interfaces found
[fwd@fw41] Interface[0]: lo0
[fwd@fw41] Interface[1]: hme0
[fwd@fw41] Interface[2]: hme1
[fwd@fw41] Filter is installed
[fwd@fw41] fwd: filter installed
[fwd@fw41] fwauthd: Installing Services
[fwd@fw41] fwauthd: service 32877 installed
[fwd@fw41] fwauthd: service 32878 installed
[fwd@fw41] fwauthd: service 32879 installed
[fwd@fw41] fwauthd: service 32880 installed
[fwd@fw41] fwauthd: service 32881 installed
[fwd@fw41] fwauthd: service 259 installed
[fwd@fw41] fwauthd: service 32882 installed
[fwd@fw41] fwauthd: service 900 installed
[fwd@fw41] opened rdp at port 259

[fwd@fw41] fwsync_client_init: no servers to connect to
[fwd@fw41] snauth_reconf: called
[fwd@fw41] clauth_reconf: clauth_no_resolve set to 0
[fwd@fw41] clauth_reconf: clauth_no_log_errors set to 0
[fwd@fw41] clauth_reconf: clauth_tolower_users set to 0
[fwd@fw41] Cleared all entries from userc_rules
[fwd@fw41] fwCert_reconf: no cert_start_grace Using default 7200
[fwd@fw41] fwCRLCache_reconf: no crl_start_grace Using default 600
[fwd@fw41] fwCRLCache_reconf: no crl_end_grace Using default 600
[fwd@fw41] isakmpd_run: ISAKMP daemon was executed under pid 1280
[fwd@fw41] fwcomm_setcrypto: deleting cpair 0 for fd 28
[fwd@fw41] fwasync_connbuf_realloc: reallocating 0 from 0 to 1056
[fwd@fw41] mdq_run: mail dequeuer was executed under pid 1281

```

```

[fwd@fw41] fwcomm_setcrypto: deleting cpair 0 for fd 29
[fwd@fw41] fwasync_connbuf_realloc: reallocating 0 from 0 to 1040
[fwd@fw41] fw_stat_tab: 0 elements
[fwd@fw41] fw_stat_tab: 0 elements
[fwd@fw41] compile_log_formats: state/local.lg already exist, do not recompile it
[fwd@fw41] syslog_run: syslogd was executed under pid 1282
[fwd@fw41] fwcomm_setcrypto: deleting cpair 0 for fd 33
[fwd@fw41] fwasync_connbuf_realloc: reallocating 0 from 0 to 1040
[fwd@fw41] fwauthd: starting pingd table check.
[1279@fw41] Alertd : finished gotoend
[1280@fw41] FW-1 ISAKMP daemon: started:
[1280@fw41] fwcomm_setcrypto: deleting cpair 0 for fd 0
[1280@fw41] fwasync_connbuf_realloc: reallocating 0 from 0 to 1056
[1280@fw41] in fwd_reload_database do_database = 1
[1280@fw41] fwa_db_init: called
[1280@fw41] del_flat_groups_cache: delete FlatGroupsCache
[1280@fw41] fwCert_reconf: no cert_start_grace Using default 7200
[1280@fw41] fwCRLCache_reconf: no crl_start_grace Using default 600
[1280@fw41] fwCRLCache_reconf: no crl_end_grace Using default 600
[1280@fw41] fwCert_PKIInit: no crl maximum size for send, using default 10000
[1280@fw41] FwPKIValidateMyCertsInit: my object has no certs
[1280@fw41] fwisakmpd_send_log: sending log message: FW-1 IKE daemon: started
[1280@fw41] fwasync_connbuf_realloc: reallocating 0 from 0 to 1181
[1280@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 9211c0, len = 157, key = 0
[fwd@fw41] comm_decrypt_buf: fd = 28, buf = 94cca8, len = 32, key = 0
[fwd@fw41] comm_decrypt_buf: fd = 28, buf = 94cca8, len = 125, key = 0
[fwd@fw41] simple_ISAKMP_log: log: FW-1 IKE daemon: started
[1280@fw41] fwike_isakmpd_pipe_handler: called without data
[fwd@fw41] process 1282: not auth process
[fwd@fw41] fwasync_do_end_conn: 33: calling 52ea68 to free opaque 936518
[fwd@fw41] fwcomm_setcrypto: deleting cpair 0 for fd 33
[fwd@fw41] ==> fw_encrypt_invoke: scheme is ISAKMP
[fwd@fw41] fw_encrypt_invoke: pckid=7fb entry=503 conn=<a0a0a0a,1052,cf28e681,21,6> arg=0
[fwd@fw41] fw_encrypt_invoke: ifid=2, rule=3
[fwd@fw41] fw_encrypt_invoke: xlatesrc=0, xlatedst=0
[fwd@fw41] fw_encrypt_invoke: xlatesport=0, xlatedport=0
[fwd@fw41] fw_encrypt_invoke: starting encryption
[fwd@fw41] get_range_from_domain: entering
[fwd@fw41] get_range_from_domain: NET addr a0a0a0a net_ip a0a0a00 net_mask fffffff0
addrRange.first a0a0a00 addrRange.last a0a0aff
[fwd@fw41] get_range_from_domain: entering
[fwd@fw41] get_range_from_domain: NET addr cf28e681 net_ip cf28e600 net_mask fffffff0
addrRange.first cf28e600 addrRange.last cf28e6ff
[fwd@fw41] set_possible_ranges: rangeUsed: 1 selfRange a0a0a00-a0a0aff otherRange
cf28e600-cf28e6ff
[fwd@fw41] fwipsec_invoke: sending request by methods 2 2 1 0 0 cf28e75a
[fwd@fw41] fwasync_connbuf_realloc: reallocating 0 from 0 to 1428
[fwd@fw41] fwcomm_encrypt_inplace: fd = 28, buf = 966b20, len = 404, key = 0
[fwd@fw41] fwike_fwd_pipe_handler: called without data
[1280@fw41] comm_decrypt_buf: fd = 0, buf = 8ed9f8, len = 32, key = 0
[1280@fw41] comm_decrypt_buf: fd = 0, buf = 8ed9f8, len = 372, key = 0
[1280@fw41] canonize_gw: Canonized ip is the same as original ip cf28e75a
[1280@fw41] RequestByMethods: used 1 my [a0a0a00-a0a0aff] peer [cf28e600-cf28e6ff]
[1280@fw41] Ass_MatchPeerMethodsIDs: cf28e75a 2020100:00 [a0a0a00-a0a0aff] [cf28e600-
cf28e6ff]
[1280@fw41] Ass_MatchPeerMethodsIDs: match has failed
[1280@fw41] MatchPeerMethodsIDs: cf28e75a 2020100:00 [a0a0a00-a0a0aff] [cf28e600-
cf28e6ff]
[1280@fw41] MatchPeerMethodsIDs: Not found
[1280@fw41] MatchPeerP1Neg: cf28e75a
[1280@fw41] MatchPeerP1Neg: no ongoing phase1 negotiations
[1280@fw41] *** AddNegotiation: ptr 921668 peer cf28e75a cookieI 00:00 msgID 00 methods
2020100 00 new count: 1
[1280@fw41] < FWIKE_ROLE_START > Id = 1
[1280@fw41] < FWIKE_ROLE_INITIATOR > Id = 1
[1280@fw41] ike_initiator: entering
[1280@fw41] InitiatorOnEnter: idRanges USED mine [a0a0a00-a0a0aff] peer's [cf28e600-
cf28e6ff]
[1280@fw41] findSAByPeer: Valid ISAKMP SA was not found
[1280@fw41] < FWIKE_EXCH_START > Id = 1
[1280@fw41] < FWIKE_EXCH_AGGRESSIVE > Id = 1

```

```

[1280@fw41] < FWIKE_PACKET_START > Id = 1
[1280@fw41] < FWIKE_AGG_PACKET_1 > Id = 1
[1280@fw41] AggCreatel: entering. ~~ Mon Apr 24 13:32:46 2000

[1280@fw41] get_strongest_method: chose encryption method 2
[1280@fw41] get_strongest_method: chose hash method 1
[1280@fw41] add_trans_to_list: adding e:2 h:1 a:1 g:2
[1280@fw41]

GetDHPrivExpLen: DH Exponent length is (300)

[1280@fw41] ~Association: efffe0e8 8e1c8
[1280@fw41] ResendOutbuf (12) (921668)
[1280@fw41] fwisakmpd_rcv_from_peer: entering
[1280@fw41] canonize_gw: Canonized ip is the same as original ip cf28e75a
[1280@fw41] MatchPeerCookieIMsgID: cf28e75a 7c349c0e8842bc96 00
[1280@fw41] MatchPeerCookieIMsgID: match found
[1280@fw41] < FWIKE_ROLE_INITIATOR > Id = 1
[1280@fw41] ike_initiator: entering
[1280@fw41] InitiatorOnEnter: idRanges USED mine [a0a0a00-a0a0aff] peer's [cf28e600-
cf28e6ff]
[1280@fw41] findSABByPeer: Valid ISAKMP SA was not found
[1280@fw41] < FWIKE_EXCH_AGGRESSIVE > Id = 1
[1280@fw41] < FWIKE_AGG_PACKET_2 > Id = 1
[1280@fw41] AggProcess2: entering ~~ Mon Apr 24 13:32:46 2000

[1280@fw41] encryption alg is: 1
[1280@fw41] hash alg is 2
[1280@fw41] auth mode is 1
[1280@fw41] expiry is +600
[1280@fw41] -- updatePayloadMap: received payload PA_SA.
[1280@fw41] -- updatePayloadMap: received payload PA_VENDORID.
[1280@fw41] -- updatePayloadMap: received payload PA_KEY.
[1280@fw41] -- updatePayloadMap: received payload PA_ID.
[1280@fw41] -- updatePayloadMap: received payload PA_NONCE.
[1280@fw41] -- updatePayloadMap: received payload PA_HASH.
[1280@fw41] AggProcess2: identifyPayloads succeeded.
[1280@fw41] processVendorIDPayload: Unknown vendor
[1280@fw41] processIDPayload: address is
[1280@fw41] < FWIKE_AGG_PACKET_2_PEERCERT > Id = 1
[1280@fw41] < FWIKE_AGG_PACKET_2_EPILOGUE > Id = 1
[1280@fw41] DhKey_genkey:
[1280@fw41] e4 e2 32 e7 b9 fa c0 af cc b8 17 db 85 a0 d2 c0 ce 8d 30 32
[1280@fw41] 44 fe 85 ac b6 20 f2 84 92 bd a3 fb 3d 8a 28 60 c2 e1 f7 99
[1280@fw41] b8 59 a6 a0 c7 8d 8b 89 ac f4 94 9f e0 83 00 b5 1b 1f e7 e9
[1280@fw41] bf 18 a6 22 2e cb bf c5 ae c8 7a 75 23 74 33 ed 42 d9 d1 99
[1280@fw41] c8 41 3a fa f9 64 16 32 27 01 f3 f1 a5 c3 f3 4e 85 e1 d5 a5
[1280@fw41] 3d 5b e7 f2 fb 15 72 93 71 07 e1 45 c0 04 7c c9 e2 05 e2 ac
[1280@fw41] 9d c6 9f 99 d7 ff ff 44
[1280@fw41] pre shared
[1280@fw41] 61 62 63 31 32 33
[1280@fw41] SKEYID:
[1280@fw41] e0 0a 0b 0d 2c dd 99 53 f5 5b c0 c3 32 c4 a6 cf c7 b7 49 55
[1280@fw41] SKEYID_D:
[1280@fw41] 62 f1 32 64 81 f7 53 58 67 fa 33 2d b2 08 2e e4 b8 4e 97 5d
[1280@fw41] SKEYID_A:
[1280@fw41] ec f4 7f e8 ac 29 1c 71 46 89 7b 12 52 4a a3 b8 a6 f3 04 92
[1280@fw41] SKEYID_E:
[1280@fw41] 2c 36 34 2b 4d 1f b2 32 3f cb 6d 94 35 a1 d5 1b 27 d5 1b 9d
[1280@fw41] ENCRYPTION KEY:
[1280@fw41] 2c 36 34 2b 4d 1f b2 32
[1280@fw41] IV:
[1280@fw41] fd fb a5 6e 4b 9a 36 2b
[1280@fw41] SA:
[1280@fw41] 00 00 00 01 00 00 00 01 00 00 00 2c 01 01 00 01 00 00 00 24
[1280@fw41] 01 01 00 00 80 01 00 01 80 02 00 02 80 03 00 01 80 04 00 02
[1280@fw41] 80 0b 00 01 00 0c 00 04 00 00 02 58
[1280@fw41] IDir_b:
[1280@fw41] 01 11 01 f4 cf 28 e7 5a
[1280@fw41] hash_R_phase1:

```

```

[1280@fw41] 89 8d d7 67 36 d3 04 19 ca e6 2c c8 1f 60 f5 b2 71 31 77 c3
[1280@fw41] < FWIKE_AGG_PACKET_3 > Id = 1
[1280@fw41] AggCreate3: entering ~~ Mon Apr 24 13:32:46 2000

[1280@fw41] hash_I_phase1:
[1280@fw41] 9a b2 04 cf 10 8b 76 6d 93 37 9a bf 82 c8 ec ad 79 bc 01 69
[1280@fw41] IkeSAFromState: cookieI: 7c349c0e8842bc96
[1280@fw41] SAstore: Isakmp sa expire time set to +600
[1280@fw41] SAstore: Isakmp sa reneg time set to +540
[1280@fw41] < FWIKE_PACKET_END > Id = 1
[1280@fw41] fwisakmpd_send_log: sending log message: Phase 1 (aggressive) completion.
DES/SHA1/Pre shared secrets
[1280@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 9211c0, len = 193, key = 0
[1280@fw41] ~Negotiation: efffe0 94aaa0
[1280@fw41] ~Association: 94aaa0 00
[1280@fw41] Neg's end
[1280@fw41] ResendOutbuf (3) (921668)
[1280@fw41] fwisakmpd_recv_from_peer: entering
[1280@fw41] fwisakmpd_recv_from_peer: Retransmission detected
[1280@fw41] comm_decrypt_buf: fd = 28, buf = 94cca8, len = 32, key = 0
[1280@fw41] comm_decrypt_buf: fd = 28, buf = 94cca8, len = 161, key = 0
[1280@fw41] simple_ISAKMP_log: log: Phase 1 (aggressive) completion. DES/SHA1/Pre shared
secrets
[1280@fw41] fwike_isakmpd_pipe_handler: called without data
[1280@fw41] RetransmitBuffer
[1280@fw41] ResendOutbuf (2) (921668)
[1280@fw41] RetransmitBuffer
[1280@fw41] ResendOutbuf (1) (921668)
[1280@fw41] RetransmitBuffer
[1280@fw41] ResendOutbuf (0) (921668)
[1280@fw41] ResendOutbuf: retrans counter is down to 0
[1280@fw41] DeleteNegotiation<1>: invoked(1): ptr 921668 peer:cf28e75a cookieI 7c349c0e
8842bc96 msgId 00 methods 2020100-00 SPIs 00 00
[1280@fw41] DeleteNegotiation: entering
[1280@fw41] CallAgain
[1280@fw41] RequestByMethods: used 1 my [a0a0a00-a0a0aff] peer [cf28e600-cf28e6ff]
[1280@fw41] Ass_MatchPeerMethodsIDs: cf28e75a 2020100:00 [a0a0a00-a0a0aff] [cf28e600-
cf28e6ff]
[1280@fw41] Ass_MatchPeerMethodsIDs: match has failed
[1280@fw41] MatchPeerMethodsIDs: cf28e75a 2020100:00 [a0a0a00-a0a0aff] [cf28e600-
cf28e6ff]
[1280@fw41] MatchPeerMethodsIDs: Not found
[1280@fw41] MatchPeerPlNeg: cf28e75a
[1280@fw41] MatchPeerPlNeg: no ongoing phase1 negotiations
[1280@fw41] *** AddNegotiation: ptr 94abd0 peer cf28e75a cookieI 00:00 msgID 00 methods
2020100 00 new count: 1
[1280@fw41] < FWIKE_ROLE_START > Id = 2
[1280@fw41] < FWIKE_ROLE_INITIATOR > Id = 2
[1280@fw41] ike_initiator: entering
[1280@fw41] InitiatorOnEnter: idRanges USED mine [a0a0a00-a0a0aff] peer's [cf28e600-
cf28e6ff]
[1280@fw41] findSAByPeer: ISAKMP SA was found
[1280@fw41] < FWIKE_EXCH_START > Id = 2
[1280@fw41] < FWIKE_EXCH_QUICK_MODE > Id = 2
[1280@fw41] < FWIKE_PACKET_START > Id = 2
[1280@fw41] < FWIKE_QM_PACKET_1 > Id = 2
[1280@fw41] QMCreatel: entering ~~ Mon Apr 24 13:32:47 2000

[1280@fw41] update_saexp_in_trans: expiration 3600 seconds
[1280@fw41] QMCreatel: rangeUsed: 1 my [a0a0a00-a0a0aff] peer [cf28e600-cf28e6ff]
[1280@fw41] RESULT: range_first a0a0a00 last a0a0aff subnet_addr a0a0a00 mask ffffffff00
[1280@fw41] RESULT: range_first cf28e600 last cf28e6ff subnet_addr cf28e600 mask ffffffff00
[1280@fw41] computeIV from:
[1280@fw41] fd fb a5 6e 4b 9a 36 2b
[1280@fw41] 0a 00 95 0c
[1280@fw41] P2 IV:
[1280@fw41] cc 4b 21 dc 86 ea e8 b3
[1280@fw41] ~Association: efffe140 8eclc8
[1280@fw41] ~Negotiation: 921668 92cac0
[1280@fw41] ~Association: 92cac0 00
[1280@fw41] Neg's end

```

```

[1280@fw41] ResendOutbuf (12) (94abd0)
[1280@fw41] fwisakmpd_recv_from_peer: entering
[1280@fw41] canonize_gw: Canonize ip is the same as original ip cf28e75a
[1280@fw41] MatchPeerCookieIMsgID: cf28e75a 7c349c0e8842bc96 a00950c
[1280@fw41] MatchPeerCookieIMsgID: match found
[1280@fw41] < FWIKE_ROLE_INITIATOR > Id = 2
[1280@fw41] ike_initiator: entering
[1280@fw41] InitiatorOnEnter: idRanges USED mine [a0a0a00-a0a0aff] peer's [cf28e600-
cf28e6ff]
[1280@fw41] findSAByPeer: ISAKMP SA was found
[1280@fw41] < FWIKE_EXCH_QUICK_MODE > Id = 2
[1280@fw41] < FWIKE_QM_PACKET_2 > Id = 2
[1280@fw41] QMProcess2: entering ~~ Mon Apr 24 13:32:47 2000

[1280@fw41] -- updatePayloadMap: received payload PA_HASH.
[1280@fw41] -- updatePayloadMap: received payload PA_SA.
[1280@fw41] -- updatePayloadMap: received payload PA_NONCE.
[1280@fw41] -- updatePayloadMap: received payload PA_ID.
[1280@fw41] -- updatePayloadMap: received payload PA_ID.
[1280@fw41] -- updatePayloadMap: received payload PA_NOTIFY.
[1280@fw41] QMProcess2: identifyPayloads succeeded.
[1280@fw41] processNotifyPayload: protocol: 3
[1280@fw41] < FWIKE_QM_PACKET_3 > Id = 2
[1280@fw41] QMCreate3: entering ~~ Mon Apr 24 13:32:47 2000

[1280@fw41] < FWIKE_PACKET_END > Id = 2
[1280@fw41] < FWIKE_EXCH_END > Id = 2
[1280@fw41] < FWIKE_ROLE_END > Id = 2
[1280@fw41] fwIsakmp_SAFFromNegCxt: initiator
[1280@fw41] ESP_SA_FromTransformList: HMAC alg: 1, HMAC keylen: 20
[1280@fw41] SPI: 3fbe2e05
[1280@fw41] DES KEY IS:
[1280@fw41] 84 aa ac 11 17 13 30 0e
[1280@fw41] HMAC KEY IS:
[1280@fw41] b7 0d ff 18 5c c3 1f 1e 5c b6 78 47 cc c6 31 71 41 11 b4 88
[1280@fw41] ESP_SA_FromTransformList: esp_expiretime for Initiator set to +3600
[1280@fw41] ESP_SA_FromTransformList: esp_expiretime for Initiator set to +3600
[1280@fw41] ESP_SA_FromTransformList: esp_renegtime set to +3563
[1280@fw41] ESP_SA_FromTransformList: HMAC alg: 1, HMAC keylen: 20
[1280@fw41] SPI: 489e9672
[1280@fw41] DES KEY IS:
[1280@fw41] b8 ea de 9d 64 15 43 2d
[1280@fw41] HMAC KEY IS:
[1280@fw41] 05 c2 d2 38 5f 4e 49 7d 0a da de e8 03 ed 3e ec 83 6a 30 37
[1280@fw41] ESP_SA_FromTransformList: esp_expiretime for Responder set to +3600
[1280@fw41] ESP_SA_FromTransformList: esp_expiretime for Responder set to +3600
[1280@fw41] ESP_SA_FromTransformList: esp_renegtime set to +3552
[1280@fw41] # of negotiations: 1
[1280@fw41] # of negs: 1
[1280@fw41] Neg: 0 ptr: 94abd0 ass: 94bc98 wait4: 00
msgId: a00950c method: 2020100;00 cookie: 7c349c0e8842bc96
req type: 1 SPIs: 00 00
[1280@fw41] # of waiting negotiations: 0
[1280@fw41] # of negs: 0
[1280@fw41] ** AssHTabs_AddAssTo: ass 948f40 peer cf28e75a cookie 7c349c0e8842bc96 msgid:
a00950c
[1280@fw41] AssHTabs_AddAssTo table b4 insertion:

[1280@fw41] AssHTabs_printall:
[1280@fw41] AssHTabs_AddAssTo after insertion:

[1280@fw41] AssHTabs_printall:
[1280@fw41] 0 ass 948f40 keyptr 8ecla0 methods 2020100:00counter 00:02 NOT gonna exp

[1280@fw41] AssHTabs_AddAssTo: ass: 948f40 8ecla0 cf28e75a
[1280@fw41] AssHTabs_AddAssTo: insertion has succeeded
[1280@fw41] ~Negotoation: efffe0 948018
[1280@fw41] ~Association: 948018 00
[1280@fw41] Neg's end
[1280@fw41] ResendOutbuf (3) (94abd0)
[1280@fw41] ReplyBy: entering

```

```

[1280@fw41] fwasync_connbuf_realloc: reallocating 9211c0 from 1181 to 5188
[1280@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 92cac0, len = 4164, key = 0
[1280@fw41] fwisakmpd_recv_from_peer: entering
[1280@fw41] fwisakmpd_recv_from_peer: Retransmission detected
[1280@fw41] fwike_isakmpd_pipe_handler: called without data
[1280@fw41] comm_decrypt_buf: fd = 28, buf = 94cca8, len = 32, key = 0
[1280@fw41] fwasync_connbuf_realloc: reallocating 94cca8 from 1056 to 5156
[1280@fw41] comm_decrypt_buf: fd = 28, buf = 9670c0, len = 4132, key = 0
[1280@fw41] fwisakmp_recv_sa_by_methods: received answer to methods request
[1280@fw41] get_userc_entry: no user entry for ip 207.40.230.0
[1280@fw41] fwisakmp_store_sa_in_tables:
[1280@fw41] myRange [a0a0a00-a0a0aff] peerRange [cf28e600-cf28e6ff]
[1280@fw41] delay writing to ISAKMP_ESP_table
[1280@fw41] fw_dtab_record_conn: vals=<a0a0a0a,41c,cf28e681,15,6;6018ac64,3,ffffd010>
[1280@fw41] fwisakmp_recv_sa_by_methods: delay is 300
[1280@fw41] fwisakmp_getmethod: Combined ESP: DES + SHA1
[1280@fw41] add_qm_ids: rangeUsed 1 [a0a0a00-a0a0aff] [cf28e600-cf28e6ff]
[1280@fw41] RESULT: range_first a0a0a00 last a0a0aff subnet_addr a0a0a00 mask ffffffff00
[1280@fw41] RESULT: range_first cf28e600 last cf28e6ff subnet_addr cf28e600 mask ffffffff00
[1280@fw41] fwcrypt_log: sending log op 16
[1280@fw41] proxy xlate input: src a0a0a0a sport 41c dst cf28e681 dport 15
[1280@fw41] fwisakmp_getmethod: Combined ESP: DES + SHA1
[1280@fw41] fwcrypt_log: sending log op 3
[1280@fw41] fwisakmp_recv_sa_by_methods: Isakmp trap success
[1280@fw41] RetransmitBuffer
[1280@fw41] ResendOutbuf (2) (94abd0)
[1280@fw41] fwisakmpd_recv_from_peer: entering
[1280@fw41] canonize_gw: Canonized ip is the same as original ip cf28e75a
[1280@fw41] MatchPeerCookieIMsgID: cf28e75a 7c349c0e8842bc96 00
[1280@fw41] MatchPeerCookieIMsgID: match failed
[1280@fw41] *** AddNegotiation: ptr 9211c0 peer cf28e75a cookieI 7c349c0e:8842bc96 msgID
7de8c798 methods 00 00 new count: 2
[1280@fw41] < FWIKE_ROLE_START > Id = 3
[1280@fw41] < FWIKE_ROLE_RESPONDER > Id = 3
[1280@fw41] FwIkeResponder: entering
[1280@fw41] FwIkeResponderOnEnter: idRanges NOT USED mine [0-0] peer's [0-0]
[1280@fw41] findSAByPeer: ISAKMP SA was found
[1280@fw41] < FWIKE_EXCH_START > Id = 3
[1280@fw41] < FWIKE_EXCH_INFORMATION > Id = 3
[1280@fw41] < FWIKE_PACKET_START > Id = 3
[1280@fw41] < FWIKE_INFO_RESPONDER > Id = 3
[1280@fw41] fwIsakmp_ProcessInfoExc p2: entering
[1280@fw41] computeIV from:
[1280@fw41] fd fb a5 6e 4b 9a 36 2b
[1280@fw41] 7d e8 c7 98
[1280@fw41] -- updatePayloadMap: received payload PA_HASH.
[1280@fw41] -- updatePayloadMap: received payload PA_NOTIFY.
[1280@fw41] ProcessInfo: identifyPayloads succeeded.
[1280@fw41] processNotifyPayload: protocol: 1
[1280@fw41] Peer cf28e75a says: payload malformed
[1280@fw41] fwisakmpd_send_log: sending log message: Received Notification from Peer:
payload malformed
[1280@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 92cac0, len = 183, key = 0
[1280@fw41] < FWIKE_PACKET_END > Id = 3
[1280@fw41] < FWIKE_EXCH_END > Id = 3
[1280@fw41] < FWIKE_ROLE_END > Id = 3
[1280@fw41] sndrcv: got Notification from peer
[1280@fw41] DeleteNegotiation<1>: invoked(1): ptr 9211c0 peer:cf28e75a cookieI 7c349c0e
8842bc96 msgId 7de8c798 methods 00-00 SPIs 00 00
[1280@fw41] DeleteNegotiation: entering
[1280@fw41] ~Negotiation: 9211c0 92df10
[1280@fw41] ~Association: 92df10 00
[1280@fw41] Neg's end
[1280@fw41] ~Negotiation: effefa0 948018
[1280@fw41] ~Association: 948018 00
[1280@fw41] Neg's end
[1280@fw41] fwisakmpd_recv_from_peer: entering
[1280@fw41] fwisakmpd_recv_from_peer: Retransmission detected
[1280@fw41] fwike_isakmpd_pipe_handler: called without data
[1280@fw41] comm_decrypt_buf: fd = 28, buf = 9670c0, len = 32, key = 0
[1280@fw41] comm_decrypt_buf: fd = 28, buf = 9670c0, len = 151, key = 0

```

```

[ fwd@fw41 ] simple_ISAKMP_log: log: Received Notification from Peer: payload malformed
[1280@fw41] RetransmitBuffer
[1280@fw41] ResendOutbuf (1) (94abd0)
[1280@fw41] fwisakmpd_rcv_from_peer: entering
[1280@fw41] canonize_gw: Canonized ip is the same as original ip cf28e75a
[1280@fw41] MatchPeerCookieIMsgID: cf28e75a 7c349c0e8842bc96 00
[1280@fw41] MatchPeerCookieIMsgID: match failed
[1280@fw41] *** AddNegotiation: ptr 9211c0 peer cf28e75a cookieI 7c349c0e:8842bc96 msgID
710de5ac methods 00 00 new count: 2
[1280@fw41] < FWIKE_ROLE_START > Id = 4
[1280@fw41] < FWIKE_ROLE_RESPONDER > Id = 4
[1280@fw41] FwIkeResponder: entering
[1280@fw41] FwIkeResponderOnEnter: idRanges NOT USED mine [0-0] peer's [0-0]
[1280@fw41] findSAByPeer: ISAKMP SA was found
[1280@fw41] < FWIKE_EXCH_START > Id = 4
[1280@fw41] < FWIKE_EXCH_INFORMATION > Id = 4
[1280@fw41] < FWIKE_PACKET_START > Id = 4
[1280@fw41] < FWIKE_INFO_RESPONDER > Id = 4
[1280@fw41] fwIsakmp_ProcessInfoExc p2: entering
[1280@fw41] computeIV from:
[1280@fw41] fd fb a5 6e 4b 9a 36 2b
[1280@fw41] 71 0d e5 ac
[1280@fw41] -- updatePayloadMap: received payload PA_HASH.
[1280@fw41] -- updatePayloadMap: received payload PA_NOTIFY.
[1280@fw41] ProcessInfo: identifyPayloads succeeded.
[1280@fw41] processNotifyPayload: protocol: 1
[1280@fw41] Peer cf28e75a says: payload malformed
[1280@fw41] fwisakmpd_send_log: sending log message: Received Notification from Peer:
payload malformed
[1280@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 92cac0, len = 183, key = 0
[1280@fw41] < FWIKE_PACKET_END > Id = 4
[1280@fw41] < FWIKE_EXCH_END > Id = 4
[1280@fw41] < FWIKE_ROLE_END > Id = 4
[1280@fw41] sndrcv: got Notification from peer
[1280@fw41] DeleteNegotiation<1>: invoked(1): ptr 9211c0 peer:cf28e75a cookieI 7c349c0e
8842bc96 msgId 710de5ac methods 00-00 SPIs 00 00
[1280@fw41] DeleteNegotiation: entering
[1280@fw41] ~Negotiation: 9211c0 92df10
[1280@fw41] ~Association: 92df10 00
[1280@fw41] Neg's end
[1280@fw41] ~Negotiation: efffe0 948018
[1280@fw41] ~Association: 948018 00
[1280@fw41] Neg's end
[1280@fw41] fwisakmpd_rcv_from_peer: entering
[1280@fw41] fwisakmpd_rcv_from_peer: Retransmission detected
[ fwd@fw41 ] comm_decrypt_buf: fd = 28, buf = 9670c0, len = 32, key = 0
[ fwd@fw41 ] comm_decrypt_buf: fd = 28, buf = 9670c0, len = 151, key = 0
[ fwd@fw41 ] simple_ISAKMP_log: log: Received Notification from Peer: payload malformed
[1280@fw41] fwike_isakmpd_pipe_handler: called without data
[1280@fw41] RetransmitBuffer
[1280@fw41] ResendOutbuf (0) (94abd0)
[1280@fw41] ResendOutbuf: retrans counter is down to 0
[1280@fw41] DeleteNegotiation<1>: invoked(1): ptr 94abd0 peer:cf28e75a cookieI 7c349c0e
8842bc96 msgId a00950c methods 2020100-00 SPIs 00 00
[1280@fw41] DeleteNegotiation: entering
[1280@fw41] ~Negotiation: 94abd0 94bc98
[1280@fw41] ~Association: 94bc98 00
[1280@fw41] Neg's end
[ fwd@fw41 ] ISAKMP_ESP_table <cf28e75a,2020100,a0a0a00,a0a0aff,cf28e600,cf28e6ff;6012201c>
[ fwd@fw41 ] fwisakmp_sendhold: (2043)

```

Output from PIX debug crypto ipsec/isakmp commands

```
crypto_isakmp_process_block: src 207.40.231.82, dest 207.40.231.90
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      auth pre-share
ISAKMP:      default group 2
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of 0x0 0x0 0x2 0x58
ISAKMP (0): atts are acceptable. Next payload is 0
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 207.40.231.82, dest 207.40.231.90
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 207.40.231.82, dest 207.40.231.90
crypto_isakmp_process_block: src 207.40.231.82, dest 207.40.231.90
crypto_isakmp_process_block: src 207.40.231.82, dest 207.40.231.90
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = -414322444

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of 0x0 0x0 0xe 0x10
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
      (key eng. msg.) dest= 207.40.231.90, src= 207.40.231.82,
      dest_proxy= 207.40.230.0/255.255.255.0/0/0 (type=4),
      src_proxy= 10.10.10.0/255.255.255.0/0/0 (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 = -414322444

ISAKMP (0): processing ID payload. message ID = -414322444
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.10.10.0/255.255.255.0 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = -414322444
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 207.40.230.0/255.255.255.0 prot 0 port 0
0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x64e54c6a(1692748906) for SA
      from 207.40.231.82 to 207.40.231.90 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 207.40.231.82, dest 207.40.231.90
OAK_QM exchange
```

```
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITIPSEC(map_alloc_entry): allocating entry 4

IPSEC(map_alloc_entry): allocating entry 3

ISAKMP (0): Creating IPsec SAs
  inbound SA from 207.40.231.82 to 207.40.231.90 (proxy 10.10.10.0 to
207.40.230.0)
  has spi 1692748906 and conn_id 4 and flags 4
  lifetime of 3600 seconds
  outbound SA from 207.40.231.90 to 207.40.231.82 (proxy 207.40.230.0 to
10.10.10.0)
  has spi 1625222624 and conn_id 3 and flags 4
  lifetime of 3600 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 207.40.231.90, src= 207.40.231.82,
  dest_proxy= 207.40.230.0/255.255.255.0/0/0 (type=4),
  src_proxy= 10.10.10.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-sha-hmac ,
  lifedur= 3600s and 0kb,
  spi= 0x64e54c6a(1692748906), conn_id= 4, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 207.40.231.90, dest= 207.40.231.82,
  src_proxy= 207.40.230.0/255.255.255.0/0/0 (type=4),
  dest_proxy= 10.10.10.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-sha-hmac ,
  lifedur= 3600s and 0kb,
  spi= 0x60deede0(1625222624), conn_id= 3, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR
```