FortiGate Antivirus Firewall to Cisco Router IPSec VPN Interoperability

Technical Note

FortiGate Antivirus Firewall to Cisco Router IPSec VPN Interoperability Technical Note	
Document Version:	Version 1
Publication Date:	18 December 2003
Description:	Describes the CLI commands used to set up site-to-site and hub-and-spoke IPSec VPN tunnels between FortiGate firewalls and Cisco routers. Provides configuration examples for four scenarios.
Products:	FortiGate-60 Antivirus Firewall FortiGate-200 Antivirus Firewall FortiGate-500 Antivirus Firewall Cisco PIX 501 Router Cisco 831 Router

Fortinet Inc.

FortiGate Antivirus Firewall to Cisco Router IPSec VPN Interoperability Technical Note
v2.50
18 December 2003

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

Table of Contents

FortiGate Antivirus Firewall to Cisco Router IPSec VPN Interoperability Technical Note

FortiGate products offer superior interoperability with other IPSec VPN gateways and client products. This technical note contains example procedures and configurations for site-to-site and hub-and-spoke IPSec VPN tunnels between FortiGate firewalls and Cisco routers.

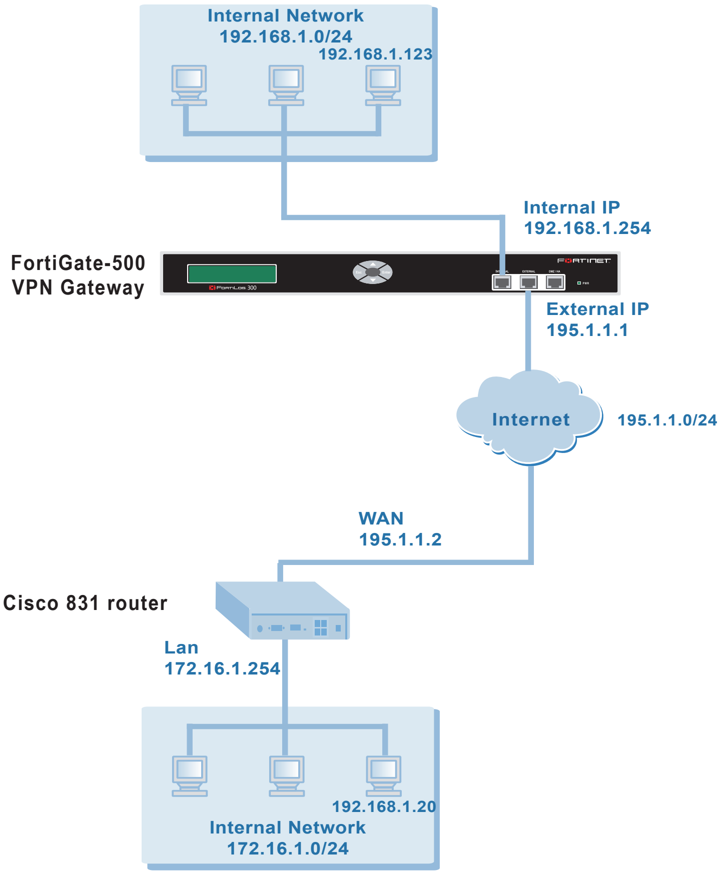
This technical note contains the following sections:

- Site-to-site VPN between FortiGate unit and Cisico 831 router
- Site-to-site VPN between FortiGate unit and Cisco PIX 501 router
- Hub-and-spoke VPN with Fortigate-200 unit as hub
- Hub-and-spoke VPN with Cisco 831 router as hub

Site-to-site VPN between FortiGate unit and Cisico 831 router

Network topology

Figure 1: FortiGate-500 to Cisco 831 Router network topology



Hardware and firmware specifications

Fortigate-500 gateway

- Version:Fortigate-500 2.50,build106,030925
- virus-db:4.126(09/03/2003 18:03)
- ids-db:2.65(09/19/2003 15:58)
- operation mode: Nat
- Hostname: Fortigate-500

Cisco 831 router

- Cisco Internetwork Operating System Software
- IOS (tm) C831 Software (C831-K9O3SY6-M), Version 12.2(13)ZH1
- EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
- Synched to technology version 12.2(14.5)T
- System image file: flash:c831-k9o3sy6-mz.122-13.ZH1.bin
- CISCO C831 (MPC857DSL) processor (revision 0x200) with 29492K/3276K bytes of memory
- 2 Ethernet/IEEE 802.3 interface(s)
- 128K bytes of non-volatile configuration memory.
- 8192K bytes of processor board System flash (Read/Write)
- 2048K bytes of processor board Web flash (Read/Write)

FortiGate-500 configuration

```
set system opmode nat

set system interface internal mode static ip 192.168.1.254
  255.255.255.0

set system interface external mode static ip 195.1.1.1
  255.255.255.0

set system hostname Fortigate-500

set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 195.1.1.2

set firewall address internal Internal_All subnet 0.0.0.0
  0.0.0.0

set firewall address external External_All subnet 0.0.0.0
  0.0.0.0

set firewall address dmz DMZ_All subnet 0.0.0.0 0.0.0.0

set firewall address internal 192_168_1_0 subnet 192.168.1.0
  255.255.255.0

set firewall address external 172_16_1_0 subnet 172.16.1.0
  255.255.255.0

set vpn ipsec phase1 to_Cisco_831 type static gw 195.1.1.2
  proposal 3des-sha1

keylife 28800 dhgrp 5  authmethod PSK fortigate nattraversal
  enable keepalive 5 dpd enable dpdidleworry 10
  dpdretrycount 3 dpdretryinterval 5 dpdidlecleanup 300
  peertype any xauthtype disable

set vpn ipsec phase2 to_172_16_1_0 phase1name to_Cisco_831
  proposal 3des-sha1keylifeseconds 1800 dhgrp 1 replay
  enable concentrator none
```

```
set firewall policy srcintf internal dstintf external
  policyid 2 srcaddr 192_168_1_0 dstaddr 172_16_1_0 schedule
  Always service ANY action encrypt vpntunnel to_172_16_1_0
  inbound allow outbound allow
set firewall policy srcintf internal dstintf external
  policyid 1 srcaddr Internal_All dstaddr External_All
  schedule Always service ANY action accept avwebfilter Scan
  nat enable
```

Cisco 831 router configuration

```
hostname CiscoRouter
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 5
 hash sha
crypto isakmp key fortigate address 195.1.1.1
!
crypto ipsec transform-set ESP_3DES_SHA esp-3des esp-sha-hmac
!
crypto map VPN 10 ipsec-isakmp
 set peer 195.1.1.1
 set transform-set ESP_3DES_SHA
 match address 101
!
interface Ethernet0
 ip address 172.16.1.254 255.255.255.0
!
interface Ethernet1
 ip address 195.1.1.2 255.255.255.0
 crypto map VPN
!
ip classless
ip route 0.0.0.0 0.0.0.0 195.1.1.1
!
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.1.0
  0.0.0.255
```

```
!
end
```

Viewing the diagose results

FortiGate unit

Enter the following diagnose command:

```
diag debug app ike 2
```

The following results appear:

```
Fortigate-500 # Get sa_connect message...195.1.1.1-
  >195.1.1.2:500, natt_mode=0
Using new connection...natt_mode=0
Set connection name = to_Cisco_831.
Tunnel 195.1.1.1 ---> 195.1.1.2:500,natt_en=1 is starting
  negotiation
Initiator:main mode is sending 1st message...
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Sending NATT VID payload (draft3 and draft1)....
Initiator: sent 195.1.1.2 main mode message #1 (OK)
set retransmit: st=3, timeout=10.

Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xB7D73DCE8B809194, Len = 100
Received Payloads= SA VID
Initiator:main mode get 1st response...
test the peer keepalive status....
Negotiate Result
Proposal_id = 1:
   Protocol_id = ISAKMP:
      trans_id = KEY_IKE.
      encapsulation = 0 (unknown)
         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
         type=OAKLEY_HASH_ALG, val=SHA.
         type=AUTH_METHOD, val=PRESHARED_KEY.
         type=OAKLEY_GROUP, val=1536.
Phase1 lifetimes=28800
Negotiate Success.(No echo).
testing the peer DPD status....
The peer does not send vid, not DPD compatible.
test the peer natt status....
The peer supports natt draft3.
Initiator: sent 195.1.1.2 main mode message #2 (OK)
set retransmit: st=3, timeout=10.

Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xB7D73DCE8B809194, Len = 368
Received Payloads= KE NONCE VID VID VID VID 130 130
Initiator:main mode get 2nd response...
Using IPS_NAT_MODE_NONE.
Responder: sent 195.1.1.2 main mode message #3 (OK)
set retransmit: st=3, timeout=10.

Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xB7D73DCE8B809194, Len = 68
Received Payloads= ID HASH
Initiator:main mode get 3rd response...
set gw: 0x8136cb8, timeout=28800.
Initiator: parsed 195.1.1.2 main mode message #3 (DONE)
Initiator:quick mode: pfs is not enabled
Try to negotiate with 1800 life seconds.
Initiator: sent 195.1.1.2 quick mode message #1 (OK)
set retransmit: st=4, timeout=10.
Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 32, Message id = 0x63D5E424, Len = 188
Received Payloads= HASH SA NONCE ID ID Notif
Initiator:quick mode get 1st response
Negotiate Result
Proposal_id = 1:
   Protocol_id = IPSEC_ESP:
      trans_id = ESP_3DES.
      encapsulation = ENCAPSULATION_MODE_TUNNEL
         type=AUTH_ALG, val=SHA1.
Phase2 esp lifetimes=1800
Using tunnel mode.
Negotiate Success.(No echo).
Initiator:Prepare to install sa.
Replay protection enable.
Set sa life soft seconds=1775.
Set sa life hard seconds=1800.
dport = 500.Initializing sa OK.
Initiator: sent 195.1.1.2 quick mode message #2 (DONE)
expire: st=4, timeout=120.
```

Cisco 831 router

Enter the following command:

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

The following results appear:

```
*Mar  1 00:04:13.507: ISAKMP (0:0): received packet from
  195.1.1.1 dport 500 sport 500 Global (N) NEW SA

*Mar  1 00:04:13.507: ISAKMP: local port 500, remote port 500

*Mar  1 00:04:13.511: ISAKMP: Find a dup sa in the avl tree
  during calling isadb_insert sa = 8157B490

*Mar  1 00:04:13.511: ISAKMP (0:2): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:04:13.511: ISAKMP (0:2): Old State = IKE_READY
  New State = IKE_R_MM1

*Mar  1 00:04:13.511: ISAKMP (0:2): processing SA payload.
  message ID = 0

*Mar  1 00:04:13.511: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:04:13.515: ISAKMP (0:2:): vendor ID seems
  Unity/DPD but hash mismatch

*Mar  1 00:04:13.515: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:04:13.515: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 233 mismatch
```

```
*Mar  1 00:04:13.515: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:04:13.515: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 157 mismatch

*Mar  1 00:04:13.515: ISAKMP (0:2): vendor ID is NAT-T v3

*Mar  1 00:04:13.515: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:04:13.515: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 221 mismatch

*Mar  1 00:04:13.515: ISAKMP: Looking for a matching key for
  195.1.1.1 in default : success

*Mar  1 00:04:13.519: ISAKMP (0:2): found peer pre-shared key
  matching 195.1.1.1

*Mar  1 00:04:13.519: ISAKMP (0:2) local preshared key found

*Mar  1 00:04:13.519: ISAKMP : Scanning profiles for xauth
  ...

*Mar  1 00:04:13.519: ISAKMP (0:2): Checking ISAKMP transform
  1 against priority 10 policy

*Mar  1 00:04:13.519: ISAKMP:      life type in seconds

*Mar  1 00:04:13.519: ISAKMP:      life duration (basic) of
  28800

*Mar  1 00:04:13.519: ISAKMP:      encryption 3DES-CBC

*Mar  1 00:04:13.519: ISAKMP:      hash SHA

*Mar  1 00:04:13.519: ISAKMP:      auth pre-share

*Mar  1 00:04:13.519: ISAKMP:      default group 5

*Mar  1 00:04:13.519: ISAKMP (0:2): atts are acceptable. Next
  payload is 0

*Mar  1 00:04:14.943: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:04:14.943: ISAKMP (0:2:): vendor ID seems
  Unity/DPD but hash mismatch

*Mar  1 00:04:14.943: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:04:14.943: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 233 mismatch

*Mar  1 00:04:14.947: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:04:14.947: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 157 mismatch

*Mar  1 00:04:14.947: ISAKMP (0:2): vendor ID is NAT-T v3
```

```
*Mar  1 00:04:14.947: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:04:14.947: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 221 mismatch

*Mar  1 00:04:14.947: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:04:14.947: ISAKMP (0:2): Old State = IKE_R_MM1
  New State = IKE_R_MM1

*Mar  1 00:04:14.951: ISAKMP (0:2): constructed NAT-T vendor-
  03 ID

*Mar  1 00:04:14.951: ISAKMP (0:2): sending packet to
  195.1.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP

*Mar  1 00:04:14.951: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:04:14.951: ISAKMP (0:2): Old State = IKE_R_MM1
  New State = IKE_R_MM2

*Mar  1 00:04:14.971: ISAKMP (0:2): received packet from
  195.1.1.1 dport 500 sport 500 Global (R) MM_SA_SETUP

*Mar  1 00:04:14.971: ISAKMP (0:2): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:04:14.971: ISAKMP (0:2): Old State = IKE_R_MM2
  New State = IKE_R_MM3

*Mar  1 00:04:14.975: ISAKMP (0:2): processing KE payload.
  message ID = 0

*Mar  1 00:04:16.395: ISAKMP (0:2): processing NONCE payload.
  message ID = 0

*Mar  1 00:04:16.395: ISAKMP: Looking for a matching key for
  195.1.1.1 in default : success

*Mar  1 00:04:16.395: ISAKMP (0:2): found peer pre-shared key
  matching 195.1.1.1

*Mar  1 00:04:16.399: ISAKMP (0:2): SKEYID state generated

*Mar  1 00:04:16.399: ISAKMP:received payload type 17

*Mar  1 00:04:16.399: ISAKMP (0:2): Detected NAT-D payload

*Mar  1 00:04:16.399: ISAKMP (0:2): NAT match MINE hash

*Mar  1 00:04:16.399: ISAKMP:received payload type 17

*Mar  1 00:04:16.399: ISAKMP (0:2): Detected NAT-D payload

*Mar  1 00:04:16.399: ISAKMP (0:2): NAT match HIS hash

*Mar  1 00:04:16.399: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:04:16.399: ISAKMP (0:2): Old State = IKE_R_MM3
  New State = IKE_R_MM3
```

```
*Mar  1 00:04:16.399: ISAKMP (0:2): constructed HIS NAT-D

*Mar  1 00:04:16.399: ISAKMP (0:2): constructed MINE NAT-D

*Mar  1 00:04:16.399: ISAKMP (0:2): sending packet to
  195.1.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH

*Mar  1 00:04:16.403: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:04:16.403: ISAKMP (0:2): Old State = IKE_R_MM3
  New State = IKE_R_MM4

*Mar  1 00:04:16.415: ISAKMP (0:2): received packet from
  195.1.1.1 dport 500 sport 500 Global (R) MM_KEY_EXCH

*Mar  1 00:04:16.419: ISAKMP (0:2): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:04:16.419: ISAKMP (0:2): Old State = IKE_R_MM4
  New State = IKE_R_MM5

*Mar  1 00:04:16.419: ISAKMP (0:2): processing ID payload.
  message ID = 0

*Mar  1 00:04:16.419: ISAKMP (0:2): peer matches *none* of
  the profiles

*Mar  1 00:04:16.419: ISAKMP (0:2): processing HASH payload.
  message ID = 0

*Mar  1 00:04:16.423: ISAKMP (0:2): SA has been authenticated
  with 195.1.1.1

*Mar  1 00:04:16.423: ISAKMP (0:2): peer matches *none* of
  the profiles

*Mar  1 00:04:16.423: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:04:16.423: ISAKMP (0:2): Old State = IKE_R_MM5
  New State = IKE_R_MM5

*Mar  1 00:04:16.427: ISAKMP (0:2): SA is doing pre-shared
  key authentication using id type ID_IPV4_ADDR

*Mar  1 00:04:16.427: ISAKMP (2): ID payload

        next-payload : 8

        type         : 1

        addr         : 195.1.1.2

        protocol     : 17

        port         : 500

        length       : 8

*Mar  1 00:04:16.427: ISAKMP (2): Total payload length: 12

*Mar  1 00:04:16.435: ISAKMP (0:2): sending packet to
  195.1.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH
```

```
*Mar  1 00:04:16.435: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:04:16.435: ISAKMP (0:2): Old State = IKE_R_MM5
  New State = IKE_P1_COMPLETE

*Mar  1 00:04:16.443: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

*Mar  1 00:04:16.443: ISAKMP (0:2): Old State =
  IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Mar  1 00:04:16.443: ISAKMP (0:2): received packet from
  195.1.1.1 dport 500 sport 500 Global (R) QM_IDLE

*Mar  1 00:04:16.443: ISAKMP: set new node 1674961956 to
  QM_IDLE

*Mar  1 00:04:16.447: ISAKMP (0:2): processing HASH payload.
  message ID = 1674961956

*Mar  1 00:04:16.447: ISAKMP (0:2): processing SA payload.
  message ID = 1674961956

*Mar  1 00:04:16.447: ISAKMP (0:2): Checking IPSec proposal 1

*Mar  1 00:04:16.447: ISAKMP: transform 1, ESP_3DES

*Mar  1 00:04:16.447: ISAKMP:   attributes in transform:

*Mar  1 00:04:16.447: ISAKMP:      encaps is 1

*Mar  1 00:04:16.447: ISAKMP:      SA life type in seconds

*Mar  1 00:04:16.447: ISAKMP:     SA life duration (basic) of
  1800

*Mar  1 00:04:16.447: ISAKMP:      authenticator is HMAC-SHA

*Mar  1 00:04:16.447: ISAKMP (0:2): atts are acceptable.

*Mar  1 00:04:16.451: IPSEC(validate_proposal_request):
  proposal part #1,

  (key eng. msg.) INBOUND local= 195.1.1.2, remote=
  195.1.1.1,

   local_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),

   remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),

   protocol= ESP, transform= esp-3des esp-sha-hmac ,

   lifedur= 0s and 0kb,

   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2

*Mar  1 00:04:16.451: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 00:04:16.451: ISAKMP (0:2): processing NONCE payload.
  message ID = 1674961956

*Mar  1 00:04:16.451: ISAKMP (0:2): processing ID payload.
  message ID = 1674961956
```

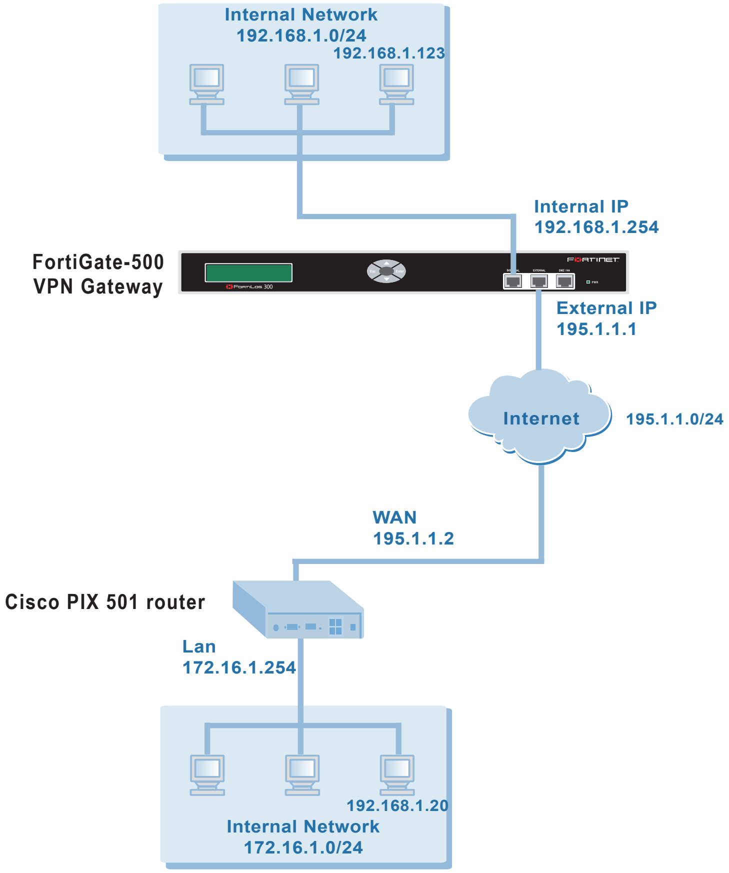
```
*Mar  1 00:04:16.455: ISAKMP (0:2): processing ID payload.
  message ID = 1674961956

*Mar  1 00:04:16.455: ISAKMP (0:2): asking for 1 spis from
  ipsec

*Mar  1 00:04:16.455: ISAKMP (0:2): Node 1674961956, Input =
  IKE_MESG_FROM_PEER, IKE_QM_EXCH

*Mar  1 00:04:16.455: ISAKMP (0:2): Old State = IKE_QM_READY
  New State = IKE_QM_SPI_STARVE

*Mar  1 00:04:16.455: IPSEC(key_engine): got a queue event...

*Mar  1 00:04:16.455: IPSEC(spi_response): getting spi
  987184639 for SA     from 195.1.1.2      to 195.1.1.1
  for prot 3

*Mar  1 00:04:16.455: ISAKMP: received ke message (2/1)

*Mar  1 00:04:16.711: ISAKMP (0:2): sending packet to
  195.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE

*Mar  1 00:04:16.711: ISAKMP (0:2): Node 1674961956, Input =
  IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY

*Mar  1 00:04:16.711: ISAKMP (0:2): Old State =
  IKE_QM_SPI_STARVE  New State = IKE_QM_R_QM2

*Mar  1 00:04:16.715: ISAKMP (0:2): received packet from
  195.1.1.1 dport 500 sport 500 Global (R) QM_IDLE

*Mar  1 00:04:16.727: ISAKMP (0:2): Creating IPSec SAs

*Mar  1 00:04:16.727:         inbound SA from 195.1.1.1 to
  195.1.1.2 (f/i)  0/ 0        (proxy 192.168.1.0 to
  172.16.1.0)

*Mar  1 00:04:16.727:         has spi 0x3AD73DFF and conn_id
  20 and flags 2

*Mar  1 00:04:16.735:         lifetime of 1800 seconds

*Mar  1 00:04:16.735:         has client flags 0x0

*Mar  1 00:04:16.735:        outbound SA from 195.1.1.2
  to 195.1.1.1  (f/i)  0/ 0 (proxy 172.16.1.0      to
  192.168.1.0    )

*Mar  1 00:04:16.735:        has spi -1713839141 and conn_id
  21 and flags A

*Mar  1 00:04:16.735:         lifetime of 1800 seconds

*Mar  1 00:04:16.735:         has client flags 0x0

*Mar  1 00:04:16.735: ISAKMP (0:2): deleting node 1674961956
  error FALSE reason"quick mode done (await)"

*Mar  1 00:04:16.735: ISAKMP (0:2): Node 1674961956, Input =
  IKE_MESG_FROM_PEER, IKE_QM_EXCH

*Mar  1 00:04:16.735: ISAKMP (0:2): Old State = IKE_QM_R_QM2
  New State = IKE_QM_PHASE2_COMPLETE
```

```
*Mar  1 00:04:16.735: IPSEC(key_engine): got a queue event...

*Mar  1 00:04:16.739: IPSEC(initialize_sas): ,

  (key eng. msg.) INBOUND local= 195.1.1.2, remote=
  195.1.1.1,

    local_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),

    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),

    protocol= ESP, transform= esp-3des esp-sha-hmac ,

    lifedur= 1800s and 0kb,

    spi= 0x3AD73DFF(987184639), conn_id= 20, keysize= 0,
  flags= 0x2

*Mar  1 00:04:16.739: IPSEC(initialize_sas): ,

  (key eng. msg.) OUTBOUND local= 195.1.1.2, remote=
  195.1.1.1,

    local_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),

    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),

    protocol= ESP, transform= esp-3des esp-sha-hmac ,

    lifedur= 1800s and 0kb,

    spi= 0x99D8E3DB(2581128155), conn_id= 21, keysize= 0,
  flags= 0xA

*Mar  1 00:04:16.739: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 00:04:16.743: IPSEC(add mtree): src 172.16.1.0, dest
  192.168.1.0, dest_port 0

*Mar  1 00:04:16.743: IPSEC(create_sa): sa created,

  (sa) sa_dest= 195.1.1.2, sa_prot= 50,

    sa_spi= 0x3AD73DFF(987184639),

    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 20

*Mar  1 00:04:16.743: IPSEC(create_sa): sa created,

  (sa) sa_dest= 195.1.1.1, sa_prot= 50,

    sa_spi= 0x99D8E3DB(2581128155),

    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 21

*Mar  1 00:04:30.279: ISAKMP (0:1): purging SA., sa=814D9E44,
  delme=814D9E44
```

Site-to-site VPN between FortiGate unit and Cisco PIX 501 router

Network topology

Figure 2: FortiGate-500 to Cisco PIX 501 Router network topology



Hardware and firmware specifications

Fortigate-500 gateway

Same as the one used in the previous example.

Cisco PIX 501 router

- Cisco PIX Firewall Version 6.3(0)144
- Cisco PIX Device Manager Version 3.0(0)133
- Hardware: PIX-501, 16 MB RAM, CPU Am5x86 133 MHz
- Flash E28F640J3 @ 0x3000000, 8MB
- BIOS Flash E28F640J3 @ 0xfffd8000, 128KB
- This PIX has a Restricted (R) license.

FortiGate-500 configuration

```
set system opmode nat

set system interface internal mode static ip 192.168.1.254
  255.255.255.0

set system interface external mode static ip 195.1.1.1
  255.255.255.0

set system hostname Fortigate-500

set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 195.1.1.2

set firewall address internal Internal_All subnet 0.0.0.0
  0.0.0.0

set firewall address external External_All subnet 0.0.0.0
  0.0.0.0

set firewall address dmz DMZ_All subnet 0.0.0.0 0.0.0.0

set firewall address internal 192_168_1_0 subnet 192.168.1.0
  255.255.255.0

set firewall address external 172_16_1_0 subnet 172.16.1.0
  255.255.255.0

set vpn ipsec phase1 to_Cisco_831 type static gw 195.1.1.2
  proposal 3des-sha1

keylife 28800 dhgrp 5  authmethod PSK fortigate nattraversal
  enable keepalive 5 dpd enable dpdidleworry 10
  dpdretrycount 3 dpdretryinterval 5 dpdidlecleanup 300
  peertype any xauthtype disable

set vpn ipsec phase2 to_172_16_1_0 phase1name to_Cisco_831
  proposal 3des-sha1  keylifeseconds 1800 dhgrp 1 replay
  enable concentrator none

set firewall policy srcintf internal dstintf external
  policyid 2 srcaddr 192_168_1_0 dstaddr 172_16_1_0 schedule
  Always service ANY action encrypt vpntunnel to_172_16_1_0
  inbound allow outbound allow

set firewall policy srcintf internal dstintf external
  policyid 1 srcaddr Internal_All dstaddr External_All
  schedule Always service ANY action accept avwebfilter Scan
  nat enable
```

Cisco PIX 501 router configuration

```
hostname pixfirewall

access-list 101 permit ip 172.16.1.0 255.255.255.0
  192.168.1.0 255.255.255.0

access-list 100 permit ip 172.16.1.0 255.255.255.0
  192.168.1.0 255.255.255.0

ip address outside 195.1.1.2 255.255.255.0
ip address inside 172.16.1.254 255.255.255.0
global (outside) 1 interface
nat (inside) 0 access-list 100
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 195.1.1.1 1
sysopt connection permit-ipsec
crypto ipsec transform-set ESP_3DES_SHA esp-3des esp-sha-hmac
crypto map VPN 10 ipsec-isakmp
crypto map VPN 10 match address 101
crypto map VPN 10 set peer 195.1.1.1
crypto map VPN 10 set transform-set ESP_3DES_SHA
crypto map VPN interface outside
isakmp enable outside
isakmp key fortigate address 195.1.1.1 netmask
  255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
```

Viewing the diagose results

FortiGate unit

Enter the following diagnose command:

```
diag debug app ike 2
```

The following results appear:

```
Get sa_connect message...195.1.1.1->195.1.1.2:500,
  natt_mode=0
Using new connection...natt_mode=0
Set connection name = to_Cisco_831.
Tunnel 195.1.1.1 ---> 195.1.1.2:500,natt_en=1 is starting
  negotiation
Initiator:main mode is sending 1st message...
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Sending NATT VID payload (draft3 and draft1)....
Initiator: sent 195.1.1.2 main mode message #1 (OK)
set retransmit: st=1, timeout=10.

Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xBC82EE9B0BEE827C, Len = 80
Received Payloads= SA
Initiator:main mode get 1st response...
test the peer keepalive status....
The peer does not send vid,not natt compatible.
Negotiate Result
Proposal_id = 1:
   Protocol_id = ISAKMP:
      trans_id = KEY_IKE.
      encapsulation = 0 (unknown)
         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
         type=OAKLEY_HASH_ALG, val=SHA.
         type=AUTH_METHOD, val=PRESHARED_KEY.
         type=OAKLEY_GROUP, val=1536.
Phase1 lifetimes=28800
Negotiate Success.(No echo).
testing the peer DPD status....
The peer does not send vid, not DPD compatible.
test the peer natt status....
The peer does not send vid,not natt compatible.
Initiator: sent 195.1.1.2 main mode message #2 (OK)
set retransmit: st=1, timeout=10.
Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xBC82EE9B0BEE827C, Len = 320
Received Payloads= KE NONCE VID VID VID VID
Initiator:main mode get 2nd response...
Responder: sent 195.1.1.2 main mode message #3 (OK)
set retransmit: st=1, timeout=10.
```

```
Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xBC82EE9B0BEE827C, Len = 76
Received Payloads= ID HASH
Initiator:main mode get 3rd response...
set gw: 0x8136cb8, timeout=28800.
Initiator: parsed 195.1.1.2 main mode message #3 (DONE)
Initiator:quick mode: pfs is not enabled
Try to negotiate with 1800 life seconds.
Initiator: sent 195.1.1.2 quick mode message #1 (OK)
set retransmit: st=2, timeout=10.
Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 5, Message id = 0xF9F8973D, Len = 84
#######  ISAKMP INFO ##########
Received Payloads= HASH Notif
######### Receive Information Payload(Protected)#########
   protocol_id=1, notify_msg=24578 (24578??), ispi_size=16
   spi=bc82ee9b0bee827c86d291336807f6ec
   Msg=
Comes 195.1.1.2:500->195.1.1.1:500,ifindex=5, external,
  vf_id=0....
Exchange Mode = 32, Message id = 0xBF571048, Len = 188
Received Payloads= HASH SA NONCE ID ID Notif
Initiator:quick mode get 1st response
Negotiate Result
Proposal_id = 1:
   Protocol_id = IPSEC_ESP:
      trans_id = ESP_3DES.
      encapsulation = ENCAPSULATION_MODE_TUNNEL
         type=AUTH_ALG, val=SHA1.
Phase2 esp lifetimes=1800
Using tunnel mode.
Negotiate Success.(No echo).
Initiator:Prepare to install sa.
Replay protection enable.
Set sa life soft seconds=1775.
Set sa life hard seconds=1800.
dport = 500.Initializing sa OK.
Initiator: sent 195.1.1.2 quick mode message #2 (DONE)
expire: st=2, timeout=120.
```

Cisco PIX 501 router

Enter the following command:

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

The following results appear:

```
crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 10
  policy
ISAKMP:      life type in seconds
ISAKMP:      life duration (basic) of 28800
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      auth pre-share
ISAKMP:      default group 5
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0:0): vendor ID is NAT-T
ISAKMP (0): processing vendor id payload
ISAKMP (0): SA is doing pre-shared key authentication using
  id type ID_FQDN
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500
```

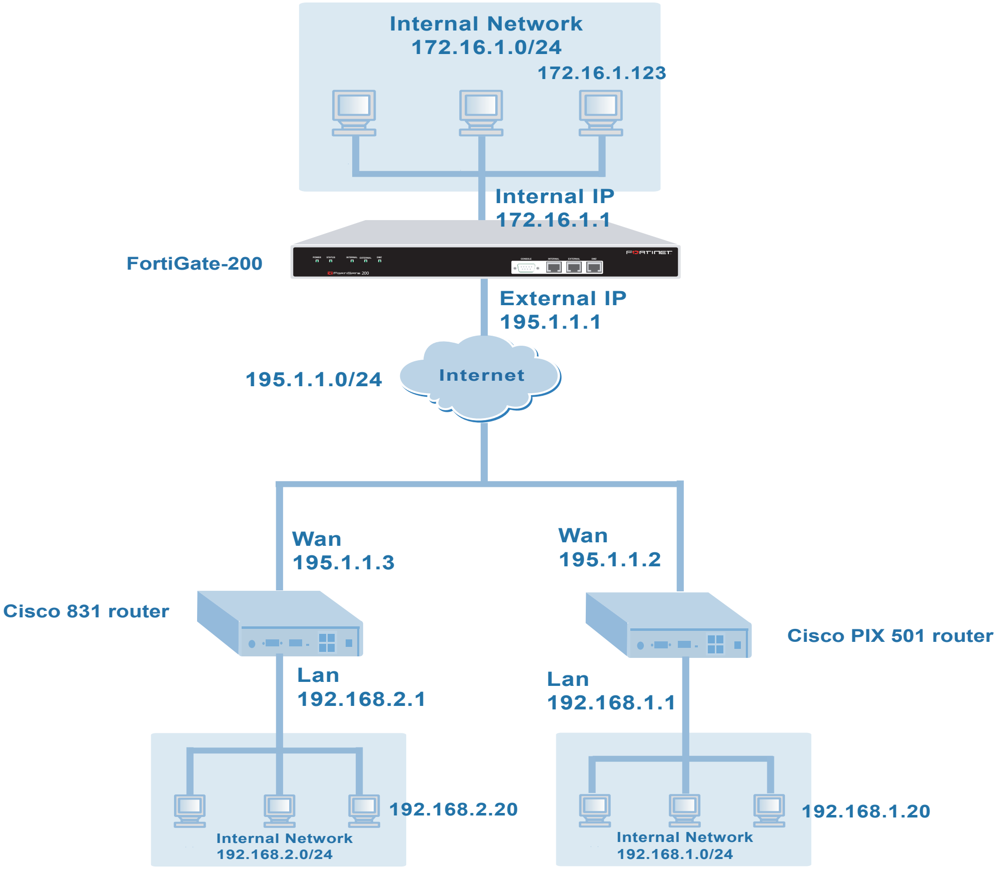
```
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
ISAKMP (0): ID payload
        next-payload : 8
        type         : 2
        protocol     : 17
        port         : 500
        length       : 15
ISAKMP (0): Total payload length: 19
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:195.1.1.1/500 Total VPN
  Peers:1
VPN Peer: ISAKMP: Peer ip:195.1.1.1/500 Ref cnt incremented
  to:1 Total VPN Peers:1
crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3210154056
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 1800
ISAKMP:      authenticator is HMAC-SHA
ISAKMP (0): atts are
  acceptable.IPSEC(validate_proposal_request): proposal
  part#1,
  (key eng. msg.) dest= 195.1.1.2, src= 195.1.1.1,
    dest_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 3210154056
ISAKMP (0): processing ID payload. message ID = 3210154056
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 192.168.1.0/255.255.255.0
  prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 3210154056
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 172.16.1.0/255.255.255.0
  prot 0 port 0IPSEC(
key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x522440ff(1378107647) for
  SA
        from       195.1.1.1 to       195.1.1.2 for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from       195.1.1.1 to       195.1.1.2
  (proxy     192.168.1.0 to      172.16.1.0)
        has spi 1378107647 and conn_id 1 and flags 4
        lifetime of 1800 seconds
        outbound SA from       195.1.1.2 to       195.1.1.1
  (proxy      172.16.1.0 to     192.168.1.0)
        has spi 3797658793 and conn_id 2 and flags 4
       lifetime of 1800 secondsIPSEC(key_engine): got a queue
  event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 195.1.1.2, src= 195.1.1.1,
    dest_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 1800s and 0kb,
    spi= 0x522440ff(1378107647), conn_id= 1, keysize= 0,
  flags= 0x4
```

```
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 195.1.1.2, dest= 195.1.1.1,
    src_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 1800s and 0kb,
    spi= 0xe25baca9(3797658793), conn_id= 2, keysize= 0,
  flags= 0x4
```

Hub-and-spoke VPN with Fortigate-200 unit as hub

Network topology

Figure 3: Hub-and-spoke VPN with FortiGate-200 unit as the hub



Hardware and firmware specifications

Fortigate 200 gateway

- Version:Fortigate-200 2.50,build133,031024
- virus-db:4.126(09/03/2003 18:03)
- ids-db:2.68(10/02/2003 15:14)
- Operation mode: Nat
- Hostname: Fortigate-200

Cisco PIX 501 router

Same as the one used in the previous example.

Cisco 831 router

- Cisco Internetwork Operating System Software
- IOS (tm) C831 Software (C831-K9O3SY6-M), Version 12.2(13)ZH1,
- EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
- Synched to technology version 12.2(14.5)T
- System image file: flash:c831-k9o3sy6-mz.122-13.ZH1.bin
- CISCO C831 (MPC857DSL) processor (revision 0x200) with 29492K/3276K bytes of memory.
- 2 Ethernet/IEEE 802.3 interface(s)
- 128K bytes of non-volatile configuration memory.
- 8192K bytes of processor board System flash (Read/Write)
- 2048K bytes of processor board Web flash (Read/Write)

FortiGate-200 configuration

```
set system interface internal mode static ip 172.16.1.1
  255.255.255.0

set system interface external mode static ip 195.1.1.1
  255.255.255.0

set system hostname Fortigate-200

set system route number 0 dst 192.168.1.0 255.255.255.0 gw1
  195.1.1.2

set system route number 1 dst 192.168.2.0 255.255.255.0 gw2
  195.1.1.3

set firewall address internal Internal_All subnet 0.0.0.0
  0.0.0.0

set firewall address external External_All subnet 0.0.0.0
  0.0.0.0

set firewall address internal 172_16_1_0 subnet 172.16.1.0
  255.255.255.0
```

```
set firewall address external 192_168_2_0 subnet 192.168.2.0
  255.255.255.0

set firewall address external 192_168_1_0 subnet 192.168.1.0
  255.255.255.0

set vpn ipsec phase1 to_192_168_1_0 type static gw 195.1.1.2
  proposal 3des-sha1 keylife 28800 dhgrp 5  authmethod PSK
  fortigate keepalive 5 dpd enable dpdidleworry 10
  dpdretrycount 3 dpdretryinterval 5 dpdidle cleanup 300
  peertype any xauthtype disable

set vpn ipsec phase1 to_192_168_2_0 type static gw 195.1.1.3
  proposal 3des-sha1 keylife 28800 dhgrp 5  authmethod PSK
  fortigate nattraversal enable keepalive 5 dpd enable
  dpdidleworry 10 dpdretrycount 3 dpdretryinterval 5
  dpdidlecleanup 300 peertype any xauthtype disable

set vpn ipsec phase2 to_192_168_1_0 phase1name to_192_168_1_0
  proposal 3des-sha1   keylifeseconds 1800 dhgrp 1 replay
  enable concentrator none

set vpn ipsec phase2 to_192_168_2_0 phase1name to_192_168_2_0
  proposal 3des-sha1 3des-md5  keylifeseconds 1800 dhgrp 1
  replay enable concentrator none

set vpn ipsec concentrator hub_and_spoke member
  to_192_168_2_0 to_192_168_1_0

set firewall policy srcintf internal dstintf external
  policyid 2 srcaddr Internal_All dstaddr 192_168_1_0
  schedule Always service ANY action encrypt vpntunnel
  to_192_168_1_0 inbound allow outbound allow

set firewall policy srcintf internal dstintf external
  policyid 3 srcaddr Internal_All dstaddr 192_168_2_0
  schedule Always service ANY action encrypt vpntunnel
  to_192_168_2_0 inbound allow outbound allow

set firewall policy srcintf internal dstintf external
  policyid 1 srcaddr Internal_All dstaddr External_All
  schedule Always service ANY action accept avwebfilter Scan
  nat enable
```

Cisco PIX 501 router configuration

```
hostname pixfirewall

access-list 100 permit ip 192.168.1.0 255.255.255.0 any

access-list 110 permit ip 192.168.1.0 255.255.255.0
  172.16.1.0 255.255.255.0

access-list 110 permit ip 192.168.1.0 255.255.255.0
  192.168.2.0 255.255.255.0

ip address outside 195.1.1.2 255.255.255.0

ip address inside 192.168.1.1 255.255.255.0
```

```
global (outside) 1 interface
nat (inside) 0 access-list 110
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 195.1.1.1 1
sysopt connection permit-ipsec
crypto ipsec transform-set ESP_3DES_SHA esp-3des esp-sha-hmac
crypto map VPN 10 ipsec-isakmp
crypto map VPN 10 match address 100
crypto map VPN 10 set peer 195.1.1.1
crypto map VPN 10 set transform-set ESP_3DES_SHA
crypto map VPN interface outside
isakmp enable outside
isakmp key fortigate address 195.1.1.1 netmask
  255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
```

Cisco 831 router configuration

```
hostname CiscoRouter
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 5
crypto isakmp key fortigate address 195.1.1.1
!
crypto ipsec transform-set ESP_3DES_SHA esp-3des esp-sha-hmac
!
crypto map VPN 10 ipsec-isakmp
 set peer 195.1.1.1
 set transform-set ESP_3DES_SHA
 match address 101
!
```

```
interface Ethernet0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet1
 ip address 195.1.1.3 255.255.255.0
 crypto map VPN
!
ip route 0.0.0.0 0.0.0.0 195.1.1.1
!
access-list 101 permit ip 192.168.2.0 0.0.0.255 any
```

Viewing the diagose results

FortiGate unit

Enter the following diagnose command:

```
diag debug app ike 2
```

The following results appear:

```
Comes 195.1.1.2:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0.
...
Exchange Mode = 2, I_COOKIE = 0xB68C98093DCB41E4, Len = 84
Set connection name = to_192_168_1_0.
Received Payloads= SA
Responder:main mode get 1st message...
test the peer keepalive status....
The peer does not send vid,not natt compatible.
testing the peer DPD status....
The peer does not send vid, not DPD compatible.
Negotiate Result
Proposal_id = 1:
   Protocol_id = ISAKMP:
      trans_id = KEY_IKE.
      encapsulation = 0 (unknown)
         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
         type=OAKLEY_HASH_ALG, val=SHA.
         type=AUTH_METHOD, val=PRESHARED_KEY.
         type=OAKLEY_GROUP, val=1536.
```

```
Phase1 lifetimes=86400
Sending VID payload....
Responder: sent 195.1.1.2 main mode message #1 (OK)
set retransmit: st=1, timeout=10.
Comes 195.1.1.2:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xB68C98093DCB41E4, Len = 320
Received Payloads= KE NONCE VID VID VID VID
Responder:main mode get 2nd message...
Responder: sent 195.1.1.2 main mode message #2 (OK)
set retransmit: st=1, timeout=10.

Comes 195.1.1.2:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xB68C98093DCB41E4, Len = 76
Received Payloads= ID HASH
Responder: main mode get 3rd message...
set gw: 0x8136c10, timeout=86400.
Responder: sent 195.1.1.2 main mode message #3 (DONE)

Comes 195.1.1.2:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 5, Message id = 0xE1A93271, Len = 84
#######  ISAKMP INFO ##########
Received Payloads= HASH Notif
######### Receive Information Payload(Protected)#########
   protocol_id=1, notify_msg=24578 (24578??), ispi_size=16
   spi=b68c98093dcb41e45836ed1576fdf085
   Msg=
Comes 195.1.1.2:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 32, Message id = 0xFB8FADE4, Len = 172
Received Payloads= HASH SA NONCE ID ID
Responder:quick mode get 1st message...
his proposal ids: peer:192.168.1.0(255.255.255.0),
  me:192.168.2.0(255.255.255.0)
kernel_comm.c, 118, tun_name=to_192_168_1_0
```

```
my policy ids: src:0.0.0.0(0.0.0.0),
  dst:192.168.1.0(255.255.255.0)
Got it
Found to_192_168_1_0:195.1.1.2.
Autokey to_192_168_1_0.
Negotiate Result
Proposal_id = 1:
   Protocol_id = IPSEC_ESP:
      trans_id = ESP_3DES.
      encapsulation = ENCAPSULATION_MODE_TUNNEL
         type=AUTH_ALG, val=SHA1.
Phase2 esp lifetimes=28800
negotiate:No pfs is set !
Using tunnel mode.
Responder:quick mode pfs is not enabled.
quick mode:idci type=4, len=8, chunk=c0a80100ffffff00
quick mode:idcr type=4, len=8, chunk=c0a80200ffffff00
Responder: sent 195.1.1.2 quick mode message #1 (OK)
set retransmit: st=3, timeout=10.

Comes 195.1.1.2:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 32, Message id = 0xFB8FADE4, Len = 60
Received Payloads= HASH
Replay protection enable.
Set sa life soft seconds=28775.
Set sa life hard seconds=28800.
Set sa life soft bytes=421527552.
Set sa life hard bytes=423624704.
dport = 500.Initializing sa OK.
Responder:quick mode done !
Responder: parsed 195.1.1.2 quick mode message #2 (DONE)
expire: st=3, timeout=120.
Get sa_connect message...195.1.1.1->195.1.1.3:500,
  natt_mode=0
Using new connection...natt_mode=0
Set connection name = to_192_168_2_0.
```

```
Tunnel 195.1.1.1 ---> 195.1.1.3:500,natt_en=1 is starting
  negotiation
Initiator:main mode is sending 1st message...
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Sending NATT VID payload (draft3 and draft1)....
Initiator: sent 195.1.1.3 main mode message #1 (OK)
set retransmit: st=4, timeout=10.

Comes 195.1.1.3:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xFCF94F5CF19487DE, Len = 100
Received Payloads= SA VID
Initiator:main mode get 1st response...
test the peer keepalive status....
Negotiate Result
Proposal_id = 1:
   Protocol_id = ISAKMP:
      trans_id = KEY_IKE.
      encapsulation = 0 (unknown)
         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
         type=OAKLEY_HASH_ALG, val=SHA.
         type=AUTH_METHOD, val=PRESHARED_KEY.
         type=OAKLEY_GROUP, val=1536.
Phase1 lifetimes=28800
Negotiate Success.(No echo).
testing the peer DPD status....
The peer does not send vid, not DPD compatible.
test the peer natt status....
The peer supports natt draft3.
Initiator: sent 195.1.1.3 main mode message #2 (OK)
set retransmit: st=4, timeout=10.
Comes 195.1.1.3:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xFCF94F5CF19487DE, Len = 368
Received Payloads= KE NONCE VID VID VID VID 130 130
```

```
Initiator:main mode get 2nd response...
Using IPS_NAT_MODE_NONE.
Responder: sent 195.1.1.3 main mode message #3 (OK)
set retransmit: st=4, timeout=10.

Comes 195.1.1.3:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xFCF94F5CF19487DE, Len = 68
Received Payloads= ID HASH
Initiator:main mode get 3rd response...
set gw: 0x8138d60, timeout=28800.
Initiator: parsed 195.1.1.3 main mode message #3 (DONE)
Initiator:quick mode: pfs is not enabled
Try to negotiate with 1800 life seconds.
Try to negotiate with 1800 life seconds.
Initiator: sent 195.1.1.3 quick mode message #1 (OK)
set retransmit: st=5, timeout=10.
Comes 195.1.1.3:500->195.1.1.1:500,ifindex=3, external,
  vf_id=0....
Exchange Mode = 32, Message id = 0x70B7A410, Len = 188
Received Payloads= HASH SA NONCE ID ID Notif
Initiator:quick mode get 1st response
Negotiate Result
Proposal_id = 1:
   Protocol_id = IPSEC_ESP:
      trans_id = ESP_3DES.
      encapsulation = ENCAPSULATION_MODE_TUNNEL
         type=AUTH_ALG, val=SHA1.
Phase2 esp lifetimes=1800
Using tunnel mode.
Negotiate Success.(No echo).
Initiator:Prepare to install sa.
Replay protection enable.
Set sa life soft seconds=1775.
Set sa life hard seconds=1800.
dport = 500.Initializing sa OK.
Initiator: sent 195.1.1.3 quick mode message #2 (DONE)
```

```
expire: st=5, timeout=120.
```

Cisco PIX 501 router

Enter the following commands:

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

The following results appear:

```
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500

OAK_MM exchange

ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10
  policy

ISAKMP:      encryption 3DES-CBC

ISAKMP:      hash SHA

ISAKMP:      default group 5

ISAKMP:      auth pre-share

ISAKMP:      life type in seconds

ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80

ISAKMP (0): atts are acceptable. Next payload is 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): SA is doing pre-shared key authentication using
  id type ID_FQDN

return status is IKMP_NO_ERROR

crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500

OAK_MM exchange

ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): ID payload

next-payload : 8

type         : 2

protocol     : 17

port         : 500

length       : 15

ISAKMP (0): Total payload length: 19

return status is IKMP_NO_ERROR
```

```
crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500

OAK_MM exchange

ISAKMP (0): processing ID payload. message ID = 0

ISAKMP (0): processing HASH payload. message ID = 0

ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M-ID of -
  74469916:fb8fade4IPSEC(key_engine): got a queue event...

IPSEC(spi_response): getting spi 0xfc67e9e3(4234668515) for
  SA

from       195.1.1.1 to       195.1.1.2 for prot 3

return status is IKMP_NO_ERROR

ISAKMP (0): sending INITIAL_CONTACT notify

ISAKMP (0): sending NOTIFY message 24578 protocol 1

VPN Peer: ISAKMP: Added new peer: ip:195.1.1.1/500 Total VPN
  Peers:1

VPN Peer: ISAKMP: Peer ip:195.1.1.1/500 Ref cnt incremented
  to:1 Total VPN Peers:1

crypto_isakmp_process_block:src:195.1.1.1, dest:195.1.1.2
  spt:500 dpt:500

OAK_QM exchange

oakley_process_quick_mode:

OAK_QM_IDLE

ISAKMP (0): processing SA payload. message ID = 4220497380

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES

ISAKMP:   attributes in transform:

ISAKMP:      encaps is 1

ISAKMP:      SA life type in seconds

ISAKMP:      SA life duration (basic) of 28800

ISAKMP:      SA life type in kilobytes

ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0

ISAKMP:      authenticator is HMAC-SHA

ISAKMP (0): atts are
  acceptable.IPSEC(validate_proposal_request): proposal part
  #1,

  (key eng. msg.) dest= 195.1.1.1, src= 195.1.1.2,

    dest_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 4220497380
ISAKMP (0): processing ID payload. message ID = 4220497380
ISAKMP (0): processing ID payload. message ID = 4220497380
ISAKMP (0): Creating IPSec SAs
        inbound SA from       195.1.1.1 to       195.1.1.2
  (proxy     192.168.2.0 to     192.168.1.0)
        has spi 4234668515 and conn_id 1 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from       195.1.1.2 to       195.1.1.1
  (proxy     192.168.1.0 to     192.168.2.0)
        has spi 3671954716 and conn_id 2 and flags 4
        lifetime of 28800 seconds
       lifetime of 4608000 kilobytesIPSEC(key_engine): got a
  queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 195.1.1.2, src= 195.1.1.1,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xfc67e9e3(4234668515), conn_id= 1, keysize= 0,
  flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 195.1.1.2, dest= 195.1.1.1,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xdadd951c(3671954716), conn_id= 2, keysize= 0,
  flags= 0x4
VPN Peer: IPSEC: Peer ip:195.1.1.1/500 Ref cnt incremented
  to:2 Total VPN Peers:1
```

```
VPN Peer: IPSEC: Peer ip:195.1.1.1/500 Ref cnt incremented
  to:3 Total VPN Peers:1

return status is IKMP_NO_ERROR
```

Cisco 831 router

Enter the following commands:

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

The following results appear:

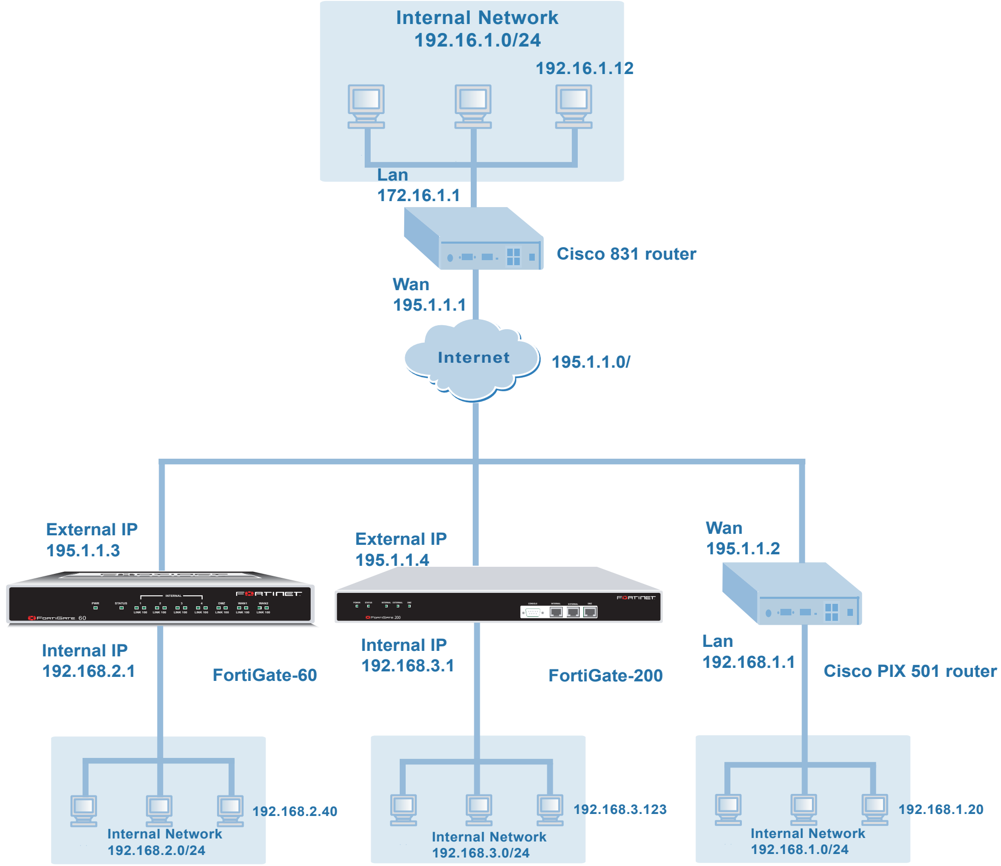
```
*Mar  1 02:05:41.847: ISAKMP: received ke message (1/1)

*Mar  1 02:05:41.847: ISAKMP: set new node 0 to QM_IDLE

*Mar  1 02:05:41.855: ISAKMP (0:3): sitting IDLE. Starting QM
  immediately (QM_IDLE      )

*Mar  1 02:05:41.855: ISAKMP (0:3): beginning Quick Mode
  exchange, M-ID of 1818846052

*Mar  1 02:05:41.859: ISAKMP (0:3): sending packet to
  195.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE

*Mar  1 02:05:41.859: ISAKMP (0:3): Node 1818846052, Input =
  IKE_MESG_INTERNAL, IKE_INIT_QM

*Mar  1 02:05:41.859: ISAKMP (0:3): Old State = IKE_QM_READY
  New State = IKE_QM_I_QM1

*Mar  1 02:05:41.875: ISAKMP (0:3): received packet from
  195.1.1.1 dport 500 sport 500 Global (R) QM_IDLE

*Mar  1 02:05:41.879: ISAKMP (0:3): processing HASH payload.
  message ID = 1818846052

*Mar  1 02:05:41.879: ISAKMP (0:3): processing SA payload.
  message ID = 1818846052

*Mar  1 02:05:41.879: ISAKMP (0:3): Checking IPSec proposal 1

*Mar  1 02:05:41.879: ISAKMP: transform 1, ESP_3DES

*Mar  1 02:05:41.879: ISAKMP:   attributes in transform:

*Mar  1 02:05:41.879: ISAKMP:      encaps is 1

*Mar  1 02:05:41.883: ISAKMP:      SA life type in seconds

*Mar  1 02:05:41.883: ISAKMP:      SA life duration (basic) of
  3600

*Mar  1 02:05:41.883: ISAKMP:      SA life type in kilobytes

*Mar  1 02:05:41.883: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0

*Mar  1 02:05:41.883: ISAKMP:      authenticator is HMAC-SHA

*Mar  1 02:05:41.883: ISAKMP (0:3): atts are acceptable.

*Mar  1 02:05:41.883: IPSEC(validate_proposal_request):
  proposal part #1,
  (key eng. msg.) INBOUND local= 195.1.1.3, remote=
  195.1.1.1,

   local_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),

   remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),

   protocol= ESP, transform= esp-3des esp-sha-hmac ,

   lifedur= 0s and 0kb,

   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2

*Mar  1 02:05:41.887: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 02:05:41.887: ISAKMP (0:3): processing NONCE payload.
  message ID = 1818846052

*Mar  1 02:05:41.887: ISAKMP (0:3): processing ID payload.
  message ID = 1818846052

*Mar  1 02:05:41.887: ISAKMP (0:3): processing ID payload.
  message ID = 1818846052

*Mar  1 02:05:41.903: ISAKMP (0:3): Creating IPSec SAs

*Mar  1 02:05:41.903:         inbound SA from 195.1.1.1 to
  195.1.1.3 (f/i)  0/ 0

        (proxy 0.0.0.0 to 192.168.2.0)

*Mar  1 02:05:41.903:         has spi 0x4BD7B1C3 and conn_id
  20 and flags 2

*Mar  1 02:05:41.903:         lifetime of 3600 seconds

*Mar  1 02:05:41.903:         lifetime of 4608000 kilobytes

*Mar  1 02:05:41.903:         has client flags 0x0

*Mar  1 02:05:41.903:        outbound SA from 195.1.1.3
  to 195.1.1.1       (f/i)  0/ 0 (proxy 192.168.2.0     to
  0.0.0.0        )

*Mar  1 02:05:41.903:         has spi -205844784 and conn_id
  21 and flags A

*Mar  1 02:05:41.903:         lifetime of 3600 seconds

*Mar  1 02:05:41.903:         lifetime of 4608000 kilobytes

*Mar  1 02:05:41.907:         has client flags 0x0

*Mar  1 02:05:41.907: IPSEC(key_engine): got a queue event...

*Mar  1 02:05:41.907: IPSEC(initialize_sas): ,

  (key eng. msg.) INBOUND local= 195.1.1.3, remote=
  195.1.1.1,

   local_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),

   remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),

   protocol= ESP, transform= esp-3des esp-sha-hmac ,
      lifedur= 3600s and 4608000kb,

      spi= 0x4BD7B1C3(1272426947), conn_id= 20, keysize= 0,
    flags= 0x2

*Mar  1 02:05:41.911: IPSEC(initialize_sas): ,

    (key eng. msg.) OUTBOUND local= 195.1.1.3, remote=
    195.1.1.1,

      local_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),

      remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),

      protocol= ESP, transform= esp-3des esp-sha-hmac ,

      lifedur= 3600s and 4608000kb,

      spi= 0xF3BB0ED0(4089122512), conn_id= 21, keysize= 0,
    flags= 0xA

*Mar  1 02:05:41.911: IPSEC(kei_proxy): head = VPN, map->ivrf
    = , kei->ivrf =

*Mar  1 02:05:41.911: IPSEC(add mtree): src 192.168.2.0, dest
    0.0.0.0, dest_port 0

*Mar  1 02:05:41.911: IPSEC(create_sa): sa created,

    (sa) sa_dest= 195.1.1.3, sa_prot= 50,

      sa_spi= 0x4BD7B1C3(1272426947),

      sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 20

*Mar  1 02:05:41.915: IPSEC(create_sa): sa created,

    (sa) sa_dest= 195.1.1.1, sa_prot= 50,

      sa_spi= 0xF3BB0ED0(4089122512),

      sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 21

*Mar  1 02:05:41.915: ISAKMP (0:3): sending packet to
    195.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE

*Mar  1 02:05:41.915: ISAKMP (0:3): deleting node 1818846052
    error FALSE reason ""

*Mar  1 02:05:41.915: ISAKMP (0:3): Node 1818846052, Input =
    IKE_MESG_FROM_PEER, IKE_QM_EXCH

*Mar  1 02:05:41.915: ISAKMP (0:3): Old State = IKE_QM_I_QM1
    New State = IKE_QM_PHASE2_COMPLETE

CiscoRouter#
```

Hub-and-spoke VPN with Cisco 831 router as hub

Network topology

Figure 4: Hub-and-spoke VPN with Cisco 831 router as the hub

\



Hardware and firmware specifications

Fortigate-200 gateway

Same as the one used in the previous example.

FortiGate-60 gateway

- Version:Fortigate-60 2.50,build133,031024
- virus-db:4.126(09/03/2003 18:03)
- ids-db:2.68(10/02/2003 15:14)
- Operation mode: Nat
- Hostname: Fortigate-60

Cisco PIX 501 router

Same as the one used in the previous example.

Cisco 831 router

Same as the one used in the previous example.

Cisco 831 router configuration

```
hostname Router
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 5
crypto isakmp key fortigate address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
crypto map VPN 10 ipsec-isakmp
 set peer 195.1.1.2
 set transform-set ESP-3DES-SHA
 match address 101
crypto map VPN 11 ipsec-isakmp
 set peer 195.1.1.3
 set transform-set ESP-3DES-SHA
 match address 102
crypto map VPN 12 ipsec-isakmp
 set peer 195.1.1.4
 set transform-set ESP-3DES-SHA
 match address 103
!
interface Ethernet0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet1
 ip address 195.1.1.1 255.255.255.0
 crypto map VPN
```

```
!
ip route 0.0.0.0 0.0.0.0 195.1.1.2
!
access-list 101 permit ip any 192.168.1.0 0.0.0.255
access-list 102 permit ip any 192.168.2.0 0.0.0.255
access-list 103 permit ip any 192.168.3.0 0.0.0.255
!
end
```

Cisco PIX 501 router configuration

```
hostname pixfirewall
access-list 100 permit ip 192.168.1.0 255.255.255.0 any
access-list 110 permit ip 192.168.1.0 255.255.255.0
  172.16.1.0 255.255.255.0
access-list 110 permit ip 192.168.1.0 255.255.255.0
  192.168.2.0 255.255.255.0
access-list 110 permit ip 192.168.1.0 255.255.255.0
  192.168.3.0 255.255.255.0
ip address outside 195.1.1.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
global (outside) 1 interface
nat (inside) 0 access-list 110
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 195.1.1.1 1
sysopt connection permit-ipsec
crypto ipsec transform-set ESP_3DES_SHA esp-3des esp-sha-hmac
crypto map VPN 10 ipsec-isakmp
crypto map VPN 10 match address 100
crypto map VPN 10 set peer 195.1.1.1
crypto map VPN 10 set transform-set ESP_3DES_SHA
crypto map VPN interface outside
isakmp enable outside
isakmp key ******** address 195.1.1.1 netmask 255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
```

FortiGate-200 configuration

```
set system opmode nat

set system interface internal mode static ip 192.168.2.1
  255.255.255.0

set system interface external mode static ip 195.1.1.3
  255.255.255.0

set system hostname Fortigate-200

set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 195.1.1.1

set firewall address internal Internal_All subnet 0.0.0.0
  0.0.0.0

set firewall address external External_All subnet 0.0.0.0
  0.0.0.0

set firewall address internal 192_168_2_0 subnet 192.168.2.0
  255.255.255.0

set firewall address external 172_16_1_0 subnet 172.16.1.0
  255.255.255.0

set firewall address external 192_168_1_0 subnet 192.168.1.0
  255.255.255.0

set firewall address external 192_168_3_0 subnet 192.168.3.0
  255.255.255.0

set firewall addrgrp external HUB_N_SPOKE member 172_16_1_0
  192_168_1_0 192_168_3_0

set vpn ipsec phase1 To_hub_172_16_1_0 type static gw
  195.1.1.1 proposal 3des-sha1   keylife 28800 dhgrp 5
  authmethod PSK fortigate nattraversal enable keepalive 5
  dpd enable dpdidleworry 10 dpdretrycount 3
  dpdretryinterval 5 dpdidlecleanup 300 peertype any
  xauthtype disable

set vpn ipsec phase2 to_hub_172_16_1_0 phase1name
  To_hub_172_16_1_0   proposal 3des-sha1   keylifeseconds
  1800 dhgrp 1 replay enable concentrator none

set firewall policy srcintf internal dstintf external
  policyid 3 srcaddr 192_168_2_0 dstaddr External_All
  schedule Always service ANY action encrypt vpntunnel
  to_hub_172_16_1_0 inbound allow

set firewall policy srcintf internal dstintf external
  policyid 2 srcaddr 192_168_2_0 dstaddr HUB_N_SPOKE
  schedule Always service ANY action encrypt vpntunnel
  to_hub_172_16_1_0 outbound allow
```

```
set firewall policy srcintf internal dstintf external
  policyid 1 srcaddr Internal_All dstaddr External_All
  schedule Always service ANY action accept avwebfilter Scan
  nat enable
```

FortiGate-60 configuration

```
set system opmode nat

set system interface internal mode static ip 192.168.3.1
  255.255.255.0

set system interface wan1 mode static ip 195.1.1.4
  255.255.255.0

set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 195.1.1.1

set firewall address internal Internal_All subnet 0.0.0.0
  0.0.0.0

set firewall address wan1 WAN1_All subnet 0.0.0.0 0.0.0.0

set firewall address internal 192_168_3_0 subnet 192.168.3.0
  255.255.255.0

set firewall address wan1 172_16_1_0 subnet 172.16.1.0
  255.255.255.0

set firewall address wan1 192_168_1_0 subnet 192.168.1.0
  255.255.255.0

set firewall address wan1 192_168_2_0 subnet 192.168.2.0
  255.255.255.0

set firewall addrgrp wan1 HUB_N_SPOKE member 172_16_1_0
  192_168_2_0 192_168_1_0

set vpn ipsec phase1 To_Hub type static gw 195.1.1.1 proposal
  3des-sha1 3des-md5  keylife 28800 dhgrp 5  authmethod PSK
  fortigate nattraversal enable keepalive 5 dpd enable
  dpdidleworry 10 dpdretrycount 3 dpdretryinterval 5
  dpdidlecleanup 300 peertype any xauthtype disable

set vpn ipsec phase2 To_Hub phase1name To_Hub   proposal
  3des-sha1   keylifeseconds 1800 dhgrp 1 replay enable
  concentrator none

set firewall policy srcintf internal dstintf wan1 policyid 3
  srcaddr 192_168_3_0 dstaddr WAN1_All schedule Always
  service ANY action encrypt vpntunnel To_Hub inbound allow

set firewall policy srcintf internal dstintf wan1 policyid 2
  srcaddr 192_168_3_0 dstaddr HUB_N_SPOKE schedule Always
  service ANY action encrypt vpntunnel To_Hub outbound allow

set firewall policy srcintf internal dstintf wan1 policyid 1
  srcaddr Internal_All dstaddr WAN1_All schedule Always
  service ANY action accept avwebfilter Scan nat enable
```

Viewing the diagose results

Cisco 831 router

Enter the following commands:

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

The following results appear:

```
*Mar  1 00:01:07.827: ISAKMP (0:0): received packet from
  195.1.1.3 dport 500 sport 500 Global (N) NEW SA

*Mar  1 00:01:07.827: ISAKMP: local port 500, remote port 500

*Mar  1 00:01:07.827: ISAKMP: insert sa successfully sa =
  81058984

*Mar  1 00:01:07.831: ISAKMP (0:1): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:01:07.831: ISAKMP (0:1): Old State = IKE_READY
  New State = IKE_R_MM1

*Mar  1 00:01:07.831: ISAKMP (0:1): processing SA payload.
  message ID = 0

*Mar  1 00:01:07.831: ISAKMP (0:1): processing vendor id
  payload

*Mar  1 00:01:07.831: ISAKMP (0:1:): vendor ID seems
  Unity/DPD but hash mismatch

*Mar  1 00:01:07.831: ISAKMP (0:1): processing vendor id
  payload

*Mar  1 00:01:07.831: ISAKMP (0:1): vendor ID seems Unity/DPD
  but major 233 mismatch

*Mar  1 00:01:07.835: ISAKMP (0:1): processing vendor id
  payload

*Mar  1 00:01:07.835: ISAKMP (0:1): vendor ID seems Unity/DPD
  but major 157 mismatch

*Mar  1 00:01:07.835: ISAKMP (0:1): vendor ID is NAT-T v3

*Mar  1 00:01:07.835: ISAKMP (0:1): processing vendor id
  payload

*Mar  1 00:01:07.835: ISAKMP (0:1): vendor ID seems Unity/DPD
  but major 221 mismatch

*Mar  1 00:01:07.835: ISAKMP: Looking for a matching key for
  195.1.1.3 in default : success

*Mar  1 00:01:07.835: ISAKMP (0:1): found peer pre-shared key
  matching 195.1.1.3

*Mar  1 00:01:07.835: ISAKMP (0:1) local preshared key found

*Mar  1 00:01:07.835: ISAKMP : Scanning profiles for xauth
  ...
```

```
*Mar  1 00:01:07.835: ISAKMP (0:1): Checking ISAKMP transform
  1 against priority 10 policy

*Mar  1 00:01:07.839: ISAKMP:      life type in seconds

*Mar  1 00:01:07.839: ISAKMP:      life duration (basic) of
  28800

*Mar  1 00:01:07.839: ISAKMP:      encryption 3DES-CBC

*Mar  1 00:01:07.839: ISAKMP:      hash SHA

*Mar  1 00:01:07.839: ISAKMP:      auth pre-share

*Mar  1 00:01:07.839: ISAKMP:      default group 5

*Mar  1 00:01:07.839: ISAKMP (0:1): atts are acceptable. Next
  payload is 0

*Mar  1 00:01:09.243: ISAKMP (0:1): processing vendor id
  payload

*Mar  1 00:01:09.243: ISAKMP (0:1:): vendor ID seems
  Unity/DPD but hash mismatch

*Mar  1 00:01:09.243: ISAKMP (0:1): processing vendor id
  payload

*Mar  1 00:01:09.243: ISAKMP (0:1): vendor ID seems Unity/DPD
  but major 233 mismatch

*Mar  1 00:01:09.243: ISAKMP (0:1): processing vendor id
  payload

*Mar  1 00:01:09.243: ISAKMP (0:1): vendor ID seems Unity/DPD
  but major 157 mismatch

*Mar  1 00:01:09.243: ISAKMP (0:1): vendor ID is NAT-T v3

*Mar  1 00:01:09.243: ISAKMP (0:1): processing vendor id
  payload

*Mar  1 00:01:09.247: ISAKMP (0:1): vendor ID seems Unity/DPD
  but major 221 mismatch

*Mar  1 00:01:09.247: ISAKMP (0:1): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:01:09.247: ISAKMP (0:1): Old State = IKE_R_MM1
  New State = IKE_R_MM1

*Mar  1 00:01:09.247: ISAKMP (0:1): constructed NAT-T vendor-
  03 ID

*Mar  1 00:01:09.247: ISAKMP (0:1): sending packet to
  195.1.1.3 my_port 500 peer_port 500 (R) MM_SA_SETUP

*Mar  1 00:01:09.251: ISAKMP (0:1): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:09.251: ISAKMP (0:1): Old State = IKE_R_MM1
  New State = IKE_R_MM2
```

```
*Mar  1 00:01:09.299: ISAKMP (0:1): received packet from
  195.1.1.3 dport 500 sport 500 Global (R) MM_SA_SETUP

*Mar  1 00:01:09.303: ISAKMP (0:1): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:01:09.303: ISAKMP (0:1): Old State = IKE_R_MM2
  New State = IKE_R_MM3

*Mar  1 00:01:09.303: ISAKMP (0:1): processing KE payload.
  message ID = 0

*Mar  1 00:01:10.707: ISAKMP (0:1): processing NONCE payload.
  message ID = 0

*Mar  1 00:01:10.711: ISAKMP: Looking for a matching key for
  195.1.1.3 in default : success

*Mar  1 00:01:10.711: ISAKMP (0:1): found peer pre-shared key
  matching 195.1.1.3

*Mar  1 00:01:10.711: ISAKMP (0:1): SKEYID state generated

*Mar  1 00:01:10.711: ISAKMP:received payload type 17

*Mar  1 00:01:10.711: ISAKMP (0:1): Detected NAT-D payload

*Mar  1 00:01:10.711: ISAKMP (0:1): NAT match MINE hash

*Mar  1 00:01:10.711: ISAKMP:received payload type 17

*Mar  1 00:01:10.711: ISAKMP (0:1): Detected NAT-D payload

*Mar  1 00:01:10.711: ISAKMP (0:1): NAT match HIS hash

*Mar  1 00:01:10.711: ISAKMP (0:1): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:01:10.711: ISAKMP (0:1): Old State = IKE_R_MM3
  New State = IKE_R_MM3

*Mar  1 00:01:10.715: ISAKMP (0:1): constructed HIS NAT-D

*Mar  1 00:01:10.715: ISAKMP (0:1): constructed MINE NAT-D

*Mar  1 00:01:10.715: ISAKMP (0:1): sending packet to
  195.1.1.3 my_port 500 peer_port 500 (R) MM_KEY_EXCH

*Mar  1 00:01:10.715: ISAKMP (0:1): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:10.715: ISAKMP (0:1): Old State = IKE_R_MM3
  New State = IKE_R_MM4

*Mar  1 00:01:10.755: ISAKMP (0:1): received packet from
  195.1.1.3 dport 500 sport 500 Global (R) MM_KEY_EXCH

*Mar  1 00:01:10.755: ISAKMP (0:1): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:01:10.759: ISAKMP (0:1): Old State = IKE_R_MM4
  New State = IKE_R_MM5

*Mar  1 00:01:10.759: ISAKMP (0:1): processing ID payload.
  message ID = 0
```

```
*Mar  1 00:01:10.759: ISAKMP (0:1): peer matches *none* of
  the profiles

*Mar  1 00:01:10.759: ISAKMP (0:1): processing HASH payload.
  message ID = 0

*Mar  1 00:01:10.763: ISAKMP (0:1): SA has been authenticated
  with 195.1.1.3

*Mar  1 00:01:10.763: ISAKMP (0:1): peer matches *none* of
  the profiles

*Mar  1 00:01:10.763: ISAKMP (0:1): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:01:10.763: ISAKMP (0:1): Old State = IKE_R_MM5
  New State = IKE_R_MM5

*Mar  1 00:01:10.763: ISAKMP (0:1): SA is doing pre-shared
  key authentication using id type ID_IPV4_ADDR

*Mar  1 00:01:10.763: ISAKMP (1): ID payload

next-payload : 8

type         : 1

addr         : 195.1.1.1

protocol     : 17

port         : 500

length       : 8

*Mar  1 00:01:10.767: ISAKMP (1): Total payload length: 12

*Mar  1 00:01:10.771: ISAKMP (0:1): sending packet to
  195.1.1.3 my_port 500 peer_port 500 (R) MM_KEY_EXCH

*Mar  1 00:01:10.779: ISAKMP (0:1): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:10.779: ISAKMP (0:1): Old State = IKE_R_MM5
  New State = IKE_P1_COMPLETE

*Mar  1 00:01:10.779: ISAKMP (0:1): Input =
  IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

*Mar  1 00:01:10.779: ISAKMP (0:1): Old State =
  IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Mar  1 00:01:10.783: ISAKMP (0:1): received packet from
  195.1.1.3 dport 500 sport 500 Global (R) QM_IDLE

*Mar  1 00:01:10.783: ISAKMP: set new node -1239048969 to
  QM_IDLE

*Mar  1 00:01:10.783: ISAKMP (0:1): processing HASH payload.
  message ID = -1239048969

*Mar  1 00:01:10.783: ISAKMP (0:1): processing SA payload.
  message ID = -1239048969

*Mar  1 00:01:10.783: ISAKMP (0:1): Checking IPSec proposal 1
```

```
*Mar  1 00:01:10.783: ISAKMP: transform 1, ESP_3DES
*Mar  1 00:01:10.787: ISAKMP:   attributes in transform:
*Mar  1 00:01:10.787: ISAKMP:      encaps is 1
*Mar  1 00:01:10.787: ISAKMP:      SA life type in seconds
*Mar  1 00:01:10.787: ISAKMP:      SA life duration (basic) of
   1800
*Mar  1 00:01:10.787: ISAKMP:      authenticator is HMAC-SHA
*Mar  1 00:01:10.787: ISAKMP (0:1): atts are acceptable.
*Mar  1 00:01:10.787: IPSEC(validate_proposal_request):
   proposal part #1,
   (key eng. msg.) INBOUND local= 195.1.1.1, remote=
   195.1.1.3,
     local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
     remote_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
     protocol= ESP, transform= esp-3des esp-sha-hmac ,
     lifedur= 0s and 0kb,
     spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar  1 00:01:10.791: IPSEC(kei_proxy): head = VPN, map->ivrf
   = , kei->ivrf =
*Mar  1 00:01:10.791: IPSEC(kei_proxy): head = VPN, map->ivrf
   = , kei->ivrf =
*Mar  1 00:01:10.791: ISAKMP (0:1): processing NONCE payload.
   message ID = -1239048969
*Mar  1 00:01:10.791: ISAKMP (0:1): processing ID payload.
   message ID = -1239048969
*Mar  1 00:01:10.791: ISAKMP (0:1): processing ID payload.
   message ID = -1239048969
*Mar  1 00:01:10.791: ISAKMP (0:1): asking for 1 spis from
   ipsec
*Mar  1 00:01:10.791: ISAKMP (0:1): Node -1239048969, Input =
   IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Mar  1 00:01:10.795: ISAKMP (0:1): Old State = IKE_QM_READY
   New State = IKE_QM_SPI_STARVE
*Mar  1 00:01:10.795: IPSEC(key_engine): got a queue event...
*Mar  1 00:01:10.803: IPSEC(spi_response): getting spi
   1550015024 for SA
from 195.1.1.1       to 195.1.1.3       for prot 3
*Mar  1 00:01:10.807: ISAKMP: received ke message (2/1)
*Mar  1 00:01:11.047: ISAKMP (0:1): sending packet to
   195.1.1.3 my_port 500 peer_port 500 (R) QM_IDLE
```

```
*Mar  1 00:01:11.047: ISAKMP (0:1): Node -1239048969, Input =
  IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY

*Mar  1 00:01:11.047: ISAKMP (0:1): Old State =
  IKE_QM_SPI_STARVE  New State = IKE_QM_R_QM2

*Mar  1 00:01:11.059: ISAKMP (0:1): received packet from
  195.1.1.3 dport 500 sport 500 Global (R) QM_IDLE

*Mar  1 00:01:11.071: ISAKMP (0:1): Creating IPSec SAs

*Mar  1 00:01:11.071:         inbound SA from 195.1.1.3 to
  195.1.1.1 (f/i)  0/ 0

        (proxy 192.168.2.0 to 0.0.0.0)

*Mar  1 00:01:11.071:         has spi 0x5C635A30 and conn_id
  20 and flags 2

*Mar  1 00:01:11.071:         lifetime of 1800 seconds

*Mar  1 00:01:11.071:         has client flags 0x0

*Mar  1 00:01:11.071:        outbound SA from 195.1.1.1
  to 195.1.1.3       (f/i)  0/ 0 (proxy 0.0.0.0         to
  192.168.2.0    )

*Mar  1 00:01:11.071:         has spi -836996023 and conn_id
  21 and flags A

*Mar  1 00:01:11.071:         lifetime of 1800 seconds

*Mar  1 00:01:11.071:         has client flags 0x0

*Mar  1 00:01:11.075: ISAKMP (0:1): deleting node -1239048969
  error FALSE reason "quick mode done (await)"

*Mar  1 00:01:11.075: ISAKMP (0:1): Node -1239048969, Input =
  IKE_MESG_FROM_PEER, IKE_QM_EXCH

*Mar  1 00:01:11.075: ISAKMP (0:1): Old State = IKE_QM_R_QM2
  New State = IKE_QM_PHASE2_COMPLETE

*Mar  1 00:01:11.075: IPSEC(key_engine): got a queue event...

*Mar  1 00:01:11.075: IPSEC(initialize_sas): ,

  (key eng. msg.) INBOUND local= 195.1.1.1, remote=
  195.1.1.3,

   local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),

   remote_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),

   protocol= ESP, transform= esp-3des esp-sha-hmac ,

   lifedur= 1800s and 0kb,

   spi= 0x5C635A30(1550015024), conn_id= 20, keysize= 0,
  flags= 0x2

*Mar  1 00:01:11.075: IPSEC(initialize_sas): ,

  (key eng. msg.) OUTBOUND local= 195.1.1.1, remote=
  195.1.1.3,
   local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
   remote_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 1800s and 0kb,
   spi= 0xCE1C7449(3457971273), conn_id= 21, keysize= 0,
  flags= 0xA
*Mar  1 00:01:11.079: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =
*Mar  1 00:01:11.079: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =
*Mar  1 00:01:11.079: IPSEC(add mtree): src 0.0.0.0, dest
  192.168.2.0, dest_port 0
*Mar  1 00:01:11.083: IPSEC(create_sa): sa created,
  (sa) sa_dest= 195.1.1.1, sa_prot= 50,
   sa_spi= 0x5C635A30(1550015024),
   sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 20
*Mar  1 00:01:11.083: IPSEC(create_sa): sa created,
  (sa) sa_dest= 195.1.1.3, sa_prot= 50,
   sa_spi= 0xCE1C7449(3457971273),
   sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 21
*Mar  1 00:01:12.603: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 195.1.1.1, remote=
  195.1.1.4,
   local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
   remote_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 3600s and 4608000kb,
   spi= 0xA920823E(2837479998), conn_id= 0, keysize= 0,
  flags= 0x400A
*Mar  1 00:01:12.607: ISAKMP: received ke message (1/1)
*Mar  1 00:01:12.607: ISAKMP (0:0): SA request profile is
  (NULL)
*Mar  1 00:01:12.607: ISAKMP: local port 500, remote port 500
*Mar  1 00:01:12.607: ISAKMP: set new node 0 to QM_IDLE
*Mar  1 00:01:12.611: ISAKMP: insert sa successfully sa =
  81421250
*Mar  1 00:01:12.611: ISAKMP (0:2): Can not start Aggressive
  mode, trying Main mode.
```

```
*Mar  1 00:01:12.611: ISAKMP: Looking for a matching key for
  195.1.1.4 in default : success

*Mar  1 00:01:12.611: ISAKMP (0:2): found peer pre-shared key
  matching 195.1.1.4

*Mar  1 00:01:12.611: ISAKMP (0:2): constructed NAT-T vendor-
  03 ID

*Mar  1 00:01:12.611: ISAKMP (0:2): constructed NAT-T vendor-
  02 ID

*Mar  1 00:01:12.611: ISAKMP (0:2): Input =
  IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM

*Mar  1 00:01:12.611: ISAKMP (0:2): Old State = IKE_READY
  New State = IKE_I_MM1

*Mar  1 00:01:12.615: ISAKMP (0:2): beginning Main Mode
  exchange

*Mar  1 00:01:12.615: ISAKMP (0:2): sending packet to
  195.1.1.4 my_port 500 peer_port 500 (I) MM_NO_STATE

*Mar  1 00:01:16.139: IPSEC(sa_request): ,

  (key eng. msg.) OUTBOUND local= 195.1.1.1, remote=
  195.1.1.2,

    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),

    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),

    protocol= ESP, transform= esp-3des esp-sha-hmac ,

    lifedur= 3600s and 4608000kb,

    spi= 0x5FFAFD(6290173), conn_id= 0, keysize= 0, flags=
  0x400A

*Mar  1 00:01:16.143: ISAKMP: received ke message (1/1)

*Mar  1 00:01:16.143: ISAKMP (0:0): SA request profile is
  (NULL)

*Mar  1 00:01:16.143: ISAKMP: local port 500, remote port 500

*Mar  1 00:01:16.143: ISAKMP: set new node 0 to QM_IDLE

*Mar  1 00:01:16.143: ISAKMP: insert sa successfully sa =
  81422594

*Mar  1 00:01:16.143: ISAKMP (0:3): Can not start Aggressive
  mode, trying Main mode.

*Mar  1 00:01:16.147: ISAKMP: Looking for a matching key for
  195.1.1.2 in default : success

*Mar  1 00:01:16.147: ISAKMP (0:3): found peer pre-shared key
  matching 195.1.1.2

*Mar  1 00:01:16.147: ISAKMP (0:3): constructed NAT-T vendor-
  03 ID
```

```
*Mar  1 00:01:16.147: ISAKMP (0:3): constructed NAT-T vendor-
  02 ID

*Mar  1 00:01:16.147: ISAKMP (0:3): Input =
  IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM

*Mar  1 00:01:16.147: ISAKMP (0:3): Old State = IKE_READY
  New State = IKE_I_MM1

*Mar  1 00:01:16.147: ISAKMP (0:3): beginning Main Mode
  exchange

*Mar  1 00:01:16.147: ISAKMP (0:3): sending packet to
  195.1.1.2 my_port 500 peer_port 500 (I) MM_NO_STATE

*Mar  1 00:01:22.615: ISAKMP (0:2): retransmitting phase 1
  MM_NO_STATE...

*Mar  1 00:01:22.615: ISAKMP (0:2): incrementing error
  counter on sa: retransmit phase 1

*Mar  1 00:01:22.615: ISAKMP (0:2): retransmitting phase 1
  MM_NO_STATE

*Mar  1 00:01:22.615: ISAKMP (0:2): sending packet to
  195.1.1.4 my_port 500 peer_port 500 (I) MM_NO_STATE

*Mar  1 00:01:22.635: ISAKMP (0:2): received packet from
  195.1.1.4 dport 500 sport 500 Global (I) MM_NO_STATE

*Mar  1 00:01:22.635: ISAKMP (0:2): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:01:22.635: ISAKMP (0:2): Old State = IKE_I_MM1
  New State = IKE_I_MM2

*Mar  1 00:01:22.639: ISAKMP (0:2): processing SA payload.
  message ID = 0

*Mar  1 00:01:22.639: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:01:22.639: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 233 mismatch

*Mar  1 00:01:22.639: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:01:22.639: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 157 mismatch

*Mar  1 00:01:22.639: ISAKMP (0:2): vendor ID is NAT-T v3

*Mar  1 00:01:22.639: ISAKMP: Looking for a matching key for
  195.1.1.4 in default : success

*Mar  1 00:01:22.639: ISAKMP (0:2): found peer pre-shared key
  matching 195.1.1.4

*Mar  1 00:01:22.639: ISAKMP (0:2) local preshared key found

*Mar  1 00:01:22.643: ISAKMP : Scanning profiles for xauth
  ...
```

```
*Mar  1 00:01:22.643: ISAKMP (0:2): Checking ISAKMP transform
  1 against priority 10 policy

*Mar  1 00:01:22.643: ISAKMP:      encryption 3DES-CBC

*Mar  1 00:01:22.643: ISAKMP:      hash SHA

*Mar  1 00:01:22.643: ISAKMP:      default group 5

*Mar  1 00:01:22.643: ISAKMP:      auth pre-share

*Mar  1 00:01:22.643: ISAKMP:      life type in seconds

*Mar  1 00:01:22.643: ISAKMP:      life duration (VPI) of  0x0
  0x1 0x51 0x80

*Mar  1 00:01:22.643: ISAKMP (0:2): atts are acceptable. Next
  payload is 0

*Mar  1 00:01:24.051: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:01:24.055: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 233 mismatch

*Mar  1 00:01:24.055: ISAKMP (0:2): processing vendor id
  payload

*Mar  1 00:01:24.055: ISAKMP (0:2): vendor ID seems Unity/DPD
  but major 157 mismatch

*Mar  1 00:01:24.055: ISAKMP (0:2): vendor ID is NAT-T v3

*Mar  1 00:01:24.055: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:01:24.055: ISAKMP (0:2): Old State = IKE_I_MM2
  New State = IKE_I_MM2

*Mar  1 00:01:24.059: ISAKMP (0:2): constructed HIS NAT-D

*Mar  1 00:01:24.059: ISAKMP (0:2): constructed MINE NAT-D

*Mar  1 00:01:24.059: ISAKMP (0:2): sending packet to
  195.1.1.4 my_port 500 peer_port 500 (I) MM_SA_SETUP

*Mar  1 00:01:24.059: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:24.059: ISAKMP (0:2): Old State = IKE_I_MM2
  New State = IKE_I_MM3

*Mar  1 00:01:24.179: ISAKMP (0:2): received packet from
  195.1.1.4 dport 500 sport 500 Global (I) MM_SA_SETUP

*Mar  1 00:01:24.179: ISAKMP (0:2): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:01:24.179: ISAKMP (0:2): Old State = IKE_I_MM3
  New State = IKE_I_MM4

*Mar  1 00:01:24.183: ISAKMP (0:2): processing KE payload.
  message ID = 0
```

```
*Mar  1 00:01:25.583: ISAKMP (0:2): processing NONCE payload.
  message ID = 0

*Mar  1 00:01:25.583: ISAKMP: Looking for a matching key for
  195.1.1.4 in default : success

*Mar  1 00:01:25.587: ISAKMP (0:2): found peer pre-shared key
  matching 195.1.1.4

*Mar  1 00:01:25.591: ISAKMP (0:2): SKEYID state generated

*Mar  1 00:01:25.591: ISAKMP:received payload type 17

*Mar  1 00:01:25.591: ISAKMP (0:2): Detected NAT-D payload

*Mar  1 00:01:25.591: ISAKMP (0:2): NAT match MINE hash

*Mar  1 00:01:25.591: ISAKMP:received payload type 17

*Mar  1 00:01:25.591: ISAKMP (0:2): Detected NAT-D payload

*Mar  1 00:01:25.591: ISAKMP (0:2): NAT match HIS hash

*Mar  1 00:01:25.591: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:01:25.591: ISAKMP (0:2): Old State = IKE_I_MM4
  New State = IKE_I_MM4

*Mar  1 00:01:25.595: ISAKMP (0:2): Send initial contact

*Mar  1 00:01:25.595: ISAKMP (0:2): SA is doing pre-shared
  key authentication using id type ID_IPV4_ADDR

*Mar  1 00:01:25.595: ISAKMP (2): ID payload

next-payload : 8

type         : 1

addr         : 195.1.1.1

protocol     : 17

port         : 500

length       : 8

*Mar  1 00:01:25.595: ISAKMP (2): Total payload length: 12

*Mar  1 00:01:25.599: ISAKMP (0:2): sending packet to
  195.1.1.4 my_port 500 peer_port 500 (I) MM_KEY_EXCH

*Mar  1 00:01:25.599: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:25.603: ISAKMP (0:2): Old State = IKE_I_MM4
  New State = IKE_I_MM5

*Mar  1 00:01:25.603: ISAKMP (0:2): received packet from
  195.1.1.4 dport 500 sport 500 Global (I) MM_KEY_EXCH

*Mar  1 00:01:25.607: ISAKMP (0:2): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH
```

```
*Mar  1 00:01:25.607: ISAKMP (0:2): Old State = IKE_I_MM5
  New State = IKE_I_MM6

*Mar  1 00:01:25.611: ISAKMP (0:2): processing ID payload.
  message ID = 0

*Mar  1 00:01:25.611: ISAKMP (0:2): processing HASH payload.
  message ID = 0

*Mar  1 00:01:25.611: ISAKMP (0:2): SA has been authenticated
  with 195.1.1.4

*Mar  1 00:01:25.615: ISAKMP (0:2): peer matches *none* of
  the profiles

*Mar  1 00:01:25.615: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:01:25.615: ISAKMP (0:2): Old State = IKE_I_MM6
  New State = IKE_I_MM6

*Mar  1 00:01:25.619: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:25.619: ISAKMP (0:2): Old State = IKE_I_MM6
  New State = IKE_P1_COMPLETE

*Mar  1 00:01:25.619: ISAKMP (0:2): beginning Quick Mode
  exchange, M-ID of -264072751

*Mar  1 00:01:25.631: ISAKMP (0:2): sending packet to
  195.1.1.4 my_port 500 peer_port 500 (I) QM_IDLE

*Mar  1 00:01:25.631: ISAKMP (0:2): Node -264072751, Input =
  IKE_MESG_INTERNAL, IKE_INIT_QM

*Mar  1 00:01:25.631: ISAKMP (0:2): Old State = IKE_QM_READY
  New State = IKE_QM_I_QM1

*Mar  1 00:01:25.631: ISAKMP (0:2): Input =
  IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

*Mar  1 00:01:25.631: ISAKMP (0:2): Old State =
  IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Mar  1 00:01:25.647: ISAKMP (0:2): received packet from
  195.1.1.4 dport 500 sport 500 Global (I) QM_IDLE

*Mar  1 00:01:25.651: ISAKMP (0:2): processing HASH payload.
  message ID = -264072751

*Mar  1 00:01:25.651: ISAKMP (0:2): processing SA payload.
  message ID = -264072751

*Mar  1 00:01:25.651: ISAKMP (0:2): Checking IPSec proposal 1

*Mar  1 00:01:25.651: ISAKMP: transform 1, ESP_3DES

*Mar  1 00:01:25.651: ISAKMP:   attributes in transform:

*Mar  1 00:01:25.651: ISAKMP:      encaps is 1

*Mar  1 00:01:25.651: ISAKMP:      SA life type in seconds
```

```
*Mar  1 00:01:25.651: ISAKMP:      SA life duration (basic) of
  3600

*Mar  1 00:01:25.651: ISAKMP:      SA life type in kilobytes

*Mar  1 00:01:25.651: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0

*Mar  1 00:01:25.655: ISAKMP:      authenticator is HMAC-SHA

*Mar  1 00:01:25.655: ISAKMP (0:2): atts are acceptable.

*Mar  1 00:01:25.655: IPSEC(validate_proposal_request):
  proposal part #1,

  (key eng. msg.) INBOUND local= 195.1.1.1, remote=
  195.1.1.4,

    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),

    remote_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),

    protocol= ESP, transform= esp-3des esp-sha-hmac ,

    lifedur= 0s and 0kb,

    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2

*Mar  1 00:01:25.655: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 00:01:25.659: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 00:01:25.659: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 00:01:25.659: ISAKMP (0:2): processing NONCE payload.
  message ID = -264072751

*Mar  1 00:01:25.659: ISAKMP (0:2): processing ID payload.
  message ID = -264072751

*Mar  1 00:01:25.659: ISAKMP (0:2): processing ID payload.
  message ID = -264072751

*Mar  1 00:01:25.671: ISAKMP (0:2): Creating IPSec SAs

*Mar  1 00:01:25.671:         inbound SA from 195.1.1.4 to
  195.1.1.1 (f/i)  0/ 0

        (proxy 192.168.3.0 to 0.0.0.0)

*Mar  1 00:01:25.671:         has spi 0xA920823E and conn_id
  22 and flags 2

*Mar  1 00:01:25.671:         lifetime of 3600 seconds

*Mar  1 00:01:25.671:         lifetime of 4608000 kilobytes

*Mar  1 00:01:25.671:         has client flags 0x0

*Mar  1 00:01:25.671:        outbound SA from 195.1.1.1
  to 195.1.1.4       (f/i)  0/ 0 (proxy 0.0.0.0         to
  192.168.3.0    )
```

```
*Mar  1 00:01:25.671:        has spi -1364439181 and conn_id
  23 and flags A

*Mar  1 00:01:25.671:         lifetime of 3600 seconds

*Mar  1 00:01:25.675:         lifetime of 4608000 kilobytes

*Mar  1 00:01:25.675:         has client flags 0x0

*Mar  1 00:01:25.675: IPSEC(key_engine): got a queue event...

*Mar  1 00:01:25.675: IPSEC(initialize_sas): ,

  (key eng. msg.) INBOUND local= 195.1.1.1, remote=
  195.1.1.4,

   local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),

   remote_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),

   protocol= ESP, transform= esp-3des esp-sha-hmac ,

   lifedur= 3600s and 4608000kb,

   spi= 0xA920823E(2837479998), conn_id= 22, keysize= 0,
  flags= 0x2

*Mar  1 00:01:25.675: IPSEC(initialize_sas): ,

  (key eng. msg.) OUTBOUND local= 195.1.1.1, remote=
  195.1.1.4,

   local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),

   remote_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),

   protocol= ESP, transform= esp-3des esp-sha-hmac ,

   lifedur= 3600s and 4608000kb,

   spi= 0xAEAC4F73(2930528115), conn_id= 23, keysize= 0,
  flags= 0xA

*Mar  1 00:01:25.679: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 00:01:25.679: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 00:01:25.679: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =

*Mar  1 00:01:25.679: IPSEC(add mtree): src 0.0.0.0, dest
  192.168.3.0, dest_port 0

*Mar  1 00:01:25.679: IPSEC(create_sa): sa created,

  (sa) sa_dest= 195.1.1.1, sa_prot= 50,

   sa_spi= 0xA920823E(2837479998),

   sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 22

*Mar  1 00:01:25.683: IPSEC(create_sa): sa created,

  (sa) sa_dest= 195.1.1.4, sa_prot= 50,

   sa_spi= 0xAEAC4F73(2930528115),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 23
*Mar  1 00:01:25.683: ISAKMP (0:2): sending packet to
  195.1.1.4 my_port 500 peer_port 500 (I) QM_IDLE
*Mar  1 00:01:25.691: ISAKMP (0:2): deleting node -264072751
  error FALSE reason ""
*Mar  1 00:01:25.691: ISAKMP (0:2): Node -264072751, Input =
  IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Mar  1 00:01:25.691: ISAKMP (0:2): Old State = IKE_QM_I_QM1
  New State = IKE_QM_PHASE2_COMPLETE
*Mar  1 00:01:26.151: ISAKMP (0:3): retransmitting phase 1
  MM_NO_STATE...
*Mar  1 00:01:26.151: ISAKMP (0:3): incrementing error
  counter on sa: retransmit phase 1
*Mar  1 00:01:26.151: ISAKMP (0:3): retransmitting phase 1
  MM_NO_STATE
*Mar  1 00:01:26.151: ISAKMP (0:3): sending packet to
  195.1.1.2 my_port 500 peer_port 500 (I) MM_NO_STATE
*Mar  1 00:01:27.291: ISAKMP (0:3): received packet from
  195.1.1.2 dport 500 sport 500 Global (I) MM_NO_STATE
*Mar  1 00:01:27.291: ISAKMP (0:3): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Mar  1 00:01:27.291: ISAKMP (0:3): Old State = IKE_I_MM1
  New State = IKE_I_MM2
*Mar  1 00:01:27.291: ISAKMP (0:3): processing SA payload.
  message ID = 0
*Mar  1 00:01:27.295: ISAKMP: Looking for a matching key for
  195.1.1.2 in default : success
*Mar  1 00:01:27.295: ISAKMP (0:3): found peer pre-shared key
  matching 195.1.1.2
*Mar  1 00:01:27.295: ISAKMP (0:3) local preshared key found
*Mar  1 00:01:27.295: ISAKMP : Scanning profiles for xauth
  ...
*Mar  1 00:01:27.295: ISAKMP (0:3): Checking ISAKMP transform
  1 against priority 10 policy
*Mar  1 00:01:27.295: ISAKMP:      encryption 3DES-CBC
*Mar  1 00:01:27.295: ISAKMP:      hash SHA
*Mar  1 00:01:27.295: ISAKMP:      default group 5
*Mar  1 00:01:27.295: ISAKMP:      auth pre-share
*Mar  1 00:01:27.295: ISAKMP:      life type in seconds
*Mar  1 00:01:27.295: ISAKMP:      life duration (VPI) of  0x0
  0x1 0x51 0x80
```

```
*Mar  1 00:01:27.299: ISAKMP (0:3): atts are acceptable. Next
  payload is 0

*Mar  1 00:01:28.723: ISAKMP (0:3): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:01:28.723: ISAKMP (0:3): Old State = IKE_I_MM2
  New State = IKE_I_MM2

*Mar  1 00:01:28.727: ISAKMP (0:3): sending packet to
  195.1.1.2 my_port 500 peer_port 500 (I) MM_SA_SETUP

*Mar  1 00:01:28.727: ISAKMP (0:3): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:28.727: ISAKMP (0:3): Old State = IKE_I_MM2
  New State = IKE_I_MM3

*Mar  1 00:01:29.883: ISAKMP (0:3): received packet from
  195.1.1.2 dport 500 sport 500 Global (I) MM_SA_SETUP

*Mar  1 00:01:29.883: ISAKMP (0:3): Input =
  IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:01:29.887: ISAKMP (0:3): Old State = IKE_I_MM3
  New State = IKE_I_MM4

*Mar  1 00:01:29.887: ISAKMP (0:3): processing KE payload.
  message ID = 0

*Mar  1 00:01:31.307: ISAKMP (0:3): processing NONCE payload.
  message ID = 0

*Mar  1 00:01:31.307: ISAKMP: Looking for a matching key for
  195.1.1.2 in default : success

*Mar  1 00:01:31.307: ISAKMP (0:3): found peer pre-shared key
  matching 195.1.1.2

*Mar  1 00:01:31.311: ISAKMP (0:3): SKEYID state generated

*Mar  1 00:01:31.311: ISAKMP (0:3): processing vendor id
  payload

*Mar  1 00:01:31.311: ISAKMP (0:3): vendor ID seems Unity/DPD
  but major 215 mismatch

*Mar  1 00:01:31.311: ISAKMP (0:3): vendor ID is XAUTH

*Mar  1 00:01:31.311: ISAKMP (0:3): processing vendor id
  payload

*Mar  1 00:01:31.311: ISAKMP (0:3): vendor ID is DPD

*Mar  1 00:01:31.315: ISAKMP (0:3): processing vendor id
  payload

*Mar  1 00:01:31.315: ISAKMP (0:3): vendor ID is Unity

*Mar  1 00:01:31.315: ISAKMP (0:3): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar  1 00:01:31.315: ISAKMP (0:3): Old State = IKE_I_MM4
  New State = IKE_I_MM4
```

```
*Mar  1 00:01:31.315: ISAKMP (0:3): Send initial contact

*Mar  1 00:01:31.315: ISAKMP (0:3): SA is doing pre-shared
   key authentication using id type ID_IPV4_ADDR

*Mar  1 00:01:31.319: ISAKMP (3): ID payload

next-payload : 8

type         : 1

addr         : 195.1.1.1

protocol     : 17

port         : 500

length       : 8

*Mar  1 00:01:31.319: ISAKMP (3): Total payload length: 12

*Mar  1 00:01:31.327: ISAKMP (0:3): sending packet to
   195.1.1.2 my_port 500 peer_port 500 (I) MM_KEY_EXCH

*Mar  1 00:01:31.327: ISAKMP (0:3): Input =
   IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:31.327: ISAKMP (0:3): Old State = IKE_I_MM4
   New State = IKE_I_MM5

*Mar  1 00:01:31.347: ISAKMP (0:3): received packet from
   195.1.1.2 dport 500 sport 500 Global (I) MM_KEY_EXCH

*Mar  1 00:01:31.351: ISAKMP (0:3): Input =
   IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar  1 00:01:31.351: ISAKMP (0:3): Old State = IKE_I_MM5
   New State = IKE_I_MM6

*Mar  1 00:01:31.355: ISAKMP (0:3): processing ID payload.
   message ID = 0

*Mar  1 00:01:31.355: ISAKMP (3): Process ID payload

type         : 2

FQDN name    : pixfirewall

protocol     : 17

port         : 500

length       : 11

*Mar  1 00:01:31.355: ISAKMP (0:3): processing HASH payload.
   message ID = 0

*Mar  1 00:01:31.359: ISAKMP (0:3): SA has been authenticated
   with 195.1.1.2

*Mar  1 00:01:31.359: ISAKMP (0:3): peer matches *none* of
   the profiles

*Mar  1 00:01:31.359: ISAKMP (0:3): Input =
   IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
```

```
*Mar  1 00:01:31.359: ISAKMP (0:3): Old State = IKE_I_MM6
  New State = IKE_I_MM6

*Mar  1 00:01:31.363: ISAKMP (0:3): Input =
  IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar  1 00:01:31.363: ISAKMP (0:3): Old State = IKE_I_MM6
  New State = IKE_P1_COMPLETE

*Mar  1 00:01:31.363: ISAKMP (0:3): beginning Quick Mode
  exchange, M-ID of -208634027

*Mar  1 00:01:31.371: ISAKMP (0:3): sending packet to
  195.1.1.2 my_port 500 peer_port 500 (I) QM_IDLE

*Mar  1 00:01:31.371: ISAKMP (0:3): Node -208634027, Input =
  IKE_MESG_INTERNAL, IKE_INIT_QM

*Mar  1 00:01:31.371: ISAKMP (0:3): Old State = IKE_QM_READY
  New State = IKE_QM_I_QM1

*Mar  1 00:01:31.371: ISAKMP (0:3): Input =
  IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

*Mar  1 00:01:31.371: ISAKMP (0:3): Old State =
  IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Mar  1 00:01:31.375: ISAKMP (0:3): received packet from
  195.1.1.2 dport 500 sport 500 Global (I) QM_IDLE

*Mar  1 00:01:31.387: ISAKMP (0:3): processing HASH payload.
  message ID = -208634027

*Mar  1 00:01:31.387: ISAKMP (0:3): processing SA payload.
  message ID = -208634027

*Mar  1 00:01:31.387: ISAKMP (0:3): Checking IPSec proposal 1

*Mar  1 00:01:31.387: ISAKMP: transform 1, ESP_3DES

*Mar  1 00:01:31.387: ISAKMP:   attributes in transform:

*Mar  1 00:01:31.387: ISAKMP:      encaps is 1

*Mar  1 00:01:31.387: ISAKMP:      SA life type in seconds

*Mar  1 00:01:31.387: ISAKMP:      SA life duration (basic) of
  3600

*Mar  1 00:01:31.391: ISAKMP:      SA life type in kilobytes

*Mar  1 00:01:31.391: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0

*Mar  1 00:01:31.391: ISAKMP:      authenticator is HMAC-SHA

*Mar  1 00:01:31.391: ISAKMP (0:3): atts are acceptable.

*Mar  1 00:01:31.391: IPSEC(validate_proposal_request):
  proposal part #1,

  (key eng. msg.) INBOUND local= 195.1.1.1, remote=
  195.1.1.2,

    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar  1 00:01:31.395: IPSEC(kei_proxy): head = VPN, map->ivrf
  = , kei->ivrf =
*Mar  1 00:01:31.395: ISAKMP (0:3): processing NONCE payload.
  message ID = -208634027
*Mar  1 00:01:31.395: ISAKMP (0:3): processing ID payload.
  message ID = -208634027
*Mar  1 00:01:31.395: ISAKMP (0:3): processing ID payload.
  message ID = -208634027
*Mar  1 00:01:31.399: ISAKMP (0:3): Creating IPSec SAs
*Mar  1 00:01:31.399:         inbound SA from 195.1.1.2 to
  195.1.1.1 (f/i)  0/ 0
        (proxy 192.168.1.0 to 0.0.0.0)
*Mar  1 00:01:31.403:         has spi 0x5FFAFD and conn_id 24
  and flags 2
*Mar  1 00:01:31.403:         lifetime of 3600 seconds
*Mar  1 00:01:31.403:         lifetime of 4608000 kilobytes
*Mar  1 00:01:31.403:         has client flags 0x0
*Mar  1 00:01:31.403:        outbound SA from 195.1.1.1
  to 195.1.1.2       (f/i)  0/ 0 (proxy 0.0.0.0         to
  192.168.1.0    )
*Mar  1 00:01:31.403:         has spi -1568214475 and conn_id
  25 and flags A
*Mar  1 00:01:31.403:         lifetime of 3600 seconds
*Mar  1 00:01:31.403:         lifetime of 4608000 kilobytes
*Mar  1 00:01:31.403:         has client flags 0x0
*Mar  1 00:01:31.407: IPSEC(key_engine): got a queue event...
*Mar  1 00:01:31.407: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 195.1.1.1, remote=
  195.1.1.2,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x5FFAFD(6290173), conn_id= 24, keysize= 0, flags=
  0x2
```

```
*Mar  1 00:01:31.407: IPSEC(initialize_sas): ,
   (key eng. msg.) OUTBOUND local= 195.1.1.1, remote=
   195.1.1.2,
     local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
     remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
     protocol= ESP, transform= esp-3des esp-sha-hmac ,
     lifedur= 3600s and 4608000kb,
     spi= 0xA286F235(2726752821), conn_id= 25, keysize= 0,
   flags= 0xA
*Mar  1 00:01:31.411: IPSEC(kei_proxy): head = VPN, map->ivrf
   = , kei->ivrf =
*Mar  1 00:01:31.411: IPSEC(add mtree): src 0.0.0.0, dest
   192.168.1.0, dest_port 0
*Mar  1 00:01:31.411: IPSEC(create_sa): sa created,
   (sa) sa_dest= 195.1.1.1, sa_prot= 50,
     sa_spi= 0x5FFAFD(6290173),
     sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 24
*Mar  1 00:01:31.411: IPSEC(create_sa): sa created,
   (sa) sa_dest= 195.1.1.2, sa_prot= 50,
     sa_spi= 0xA286F235(2726752821),
     sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 25
*Mar  1 00:01:31.415: ISAKMP (0:3): sending packet to
   195.1.1.2 my_port 500 peer_port 500 (I) QM_IDLE
*Mar  1 00:01:31.415: ISAKMP (0:3): deleting node -208634027
   error FALSE reason ""
*Mar  1 00:01:31.415: ISAKMP (0:3): Node -208634027, Input =
   IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Mar  1 00:01:31.415: ISAKMP (0:3): Old State = IKE_QM_I_QM1
   New State = IKE_QM_PHASE2_COMPLETE
```

FortiGate-60 unit

Enter the following command:

```
diag debug app ike 2
```

The following results appear:

```
Comes 195.1.1.1:500->195.1.1.4:500,ifindex=3, wan1,
   vf_id=0....
Exchange Mode = 2, I_COOKIE = 0x5851011CCC07842A, Len = 368
Received Payloads= KE NONCE VID VID VID VID 130 130
Responder:main mode get 2nd message...
```

```
Using IPS_NAT_MODE_NONE.
Responder: sent 195.1.1.1 main mode message #2 (OK)
set retransmit: st=1, timeout=10.
Comes 195.1.1.1:500->195.1.1.4:500,ifindex=3, wan1,
  vf_id=0....
Exchange Mode = 2, I_COOKIE = 0x5851011CCC07842A, Len = 100
Received Payloads= ID HASH Notif
Responder: main mode get 3rd message...
set gw: 0x8136c38, timeout=86400.
Responder: sent 195.1.1.1 main mode message #3 (DONE)
Comes 195.1.1.1:500->195.1.1.4:500,ifindex=3, wan1,
  vf_id=0....
Exchange Mode = 32, Message id = 0xF04291D1, Len = 172
Received Payloads= HASH SA NONCE ID ID
Responder:quick mode get 1st message...
his proposal ids: peer:0.0.0.0(0.0.0.0),
  me:192.168.3.0(255.255.255.0)
kernel_comm.c, 118, tun_name=To_Hub
my policy ids: src:192.168.3.0(255.255.255.0),
  dst:0.0.0.0(0.0.0.0)
Got it
Found To_Hub:195.1.1.1.
Autokey To_Hub.
Negotiate Result
Proposal_id = 1:
   Protocol_id = IPSEC_ESP:
      trans_id = ESP_3DES.
      encapsulation = ENCAPSULATION_MODE_TUNNEL
         type=AUTH_ALG, val=SHA1.
Phase2 esp lifetimes=3600
negotiate:No pfs is set !
Using tunnel mode.
Responder:quick mode pfs is not enabled.
quick mode:idci type=4, len=8, chunk=0000000000000000
quick mode:idcr type=4, len=8, chunk=c0a80300ffffff00
Responder: sent 195.1.1.1 quick mode message #1 (OK)
set retransmit: st=3, timeout=10.
```

```
Comes 195.1.1.1:500->195.1.1.4:500,ifindex=3, wan1,
  vf_id=0....

Exchange Mode = 32, Message id = 0xF04291D1, Len = 60

Received Payloads= HASH

Replay protection enable.

Set sa life soft seconds=3550.

Set sa life hard seconds=3600.

Set sa life soft bytes=422576128.

Set sa life hard bytes=423624704.

dport = 500.Initializing sa OK.

Responder:quick mode done !

Responder: parsed 195.1.1.1 quick mode message #2 (DONE)

expire: st=3, timeout=120.
```