



CHECK POINT™
Software Technologies Ltd.

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

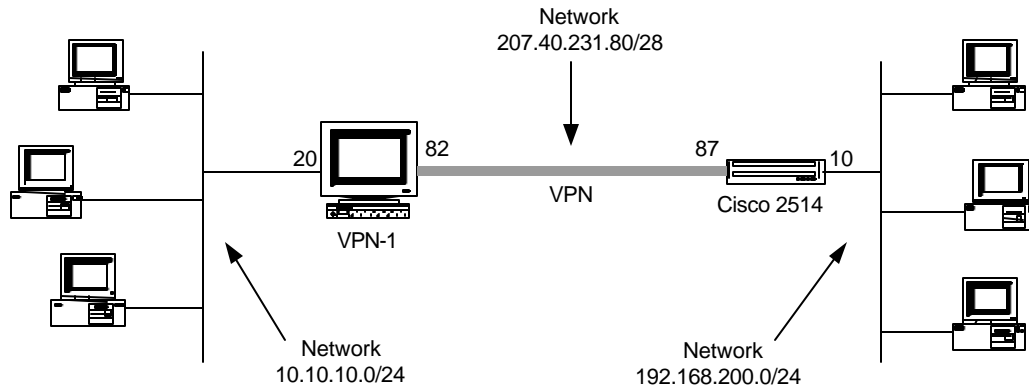
Authored By: David Dietrich
Date: July 10, 2000
Purpose: To describe and document how to configure IKE VPN's with Cisco IOS
Version: 1.0

Table of Contents

Overview.....	2
Configuring VPN-1 objects and rules	2
IOS Configuration	8
Tips and Troubleshooting.....	9
Reference information.....	10
Complete router IOS config file for the simple gateway to gateway VPN example	10
Output from fwd -d during successful VPN traverse (quite verbose):.....	12
Output from IOS debug crypto ipsec/isakmp/engine commands.....	17

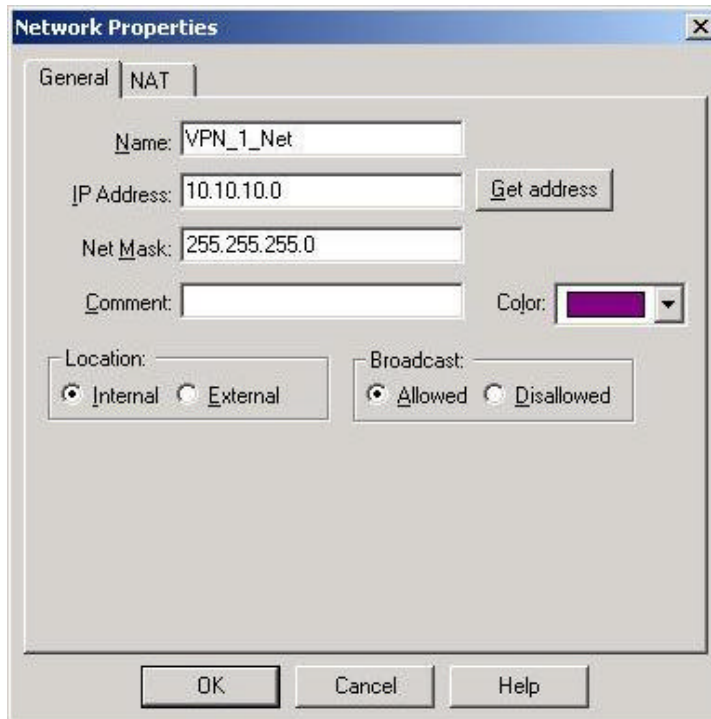
Overview

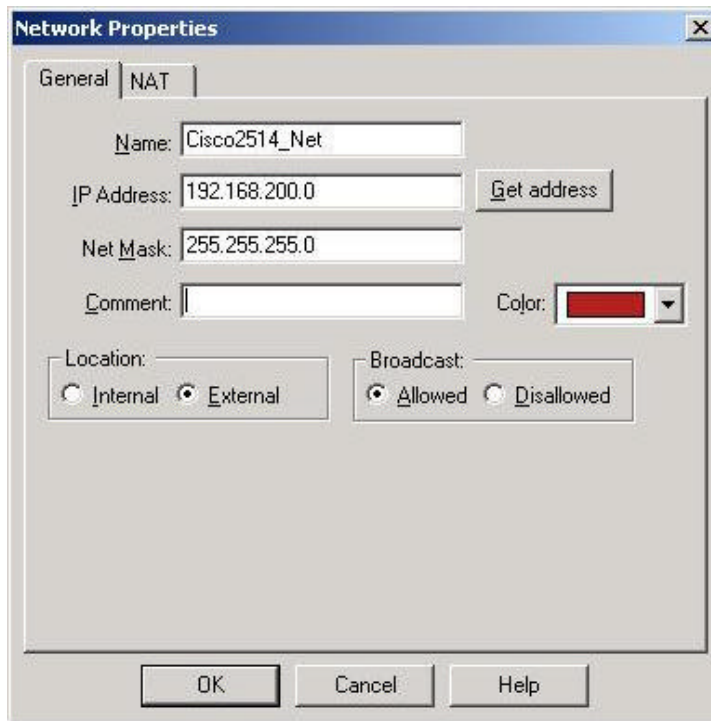
This document describes a simple IPSEC vpn configuration between a VPN-1 gateway, version 4.1 SP1 and a Cisco router with IOS version 12.0.9. The authentication method used will be shared secrets. This configuration will describe a simple vpn per the following network diagram:



Configuring VPN-1 objects and rules

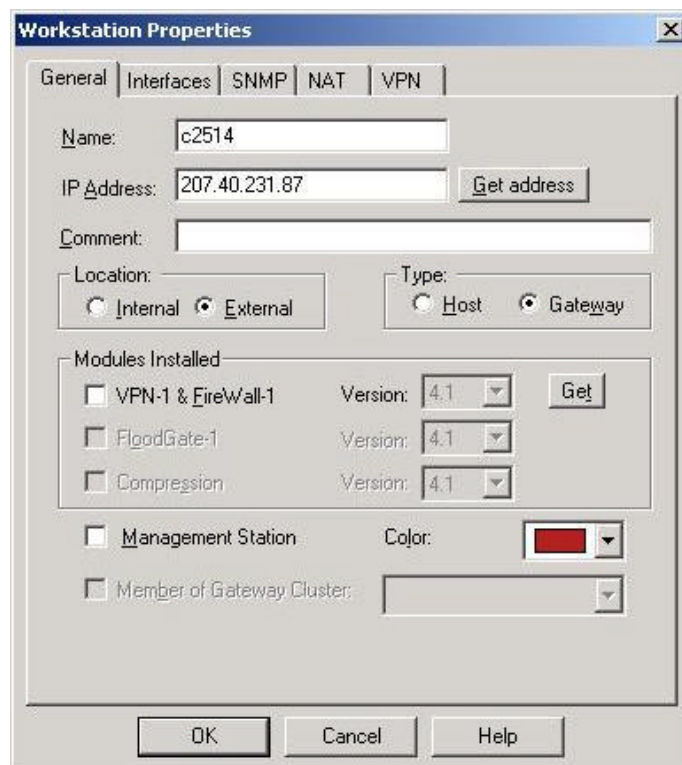
Create network objects to represent the traffic that the VPN-1 gateway and the router will encrypt. In this example, this will be the two networks behind the VPN-1 gateway and the router.



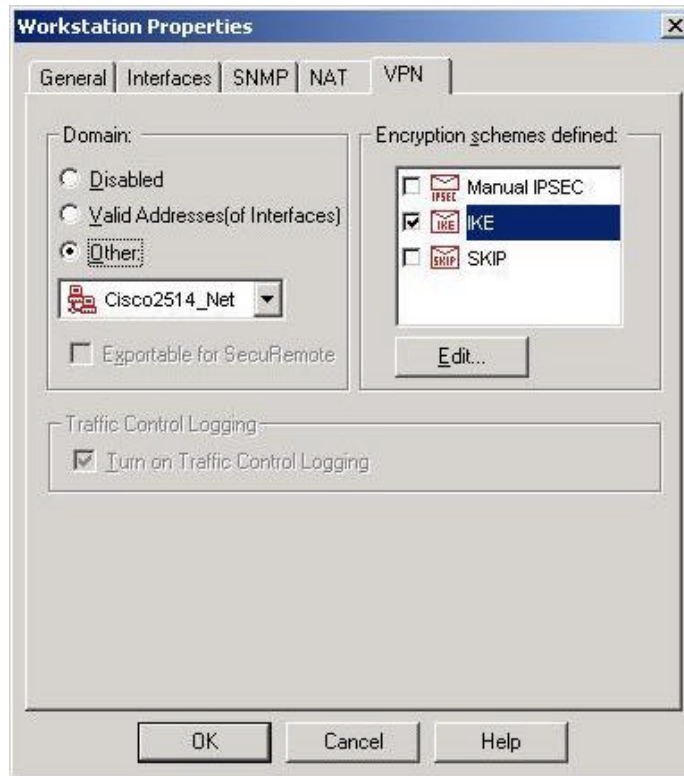


Create a workstation object for the router

In the general tab, select location External and type Gateway



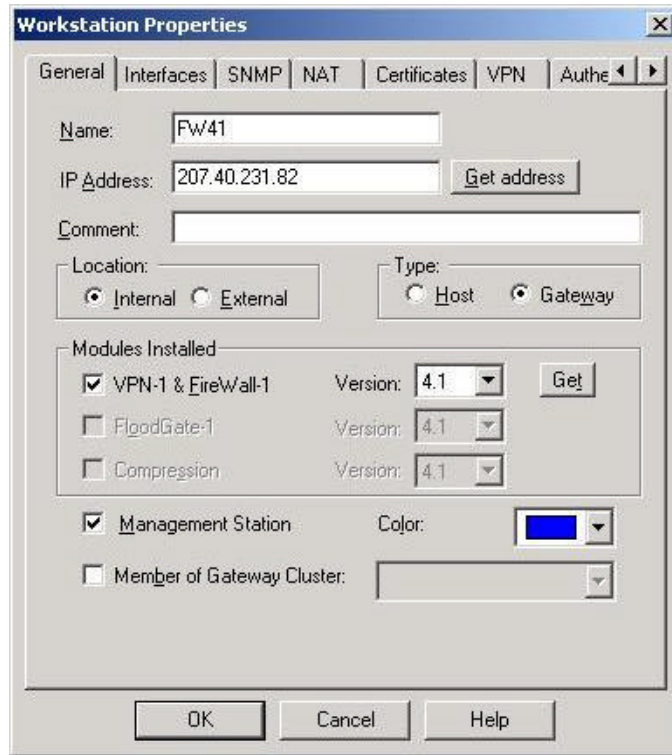
In the VPN tab identify the router's network object as the encryption domain, on the left. On the right, select IKE as the scheme. After selecting IKE, select the Edit button...



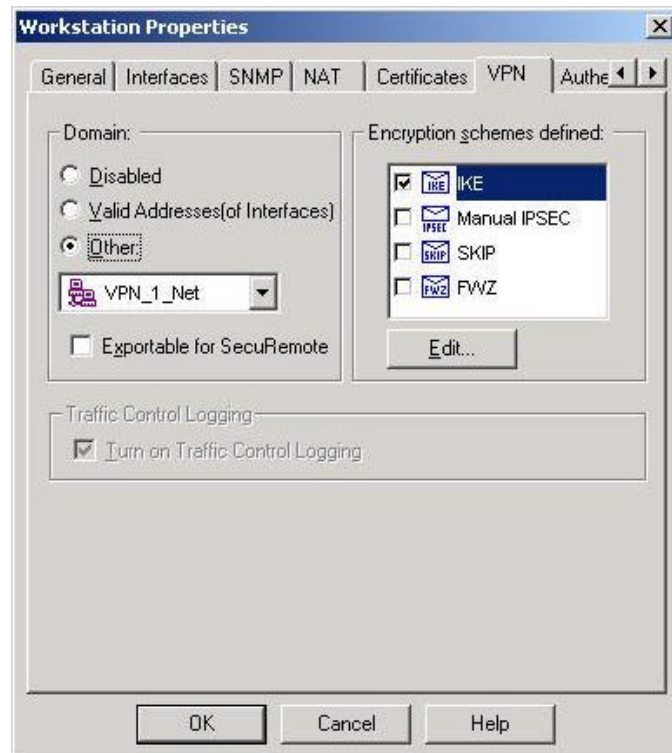
In the IKE Properties, select the methods you intend to use for IKE security association negotiations. In this example we'll use DES encryption and SHA hash algorithm. Check Aggressive Mode and Subnet support as well. Note: 3DES is a better encryption method, of course. The lab IOS version we had was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



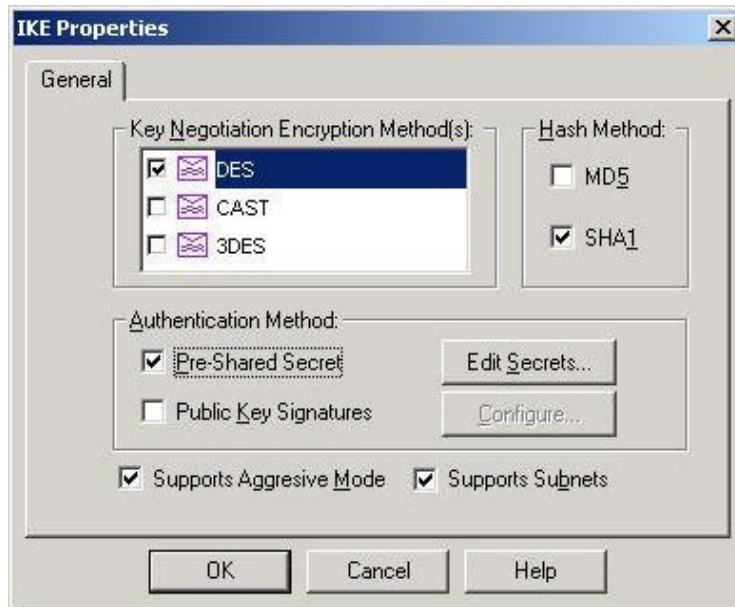
Create a workstation object for the VPN-1 gateway



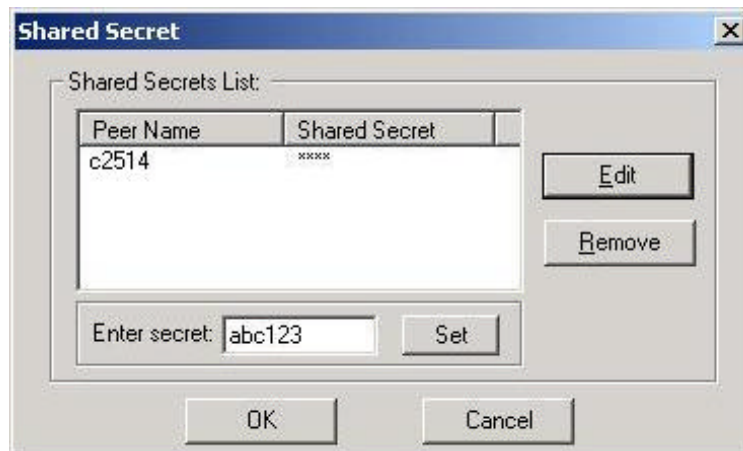
In the VPN tab identify the VPN-1 gateway's network object as the encryption Domain, on the left. On the right, select IKE as the scheme. After selecting IKE, select the Edit button...



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.



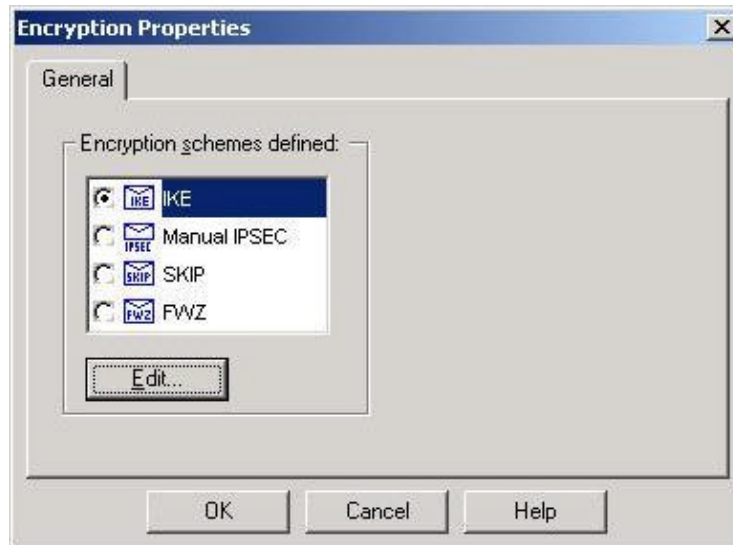
Create the encryption rule in the VPN-1 Policy editor

In this example, we're encrypting all traffic between the protected networks. Right click on the Encrypt Action and edit Encryption Properties....

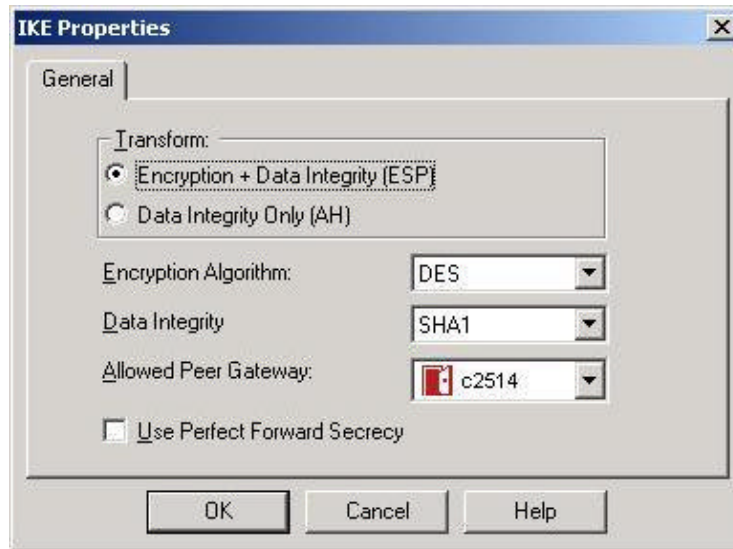


Right click on Encrypt, edit encryption properties

Select IKE. Then select Edit and continue...



Select the appropriate properties. The selected algorithms will match the transform defined later on the router. These properties pertain to Phase 2 negotiation establishing IPSEC security association. In this example, Perfect Forward Secrecy is not used.



IOS 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. First we'll show the specific commands for the vpn configuration with some discussion. A listing of the full config we used will follow.

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.

```
access-list 101 permit ip 192.168.200.0 0.0.0.255 10.10.10.0 0.0.0.255  
access-list 101 permit ip 10.10.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

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. NOTE: When default values are used the config commands will not display in the config file. In this example, the encryption and hash are default values (des-sha).

```
crypto isakmp policy 10  
authentication pre-share  
encryption des  
hash sha
```

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

group 2

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

```
crypto isakmp key abc123 address 207.40.231.82
```

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 testset 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
 set peer 207.40.231.82
 set transform-set testset
 match address 101
```

Apply the crypto map set to the interface through which IPsec traffic will flow. Applying the crypto map set to an interface instructs the router 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.

```
interface Ethernet0
 crypto map testmap
```

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.

Tips and Troubleshooting

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

Router:

```
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 IOS during the negotiations can be useful.

Router:

```
debug crypto ipsec  
debug crypto engine  
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 router IOS config file for the simple gateway to gateway VPN example

```
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
service udp-small-servers  
service tcp-small-servers  
!  
hostname Router  
!  
enable password *****  
!  
ip subnet-zero  
!  
!
```

```

crypto isakmp policy 10
  authentication pre-share
  group 2
  lifetime 3600
crypto isakmp key abc123 address 207.40.231.82
!
!
crypto ipsec transform-set testset esp-des esp-sha-hmac
!
!
crypto map testmap 10 ipsec-isakmp
  set peer 207.40.231.82
  set transform-set testset
  match address 101
!
!
interface Ethernet0
  ip address 207.40.231.87 255.255.255.240
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
  crypto map testmap
!
interface Ethernet1
  ip address 192.168.200.10 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
!
interface Serial0
  no ip address
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
  shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 207.40.231.82
!
access-list 101 permit ip 192.168.200.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 101 permit ip 10.10.10.0 0.0.0.255 192.168.200.0 0.0.0.255
!
line con 0
  transport input none
line aux 0
  transport input all
line vty 0 4
  password cisco
  login
end

```

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

```
[fwd@fw41] ==> fw_encrypt_invoke: scheme is ISAKMP
[fwd@fw41] fw_encrypt_invoke: pckid=5d9d2 entry=0 conn=<a0a0a0a,3,a0a0a14,0,1> arg=800
[fwd@fw41] fw_encrypt_invoke: ifid=1, 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: gateway connected to both endpoints
[fwd@fw41] allow_encryption: table=accepted, vals=<a0a0a0a,3,a0a0a14,0,1>
[fwd@fw41] fw_dtab_record_conn: vals=<a0a0a0a,3,a0a0a14,0,1;0,1,ffffd004>
[fwd@fw41] allow_encryption: sending packet id 5d9d2
[fwd@fw41] fwcrypt_log: protocol reason : gateway connected to both endpoints
[fwd@fw41] fwcrypt_log: sending log op 2
[fwd@fw41] ==> fw_encrypt_invoke: scheme is ISAKMP
[fwd@fw41] fw_encrypt_invoke: pckid=5d9d5 entry=0 conn=<a0a0a14,3,a0a0a0a,0,1> arg=0
[fwd@fw41] fw_encrypt_invoke: ifid=1, rule=3
[fwd@fw41] fw_encrypt_invoke: xlatesrc=0, xlatedst=0
[fwd@fw41] fw_encrypt_invoke: xlatesport=0, xlatedport=3b5c
[fwd@fw41] fw_encrypt_invoke: gateway connected to both endpoints
[fwd@fw41] allow_encryption: table=accepted, vals=<a0a0a14,3,a0a0a0a,0,1>
[fwd@fw41] fw_dtab_record_conn: vals=<a0a0a14,3,a0a0a0a,0,1;0,1,ffffd004>
[fwd@fw41] allow_encryption: sending packet id 5d9d5
[fwd@fw41] fwcrypt_log: protocol reason : gateway connected to both endpoints
[fwd@fw41] fwcrypt_log: sending log op 2
[fwd@fw41] ==> fw_encrypt_invoke: scheme is ISAKMP
[fwd@fw41] fw_encrypt_invoke: pckid=5da04 entry=503 conn=<a0a0a0a,1038,c0a8c814,21,6>
arg=0
[fwd@fw41] fw_encrypt_invoke: ifid=1, 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 ffffff00
addrRange.first a0a0a00 addrRange.last a0a0aff
[fwd@fw41] get_range_from_domain: entering
[fwd@fw41] get_range_from_domain: NET addr c0a8c814 net_ip c0a8c800 net_mask ffffff00
addrRange.first c0a8c800 addrRange.last c0a8c8ff
[fwd@fw41] set_possible_ranges: rangeUsed: 1 selfRange a0a0a00-a0a0aff otherRange
c0a8c800-c0a8c8ff
[fwd@fw41] fwipsec_invoke: sending request by methods 2 2 1 0 0 cf28e757
[fwd@fw41] fwasync_connbuf_realloc: reallocating 0 from 0 to 1428
[fwd@fw41] fwcomm_encrypt_inplace: fd = 29, buf = 96bc38, len = 404, key = 0
[17104@fw41] comm_decrypt_buf: fd = 0, buf = 8f2538, len = 32, key = 0
[17104@fw41] comm_decrypt_buf: fd = 0, buf = 8f2538, len = 372, key = 0
[17104@fw41] canonize_gw: Canonized ip is the same as original ip cf28e757
[17104@fw41] RequestByMethods: used 1 my [a0a0a00-a0a0aff] peer [c0a8c800-c0a8c8ff]
[17104@fw41] Ass_MatchPeerMethodsIDs: cf28e757 2020100:00 [a0a0a00-a0a0aff] [c0a8c800-
c0a8c8ff]
[17104@fw41] Ass_MatchPeerMethodsIDs: match has failed
[17104@fw41] MatchPeerMethodsIDs: cf28e757 2020100:00 [a0a0a00-a0a0aff] [c0a8c800-
c0a8c8ff]
[17104@fw41] MatchPeerMethodsIDs: Not found
[17104@fw41] MatchPeerPlNeg: cf28e757
[17104@fw41] MatchPeerPlNeg: no ongoing phasel negotiations
[17104@fw41] *** AddNegotiation: ptr 935b88 peer cf28e757 cookieI 00:00 msgID 00 methods
2020100 00 new count: 1
[fwd@fw41] fwike_fwd_pipe_handler: called without data
[17104@fw41] < FWIKE_ROLE_START > Id = 1
[17104@fw41] < FWIKE_ROLE_INITIATOR > Id = 1
[17104@fw41] ike_initiator: entering
[17104@fw41] InitiatorOnEnter: idRanges USED mine [a0a0a00-a0a0aff] peer's [c0a8c800-
c0a8c8ff]
[17104@fw41] findSAByPeer: Valid ISAKMP SA was not found
[17104@fw41] < FWIKE_EXCH_START > Id = 1
[17104@fw41] < FWIKE_EXCH_AGGRESSIVE > Id = 1
```

```

[17104@fw41] < FWIKE_PACKET_START > Id = 1
[17104@fw41] < FWIKE_AGG_PACKET_1 > Id = 1
[17104@fw41] AggCreatel: entering. ~~ Wed Jul 5 12:23:15 2000

[17104@fw41] get_strongest_method: chose encryption method 2
[17104@fw41] get_strongest_method: chose hash method 1
[17104@fw41] add_trans_to_list: adding e:2 h:1 a:1 g:2
[17104@fw41]

GetDHPrivExpLen: DH Exponent length is (300)

[17104@fw41] ~Association: efffe998 8ea708
[17104@fw41] ResendOutbuf (12) (935b88)
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (11) (935b88)
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (10) (935b88)
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (9) (935b88)
[17104@fw41] fwisakmpd_rcv_from_peer: entering
[17104@fw41] canonize_gw: Canonized ip is the same as original ip cf28e757
[17104@fw41] MatchPeerCookieIMsgID: cf28e757 a52895de8e502ae0 00
[17104@fw41] MatchPeerCookieIMsgID: match found
[17104@fw41] < FWIKE_ROLE_INITIATOR > Id = 1
[17104@fw41] ike_initiator: entering
[17104@fw41] InitiatorOnEnter: idRanges USED mine [a0a0a00-a0a0aff] peer's [c0a8c800-c0a8c8ff]
[17104@fw41] findsABByPeer: Valid ISAKMP SA was not found
[17104@fw41] < FWIKE_EXCH_AGGRESSIVE > Id = 1
[17104@fw41] < FWIKE_AGG_PACKET_2 > Id = 1
[17104@fw41] AggProcess2: entering ~~ Wed Jul 5 12:23:22 2000

[17104@fw41] encryption alg is: 1
[17104@fw41] hash alg is 2
[17104@fw41] auth mode is 1
[17104@fw41] expiry is +300
[17104@fw41] -- updatePayloadMap: received payload PA_SA.
[17104@fw41] -- updatePayloadMap: received payload PA_VENDORID.
[17104@fw41] -- updatePayloadMap: received payload PA_KEY.
[17104@fw41] -- updatePayloadMap: received payload PA_ID.
[17104@fw41] -- updatePayloadMap: received payload PA_NONCE.
[17104@fw41] -- updatePayloadMap: received payload PA_HASH.
[17104@fw41] AggProcess2: identifyPayloads succeeded.
[17104@fw41] processVendorIDPayload: Unknown vendor
[17104@fw41] processIDPayload: address is
[17104@fw41] < FWIKE_AGG_PACKET_2_PEERCERT > Id = 1
[17104@fw41] < FWIKE_AGG_PACKET_2_EPILOGUE > Id = 1
[17104@fw41] DhKey_genkey:
[17104@fw41] 6c 15 6c d1 01 35 04 4f 9f fa 7b 35 8d 80 d6 d0 13 c4 74 c9
[17104@fw41] 21 47 ee 0e c4 77 ce b6 5b 00 bd 84 be 75 c2 bd 86 1c c6 3e
[17104@fw41] 0a 5e 6b fc 46 5b de ef 7b c0 b8 fd 78 a1 3b 7d ac 3e e2 5a
[17104@fw41] 4c 94 ff 08 d7 0a 4a 40 ea 70 fd 12 ed cb 70 ee 10 44 29 a8
[17104@fw41] f6 fa 14 d4 0c 52 85 12 8d c6 9c 7e 61 2c b9 7c 3c b2 c1 10
[17104@fw41] 9a b0 23 89 34 38 94 19 86 df 99 d9 88 6c 19 c2 23 11 7a 36
[17104@fw41] ef a6 96 6f fc 10 39 0a
[17104@fw41] pre shared
[17104@fw41] 61 62 63 31 32 33
[17104@fw41] SKEYID:
[17104@fw41] 2d f9 d1 5c ee 61 7c ab cf 54 5a 56 fe 56 13 d5 c6 08 45 3e
[17104@fw41] SKEYID_D:
[17104@fw41] eb f7 1c 6d 6d 24 18 9e 98 28 b8 d7 7d b1 e9 c6 c3 dc 04 da
[17104@fw41] SKEYID_A:
[17104@fw41] 9f 7a c1 31 cf e1 e3 6d 8d 28 25 57 8a 1d 17 7a a2 69 3b 41
[17104@fw41] SKEYID_E:
[17104@fw41] 69 f1 68 4f 8f 73 0d b1 42 13 c3 75 a7 94 27 ff 3b 38 2c 12
[17104@fw41] ENCRYPTION KEY:
[17104@fw41] 69 f1 68 4f 8f 73 0d b1
[17104@fw41] IV:
[17104@fw41] 44 c0 26 b5 0b c7 b1 09
[17104@fw41] SA:

```

```

[17104@fw41] 00 00 00 01 00 00 00 01 00 00 00 2c 01 01 00 01 00 00 00 24
[17104@fw41] 01 01 00 00 80 01 00 01 80 02 00 02 80 03 00 01 80 04 00 02
[17104@fw41] 80 0b 00 01 00 0c 00 04 00 00 01 2c
[17104@fw41] IDir_b:
[17104@fw41] 01 11 01 f4 cf 28 e7 57
[17104@fw41] hash_R_phase1:
[17104@fw41] 1b 28 7b 6e 6d af d7 e9 67 dd 15 7b 63 eb f8 56 8a 11 6f 62
[17104@fw41] < FWIKE_AGG_PACKET_3 > Id = 1
[17104@fw41] AggCreate3: entering ~~ Wed Jul 5 12:23:22 2000

[17104@fw41] hash_I_phase1:
[17104@fw41] 48 8f 9f 20 8a 5d 73 d6 d4 09 74 e0 9b 14 5d 5d 01 70 6f 95
[17104@fw41] IkeSAFromState: cookieI: a52895de8e502ae0
[17104@fw41] SASTore: Isakmp sa expire time set to +300
[17104@fw41] SASTore: Isakmp sa reneg time set to +240
[17104@fw41] < FWIKE_PACKET_END > Id = 1
[17104@fw41] fwisakmpd_send_log: sending log message: Phase 1 (aggressive) completion.
DES/SHA1/Pre shared secrets
[17104@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 9356e0, len = 193, key = 0
[17104@fw41] ~Negotiation: effff850 953188
[17104@fw41] ~Association: 953188 00
[17104@fw41] Neg's end
[17104@fw41] ResendOutbuf (3) (935b88)
[17104@fw41] comm_decrypt_buf: fd = 29, buf = 951b48, len = 32, key = 0
[17104@fw41] comm_decrypt_buf: fd = 29, buf = 951b48, len = 161, key = 0
[17104@fw41] simple_ISAKMP_log: log: Phase 1 (aggressive) completion. DES/SHA1/Pre shared
secrets
[17104@fw41] fwike_isakmpd_pipe_handler: called without data
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (2) (935b88)
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (1) (935b88)
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (0) (935b88)
[17104@fw41] ResendOutbuf: retrans counter is down to 0
[17104@fw41] DeleteNegotiation<1>: invoked(1): ptr 935b88 peer:cf28e757 cookieI a52895de
8e502ae0 msgId 00 methods 2020100-00 SPIs 00 00
[17104@fw41] DeleteNegotiation: entering
[17104@fw41] CallAgain
[17104@fw41] RequestByMethods: used 1 my [a0a0a00-a0a0aff] peer [c0a8c800-c0a8c8ff]
[17104@fw41] Ass_MatchPeerMethodsIDs: cf28e757 2020100:00 [a0a0a00-a0a0aff] [c0a8c800-
c0a8c8ff]
[17104@fw41] Ass_MatchPeerMethodsIDs: match has failed
[17104@fw41] MatchPeerMethodsIDs: cf28e757 2020100:00 [a0a0a00-a0a0aff] [c0a8c800-
c0a8c8ff]
[17104@fw41] MatchPeerMethodsIDs: Not found
[17104@fw41] MatchPeerPlNeg: cf28e757
[17104@fw41] MatchPeerPlNeg: no ongoing phase1 negotiations
[17104@fw41] *** AddNegotiation: ptr 953188 peer cf28e757 cookieI 00:00 msgID 00 methods
2020100 00 new count: 1
[17104@fw41] < FWIKE_ROLE_START > Id = 2
[17104@fw41] < FWIKE_ROLE_INITIATOR > Id = 2
[17104@fw41] ike_initiator: entering
[17104@fw41] InitiatorOnEnter: idRanges USED mine [a0a0a00-a0a0aff] peer's [c0a8c800-
c0a8c8ff]
[17104@fw41] findSAByPeer: ISAKMP SA was found
[17104@fw41] < FWIKE_EXCH_START > Id = 2
[17104@fw41] < FWIKE_EXCH_QUICK_MODE > Id = 2
[17104@fw41] < FWIKE_PACKET_START > Id = 2
[17104@fw41] < FWIKE_QM_PACKET_1 > Id = 2
[17104@fw41] QMCreate1: entering ~~ Wed Jul 5 12:23:22 2000

[17104@fw41] update_saexp_in_trans: expiration 1800 seconds
[17104@fw41] QMCreate1: rangeUsed: 1 my [a0a0a00-a0a0aff] peer [c0a8c800-c0a8c8ff]
[17104@fw41] RESULT: range_first a0a0a00 last a0a0aff subnet_addr a0a0a00 mask ffffffff00
[17104@fw41] RESULT: range_first c0a8c800 last c0a8c8ff subnet_addr c0a8c800 mask
ffffffff00
[17104@fw41] computeIV from:
[17104@fw41] 44 c0 26 b5 0b c7 b1 09
[17104@fw41] a8 82 0c 69
[17104@fw41] P2 IV:

```

```

[17104@fw41] 9f 26 0c b1 aa 2a 18 7a
[17104@fw41] ~Association: efffe9f0 8ea708
[17104@fw41] ~Negotiation: 935b88 935d40
[17104@fw41] ~Association: 935d40 00
[17104@fw41] Neg's end
[17104@fw41] ResendOutbuf (12) (953188)
[17104@fw41] fwisakmpd_rcv_from_peer: entering
[17104@fw41] canonize_gw: Canonized ip is the same as original ip cf28e757
[17104@fw41] MatchPeerCookieIMsgID: cf28e757 a52895de8e502ae0 a8820c69
[17104@fw41] MatchPeerCookieIMsgID: match found
[17104@fw41] < FWIKE_ROLE_INITIATOR > Id = 2
[17104@fw41] ike_initiator: entering
[17104@fw41] InitiatorOnEnter: idRanges USED mine [a0a0a00-a0a0aff] peer's [c0a8c800-
c0a8c8ff]
[17104@fw41] findSABByPeer: ISAKMP SA was found
[17104@fw41] < FWIKE_EXCH_QUICK_MODE > Id = 2
[17104@fw41] < FWIKE_QM_PACKET_2 > Id = 2
[17104@fw41] QMProcess2: entering ~~ Wed Jul 5 12:23:23 2000

[17104@fw41] -- updatePayloadMap: received payload PA_HASH.
[17104@fw41] -- updatePayloadMap: received payload PA_SA.
[17104@fw41] -- updatePayloadMap: received payload PA_NONCE.
[17104@fw41] -- updatePayloadMap: received payload PA_ID.
[17104@fw41] -- updatePayloadMap: received payload PA_ID.
[17104@fw41] -- updatePayloadMap: received payload PA_NOTIFY.
[17104@fw41] QMProcess2: identifyPayloads succeeded.
[17104@fw41] processNotifyPayload: protocol: 3
[17104@fw41] < FWIKE_QM_PACKET_3 > Id = 2
[17104@fw41] QMCreate3: entering ~~ Wed Jul 5 12:23:23 2000

[17104@fw41] < FWIKE_PACKET_END > Id = 2
[17104@fw41] < FWIKE_EXCH_END > Id = 2
[17104@fw41] < FWIKE_ROLE_END > Id = 2
[17104@fw41] fwIsakmp_SAFFromNegCxt: initiator
[17104@fw41] ESP_SA_FromTransformList: HMAC alg: 1, HMAC keylen: 20
[17104@fw41] SPI: b940c576
[17104@fw41] DES KEY IS:
[17104@fw41] 21 a0 17 c5 bb 32 36 22
[17104@fw41] HMAC KEY IS:
[17104@fw41] 69 df da 03 2e 36 b5 09 dc 4d 7f 86 dd 9f 13 8d 3b a7 a2 8a
[17104@fw41] ESP_SA_FromTransformList: esp_expiretime for Initiator set to +1800
[17104@fw41] ESP_SA_FromTransformList: esp_expiretime for Initiator set to +1800
[17104@fw41] ESP_SA_FromTransformList: esp_renegtime set to +1753
[17104@fw41] ESP_SA_FromTransformList: HMAC alg: 1, HMAC keylen: 20
[17104@fw41] SPI: 21162177
[17104@fw41] DES KEY IS:
[17104@fw41] 6c cf 02 13 23 e7 75 dd
[17104@fw41] HMAC KEY IS:
[17104@fw41] b6 ea 36 8d 8f a0 ac eb 91 26 d9 46 db 2b dc 91 28 81 0f b6
[17104@fw41] ESP_SA_FromTransformList: esp_expiretime for Responder set to +1800
[17104@fw41] ESP_SA_FromTransformList: esp_expiretime for Responder set to +1800
[17104@fw41] ESP_SA_FromTransformList: esp_renegtime set to +1755
[17104@fw41] # of negotiations: 1
[17104@fw41] # of negs: 1
[17104@fw41] Neg: 0 ptr: 953188 ass: 953340 wait4: 00
[17104@fw41] msgId: a8820c69 method: 2020100;00 cookie: a52895de8e502ae0
[17104@fw41] req type: 1 SPIs: 00 00
[17104@fw41] # of waiting negotiations: 0
[17104@fw41] # of negs: 0
[17104@fw41] ** AssHTabs_AddAssTo: ass 9515f8 peer cf28e757 cookie a52895de8e502ae0
msgId: a8820c69
[17104@fw41] AssHTabs_AddAssTo table b4 insertion:

[17104@fw41] AssHTabs_printall:
[17104@fw41] AssHTabs_AddAssTo after insertion:

[17104@fw41] AssHTabs_printall:
[17104@fw41] 0 ass 9515f8 keyptr 8ea708 methods 2020100:00counter 00:02 NOT gonna exp

[17104@fw41] AssHTabs_AddAssTo: ass: 9515f8 8ea708 cf28e757
[17104@fw41] AssHTabs_AddAssTo: insertion has succeeded

```

```

[17104@fw41] ~Negotoation: effff850 9506d0
[17104@fw41] ~Association: 9506d0 00
[17104@fw41] Neg's end
[17104@fw41] ResendOutbuf (3) (953188)
[17104@fw41] ReplyBy: entering
[17104@fw41] fwasync_connbuf_realloc: reallocating 9356e0 from 1181 to 5188
[17104@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 9356e0, len = 4164, key = 0
[17104@fw41] comm_decrypt_buf: fd = 29, buf = 951b48, len = 32, key = 0
[17104@fw41] fwasync_connbuf_realloc: reallocating 951b48 from 1056 to 5156
[17104@fw41] comm_decrypt_buf: fd = 29, buf = 96c1d8, len = 4132, key = 0
[17104@fw41] fwisakmp_rcv_sa_by_methods: received answer to methods request
[17104@fw41] get_userc_entry: no user entry for ip 192.168.200.0
[17104@fw41] fwisakmp_store_sa_in_tables:
[17104@fw41] myRange [a0a0a00-a0a0aff] peerRange [c0a8c800-c0a8c8ff]
[17104@fw41] delay writing to ISAKMP_ESP_table
[17104@fw41] fw_dtab_record_conn: vals=<a0a0a0a,40e,c0a8c814,15,6;60186d0c,3,ffffd010>
[17104@fw41] fwisakmp_rcv_sa_by_methods: delay is 300
[17104@fw41] fwisakmp_getmethod: Combined ESP: DES + SHA1
[17104@fw41] add_qm_ids: rangeUsed 1 [a0a0a00-a0a0aff] [c0a8c800-c0a8c8ff]
[17104@fw41] RESULT: range_first a0a0a00 last a0a0aff subnet_addr a0a0a00 mask ffffffff00
[17104@fw41] RESULT: range_first c0a8c800 last c0a8c8ff subnet_addr c0a8c800 mask ffffffff00
[17104@fw41] fwcrypt_log: sending log op 16
[17104@fw41] proxy xlate input: src a0a0a0a sport 40e dst c0a8c814 dport 15
[17104@fw41] fwisakmp_getmethod: Combined ESP: DES + SHA1
[17104@fw41] fwcrypt_log: sending log op 3
[17104@fw41] fwisakmp_rcv_sa_by_methods: Isakmp trap success
[17104@fw41] fwike_isakmpd_pipe_handler: called without data
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (2) (953188)
[17104@fw41] fwisakmpd_rcv_from_peer: entering
[17104@fw41] canonize_gw: Canonized ip is the same as original ip cf28e757
[17104@fw41] MatchPeerCookieIMsgID: cf28e757 a52895de8e502ae0 00
[17104@fw41] MatchPeerCookieIMsgID: match failed
[17104@fw41] *** AddNegotiation: ptr 9525b0 peer cf28e757 cookieI a52895de:8e502ae0
msgID b5a542de methods 00 00 new count: 2
[17104@fw41] < FWIKE_ROLE_START > Id = 3
[17104@fw41] < FWIKE_ROLE_RESPONDER > Id = 3
[17104@fw41] FwIkeResponder: entering
[17104@fw41] FwIkeResponderOnEnter: idRanges NOT USED mine [0-0] peer's [0-0]
[17104@fw41] findSAByPeer: ISAKMP SA was found
[17104@fw41] < FWIKE_EXCH_START > Id = 3
[17104@fw41] < FWIKE_EXCH_INFORMATION > Id = 3
[17104@fw41] < FWIKE_PACKET_START > Id = 3
[17104@fw41] < FWIKE_INFO_RESPONDER > Id = 3
[17104@fw41] fwIsakmp_ProcessInfoExc p2: entering
[17104@fw41] computeIV from:
[17104@fw41] 44 c0 26 b5 0b c7 b1 09
[17104@fw41] b5 a5 42 de
[17104@fw41] -- updatePayloadMap: received payload PA_HASH.
[17104@fw41] -- updatePayloadMap: received payload PA_NOTIFY.
[17104@fw41] ProcessInfo: identifyPayloads succeeded.
[17104@fw41] processNotifyPayload: protocol: 1
[17104@fw41] Peer cf28e757 says: payload malformed
[17104@fw41] fwisakmpd_send_log: sending log message: Received Notification from Peer:
payload malformed
[17104@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 9356e0, len = 183, key = 0
[17104@fw41] < FWIKE_PACKET_END > Id = 3
[17104@fw41] < FWIKE_EXCH_END > Id = 3
[17104@fw41] < FWIKE_ROLE_END > Id = 3
[17104@fw41] sndrcv: got Notification from peer
[17104@fw41] DeleteNegotiation<1>: invoked(1): ptr 9525b0 peer:cf28e757 cookieI a52895de
8e502ae0 msgId b5a542de methods 00-00 SPIs 00 00
[17104@fw41] DeleteNegotiation: entering
[17104@fw41] ~Negotoation: 9525b0 936b30
[17104@fw41] ~Association: 936b30 00
[17104@fw41] Neg's end
[17104@fw41] ~Negotoation: effff850 9506d0
[17104@fw41] ~Association: 9506d0 00
[17104@fw41] Neg's end
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (1) (953188)

```

```

[fw41@fw41] comm_decrypt_buf: fd = 29, buf = 96c1d8, len = 32, key = 0
[fw41@fw41] comm_decrypt_buf: fd = 29, buf = 96c1d8, len = 151, key = 0
[fw41@fw41] simple_ISAKMP_log: log: Received Notification from Peer: payload malformed
[17104@fw41] fwike_isakmpd_pipe_handler: called without data
[17104@fw41] fwisakmpd_rcv_from_peer: entering
[17104@fw41] canonize_gw: Canonized ip is the same as original ip cf28e757
[17104@fw41] MatchPeerCookieIMsgID: cf28e757 a52895de8e502ae0 00
[17104@fw41] MatchPeerCookieIMsgID: match failed
[17104@fw41] *** AddNegotiation: ptr 952b70 peer cf28e757 cookieI a52895de:8e502ae0
msgID b6ecc488 methods 00 00 new count: 2
[17104@fw41] < FWIKE_ROLE_START > Id = 4
[17104@fw41] < FWIKE_ROLE_RESPONDER > Id = 4
[17104@fw41] FwIkeResponder: entering
[17104@fw41] FwIkeResponderOnEnter: idRanges NOT USED mine [0-0] peer's [0-0]
[17104@fw41] findSABByPeer: ISAKMP SA was found
[17104@fw41] < FWIKE_EXCH_START > Id = 4
[17104@fw41] < FWIKE_EXCH_INFORMATION > Id = 4
[17104@fw41] < FWIKE_PACKET_START > Id = 4
[17104@fw41] < FWIKE_INFO_RESPONDER > Id = 4
[17104@fw41] fwIsakmp_ProcessInfoExc p2: entering
[17104@fw41] computeIV from:
[17104@fw41] 44 c0 26 b5 0b c7 b1 09
[17104@fw41] b6 ec c4 88
[17104@fw41] -- updatePayloadMap: received payload PA_HASH.
[17104@fw41] -- updatePayloadMap: received payload PA_NOTIFY.
[17104@fw41] ProcessInfo: identifyPayloads succeeded.
[17104@fw41] processNotifyPayload: protocol: 1
[17104@fw41] Peer cf28e757 says: payload malformed
[17104@fw41] fwisakmpd_send_log: sending log message: Received Notification from Peer:
payload malformed
[17104@fw41] fwcomm_encrypt_inplace: fd = 0, buf = 9356e0, len = 183, key = 0
[17104@fw41] < FWIKE_PACKET_END > Id = 4
[17104@fw41] < FWIKE_EXCH_END > Id = 4
[17104@fw41] < FWIKE_ROLE_END > Id = 4
[17104@fw41] sndrcv: got Notification from peer
[17104@fw41] DeleteNegotiation<1>: invoked(1): ptr 952b70 peer:cf28e757 cookieI a52895de
8e502ae0 msgId b6ecc488 methods 00-00 SPIs 00 00
[17104@fw41] DeleteNegotiation: entering
[17104@fw41] ~Negotiation: 952b70 936b30
[17104@fw41] ~Association: 936b30 00
[17104@fw41] Neg's end
[17104@fw41] ~Negotiation: effff850 9506d0
[17104@fw41] ~Association: 9506d0 00
[17104@fw41] Neg's end
[17104@fw41] fwisakmpd_rcv_from_peer: entering
[17104@fw41] fwisakmpd_rcv_from_peer: Retransmission detected
[fw41@fw41] comm_decrypt_buf: fd = 29, buf = 96c1d8, len = 32, key = 0
[fw41@fw41] comm_decrypt_buf: fd = 29, buf = 96c1d8, len = 151, key = 0
[fw41@fw41] simple_ISAKMP_log: log: Received Notification from Peer: payload malformed
[17104@fw41] fwike_isakmpd_pipe_handler: called without data
[17104@fw41] RetransmitBuffer
[17104@fw41] ResendOutbuf (0) (953188)
[17104@fw41] ResendOutbuf: retrans counter is down to 0
[17104@fw41] DeleteNegotiation<1>: invoked(1): ptr 953188 peer:cf28e757 cookieI a52895de
8e502ae0 msgId a8820c69 methods 2020100-00 SPIs 00 00
[17104@fw41] DeleteNegotiation: entering
[17104@fw41] ~Negotiation: 953188 953340
[17104@fw41] ~Association: 953340 00
[17104@fw41] Neg's end
[fw41@fw41] ISAKMP_ESP_table <cf28e757,2020100,a0a0a00,a0a0aff,c0a8c800,c0a8c8ff;608f0ce4>
[fw41@fw41] fwisakmp_sendhold: (383492)

```

Output from IOS debug crypto ipsec/isakmp/engine commands

```

3w1d: ISAKMP (0): received packet from 207.40.231.82 (N) NEW SA
3w1d: ISAKMP (100): processing SA payload. message ID = 0
3w1d: ISAKMP (100): Checking ISAKMP transform 1 against priority 10 policy
3w1d: ISAKMP: encryption DES-CBC
3w1d: ISAKMP: hash SHA

```

```

3wld: ISAKMP:      auth pre-share
3wld: ISAKMP:      default group 2
3wld: ISAKMP:      life type in seconds
3wld: ISAKMP:      life duration (VPI) of  0x0 0x0 0x1 0x2C
3wld: ISAKMP (100): atts are acceptable. Next payload is 0
3wld: Crypto engine 0: generate alg param

3wld: CRYPTO_ENGINE: Dh phase 1 status: 0
3wld: ISAKMP (100): processing KE payload. message ID = 0
3wld: Crypto engine 0: generate alg param

3wld: ISAKMP (100): processing NONCE payload. message ID = 0
3wld: ISAKMP (100): processing ID payload. message ID = 0
3wld: Crypto engine 0: create ISAKMP SKEYID for conn id 100
3wld: ISAKMP (100): SKEYID state generated
3wld: ISAKMP (100): ID payload
    next-payload : 10
    type          : 1
    protocol      : 17
    port          : 500
    length        : 8
3wld: ISAKMP (100): Total payload length: 12
3wld: generate hmac context for conn id 100
3wld: ISAKMP (100): sending packet to 207.40.231.82 (R) AG_INIT_EXCH
3wld: ISAKMP (0): received packet from 207.40.231.82 (N) NEW SA
3wld: CRYPTO(eps_release_crypto_conn_entry): released conn 101
3wld: ISAKMP (0): received packet from 207.40.231.82 (N) NEW SA
3wld: CRYPTO(eps_release_crypto_conn_entry): released conn 102
3wld: ISAKMP (0): received packet from 207.40.231.82 (N) NEW SA
3wld: CRYPTO(eps_release_crypto_conn_entry): released conn 103
3wld: ISAKMP (100): received packet from 207.40.231.82 (R) AG_INIT_EXCH
3wld: ISAKMP (100): processing HASH payload. message ID = 0
3wld: generate hmac context for conn id 100
3wld: ISAKMP (100): SA has been authenticated with 207.40.231.82
3wld: ISAKMP (100): received packet from 207.40.231.82 (R) QM_IDLE
3wld: %CRYPTO-6-IKMP_NOT_ENCRYPTED: IKE packet from 207.40.231.82  was not encrypted and
it should've been.
3wld: ISAKMP (100): received packet from 207.40.231.82 (R) QM_IDLE
3wld: %CRYPTO-6-IKMP_NOT_ENCRYPTED: IKE packet from 207.40.231.82  was not encrypted and
it should've been.
3wld: ISAKMP (100): received packet from 207.40.231.82 (R) QM_IDLE
3wld: generate hmac context for conn id 100
3wld: ISAKMP (100): processing SA payload. message ID = -1467872151
3wld: ISAKMP (100): Checking IPsec proposal 1
3wld: ISAKMP: transform 1, ESP_DES
3wld: ISAKMP:      attributes in transform:
3wld: ISAKMP:      SA life type in seconds
3wld: ISAKMP:      SA life duration (VPI) of  0x0 0x0 0x7 0x8
3wld: ISAKMP:      authenticator is HMAC-SHA
3wld: ISAKMP:      encaps is 1
3wld: ISAKMP (100): atts are acceptable.
3wld: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 207.40.231.87, src= 207.40.231.82,
    dest_proxy= 192.168.200.0/255.255.255.0/0/0 (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
3wld: ISAKMP (100): processing NONCE payload. message ID = -1467872151
3wld: ISAKMP (100): processing ID payload. message ID = -1467872151
3wld: ISAKMP (100): ID_IPV4_ADDR_SUBNET src 10.10.10.0/255.255.255.0 prot 0 port 0
3wld: ISAKMP (100): processing ID payload. message ID = -1467872151
3wld: ISAKMP (100): ID_IPV4_ADDR_SUBNET dst 192.168.200.0/255.255.255.0 prot 0 port 0
3wld: IPSEC(key_engine): got a queue event...
3wld: IPSEC(spi_response): getting spi 555098487 for SA
    from 207.40.231.82  to 207.40.231.87  for prot 3
3wld: generate hmac context for conn id 100
3wld: ISAKMP (100): sending packet to 207.40.231.82 (R) QM_IDLE
3wld: ISAKMP (100): received packet from 207.40.231.82 (R) QM_IDLE
3wld: generate hmac context for conn id 100
3wld: ISAKMP (100): Creating IPsec SAs

```

```

3wld:      inbound SA from 207.40.231.82   to 207.40.231.87   (proxy 10.10.10.0
to 192.168.200.0 )
3wld:      has spi 555098487 and conn_id 104 and flags 4
3wld:      lifetime of 1800 seconds
3wld:      outbound SA from 207.40.231.87   to 207.40.231.82   (proxy 192.168.200.0
to 10.10.10.0 )
3wld:      has spi -1186937482 and conn_id 105 and flags 4
3wld:      lifetime of 1800 seconds
3wld: IPSEC(key_engine): got a queue event...
3wld: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 207.40.231.87, src= 207.40.231.82,
  dest_proxy= 192.168.200.0/255.255.255.0/0/0 (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= 1800s and 0kb,
  spi= 0x21162177(555098487), conn_id= 104, keysize= 0, flags= 0x4
3wld: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 207.40.231.87, dest= 207.40.231.82,
  src_proxy= 192.168.200.0/255.255.255.0/0/0 (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= 1800s and 0kb,
  spi= 0xB940C576(3108029814), conn_id= 105, keysize= 0, flags= 0x4
3wld: IPSEC(create_sa): sa created,
  (sa) sa_dest= 207.40.231.87, sa_prot= 50,
  sa_spi= 0x21162177(555098487),
  sa_trans= esp-des esp-sha-hmac , sa_conn_id= 104
3wld: IPSEC(create_sa): sa created,
  (sa) sa_dest= 207.40.231.82, sa_prot= 50,
  sa_spi= 0xB940C576(3108029814),
  sa_trans= esp-des esp-sha-hmac , sa_conn_id= 105
3wld: ISAKMP (100): received packet from 207.40.231.82 (R) QM_IDLE
3wld: ISAKMP: reserved not zero on payload 8!
3wld: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 207.40.231.82   failed its sanity
check or is malformed
3wld: generate hmac context for conn id 100
3wld: ISAKMP (100): sending packet to 207.40.231.82 (R) QM_IDLE
3wld: ISAKMP (100): received packet from 207.40.231.82 (R) QM_IDLE
3wld: ISAKMP: reserved not zero on payload 8!
3wld: generate hmac context for conn id 100
3wld: ISAKMP (100): sending packet to 207.40.231.82 (R) QM_IDLE
3wld: ISAKMP (100): retransmitting phase 1...
3wld: ISAKMP (100): sending packet to 207.40.231.82 (R) QM_IDLE
3wld: ISADB: reaper checking SA, conn_id = 100

```