

IOS IPsec NAT 투명성과 VPN 클라이언트 컨피그레이션 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[라우터 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[관련 정보](#)

소개

이 문서는 IPsec NAT(Network Address Translation) 투명성 기능의 Cisco IOS® 지원을 위한 샘플 컨피그레이션입니다. 또한 NAT와 IPsec 간에 알려진 여러 가지 비호환성 문제를 해결하여 네트워크에서 NAT 또는 PAT(Point Address Translation)를 통해 이동하는 IPsec 트래픽을 지원합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 2621 Router 12.2.13.7T1 이상
- Cisco VPN Client 3.6.3(컨피그레이션은 표시되지 않음)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

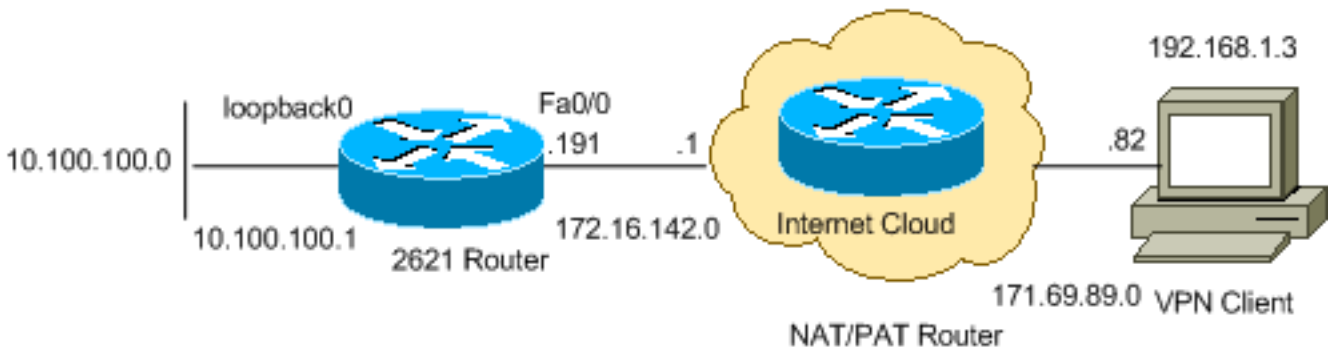
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



라우터 컨피그레이션

다음 단계를 완료하십시오.

1. 스위치가 실행되는 소프트웨어 버전을 표시하려면 **show version** 명령을 실행합니다.

```
2621#show version
```

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.2(13.7)T1,
MAINTENANCE INTERIM SOFTWARE
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 21-Dec-02 14:10 by ccai
Image text-base: 0x80008098, data-base: 0x818B6330
```

```
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
ROM: C2600 Software (C2600-IK9O3S3-M), Version 12.2(13.7)T1,
MAINTENANCE INTERIM SOFTWARE
```

```
2621 uptime is 33 minutes
System returned to ROM by reload
System image file is "flash:c2600-ik9o3s3-mz.122-13.7.T1"
```

```
cisco 2621 (MPC860) processor (revision 0x102) with 60416K/5120K bytes of memory.
Processor board ID JAB0407020V (2751454139)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
2 FastEthernet/IEEE 802.3 interface(s)
2 Channelized T1/PRI port(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
```

Configuration register is 0x2102

2. show run 명령을 실행합니다.

```
2621#show run
```

```
Building configuration...
```

```
Current configuration : 2899 bytes
```

```
!  
version 12.2  
service timestamps debug datetime msec localtime  
service timestamps log datetime msec localtime  
no service password-encryption  
!  
hostname 2621  
!  
boot system flash  
logging queue-limit 100  
enable secret 5 $1$dGFC$VA28yOWzxlCKyjldq8SkE/  
!  
username cisco password 0 cisco123  
username client password 0 testclient  
aaa new-model  
!  
!  
aaa authentication login userauthen local  
aaa authorization network foo local  
aaa session-id common  
ip subnet-zero  
ip cef  
!  
!  
no ip domain lookup  
ip domain name cisco.com  
!  
!  
!  
!  
crypto isakmp policy 20  
  encr 3des  
  hash md5  
  authentication pre-share  
  group 2  
crypto isakmp keepalive 40 5  
!--- Allows an IPsec node to send NAT keepalive !--- packets every 20 seconds. crypto  
isakmp nat keepalive 20  
!  
crypto isakmp client configuration group cisco  
  key test1234  
  pool test  
  acl 120  
!  
!  
!--- Transform set "test" which uses Triple DES !--- encryptions and MD5 (HMAC variant) !--  
- for data packet authentication: crypto ipsec transform-set test esp-3des esp-md5-hmac  
crypto ipsec transform-set foo esp-3des esp-sha-hmac  
!  
crypto ipsec profile greprotect  
!  
!  
!--- Dynamic crypto map. crypto dynamic-map dynmap 1  
set transform-set foo  
match address 199  
!  
!
```

```
crypto map test client authentication list userauthen
crypto map test isakmp authorization list foo
crypto map test client configuration address respond
!--- Adds a dynamic crypto map set to a static crypto map set. crypto map test 20 ipsec-
isakmp dynamic dynmap
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
controller T1 0/0
    framing sf
    linecode ami
!
controller T1 0/1
    framing sf
    linecode ami
!
!
!
interface Loopback0
    ip address 10.100.100.1 255.255.255.0
    ip nat inside
!
interface FastEthernet0/0
    ip address 172.16.142.191 255.255.255.0
    ip nat outside
    no ip route-cache
    no ip mroute-cache
    duplex auto
    speed auto
    !--- Applies a crypto map set to an interface. crypto map test
!
interface FastEthernet0/1
    ip address 10.130.13.13 255.255.0.0
    duplex auto
    speed auto
!
ip local pool test 192.168.1.1 192.168.1.250
ip nat inside source route-map nonat interface FastEthernet0/0 overload
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.142.1
!
ip pim bidir-enable
!
!
access-list 101 permit ip any any
access-list 101 permit esp any any
access-list 101 permit udp any any eq isakmp
```

```

access-list 101 permit ip 192.168.0.0 0.0.255.255 10.100.100.0 0.0.0.255
access-list 111 permit ip 10.100.100.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 112 deny ip 10.100.100.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 112 deny ip 10.100.100.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 112 permit ip 10.100.100.0 0.0.0.255 any
access-list 120 permit ip 10.100.100.0 0.0.0.255 192.168.1.0 0.0.0.255
!--- IPsec access list defines which traffic to protect. access-list 199 permit ip
10.100.100.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 199 permit ip host 172.16.142.191 192.168.1.0 0.0.0.255
!
route-map nonat permit 10
  match ip address 112
!
radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password cisco
!
!
end

2621#

```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output [Interpreter 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show crypto isakmp sa** - 피어에 있는 현재 모든 IKE(Internet Key Exchange) 보안 연결(SA)을 표시합니다.

```

2621#show crypto isakmp sa
  f_vrf/i_vrf    dst          src          state        conn-id slot
  /             172.16.142.191 171.69.89.82 QM_IDLE     4       0

```

- **show crypto ipsec sa** - 현재 SA에서 사용하는 설정을 표시합니다.

```

2621#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: test, local addr. 172.16.142.191

  protected vrf:
    local ident (addr/mask/prot/port): (10.100.100.0/255.255.255.0/0/0)
!--- Subnet behind local VPN router. remote ident (addr/mask/prot/port):
(192.168.1.3/255.255.255.255/0/0) !--- Subnet behind remote VPN router. current_peer:
171.69.89.82:4500 PERMIT, flags={ } #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11
#pkts decaps: 11, #pkts decrypt: 11, #pkts verify 11 #pkts compressed: 0, #pkts

```

```

decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0,
#pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.:
172.16.142.191, remote crypto endpt.: 171.69.89.82 !--- IP address of Encapsulating Security
Payload (ESP) endpoints. path mtu 1500, media mtu 1500 current outbound spi: 9A12903F
inbound esp sas: spi: 0xD44C2AFE(3561761534) !--- SPI inbound (ESP tunnel). transform: esp-
3des esp-sha-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2002, flow_id:
3, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4513510/3476)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
    spi: 0x9A12903F(2584907839)
!--- Security parameter index (SPI) outbound (ESP tunnel). transform: esp-3des esp-sha-hmac
, in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2003, flow_id: 4, crypto map:
test
    sa timing: remaining key lifetime (k/sec): (4513511/3476)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:

outbound pcp sas:

protected vrf:
    local ident (addr/mask/prot/port): (172.16.142.191/255.255.255.255/0/0)
!--- Next tunnel. remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0)
current_peer: 171.69.89.82:4500 PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0, #pkts
digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0,
#pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.:
172.16.142.191, remote crypto endpt.: 171.69.89.82 path mtu 1500, media mtu 1500 current
outbound spi: 1CD14C06 inbound esp sas: spi: 0x1EAC399E(514603422) transform: esp-3des esp-
sha-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2000, flow_id: 1, crypto
map: test sa timing: remaining key lifetime (k/sec): (4434590/3471) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0x1CD14C06(483478534) transform: esp-3des esp-sha-hmac , in use settings ={Tunnel UDP-
Encaps, } slot: 0, conn id: 2001, flow_id: 2, crypto map: test sa timing: remaining key
lifetime (k/sec): (4434590/3469) IV size: 8 bytes replay detection support: Y outbound ah
sas: outbound pcp sas:

```

- **show crypto engine connection active** - 암호화 엔진 통계를 표시합니다.패킷 수를 표시합니다.

```
2621#show crypto engine connection active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
4	FastEthernet0/0	172.16.142.191	set	HMAC_MD5+3DES_56_C	0	0
2000	FastEthernet0/0	172.16.142.191	set	HMAC_SHA+3DES_56_C	0	0
2001	FastEthernet0/0	172.16.142.191	set	HMAC_SHA+3DES_56_C	0	0
2002	FastEthernet0/0	172.16.142.191	set	HMAC_SHA+3DES_56_C	0	11
2003	FastEthernet0/0	172.16.142.191	set	HMAC_SHA+3DES_56_C	11	0

- **show crypto engine [brief | configuration]**(**컨피그레이션**)—암호화 엔진에 대한 컨피그레이션 정보의 요약을 표시합니다.특별 권한 EXEC 모드에서 이 명령을 사용합니다.이 명령은 모든 암호화 엔진을 표시하고 AIM-VPN 제품 이름을 표시합니다.

```
2621#show crypto engine configuration
```

```

crypto engine name: unknown
!--- Name of the crypto engine as assigned with the !--- key-name argument in the crypto key
generate dss command.

```



```

*Mar 1 00:32:13.115: ISAKMP (0:4): purging node 428915319
*Mar 1 00:32:23.199: ISAKMP (0:4): received packet from 171.69.89.82
                        dport 4500 sport 4500 Global (R) QM_IDLE
*Mar 1 00:32:23.199: ISAKMP: set new node -1483946735 to QM_IDLE
*Mar 1 00:32:23.203: ISAKMP (0:4): processing HASH payload. message ID = -1483946735
*Mar 1 00:32:23.203: ISAKMP (0:4): processing NOTIFY unknown protocol 1
                        spi 0, message ID = -1483946735, sa = 82443410
*Mar 1 00:32:23.203: ISAKMP (0:4): deleting node -1483946735 error
                        FALSE reason "informational (in) state 1"
*Mar 1 00:32:23.203: ISAKMP (0:4): Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY
*Mar 1 00:32:23.203: ISAKMP (0:4): Old State = IKE_P1_COMPLETE
                        New State = IKE_P1_COMPLETE

```

```

*Mar 1 00:32:33.147: ISAKMP (0:4): purging node -1677054470

```

- **debug ip packet [detail]**—일반 IP 디버깅 정보 및 IP 보안 옵션(IPSO) 보안 트랜잭션을 표시합니다.

- **debug ip icmp** - ICMP(Internal Control Message Protocol) 트랜잭션에 대한 정보를 표시합니다

```

Generic IP:

```

```

    ICMP packet debugging is on
    IP packet debugging is on (detailed)

```

```

*Mar 1 00:38:43.735: IP: s=171.69.89.82 (FastEthernet0/0), d=172.16.142.191
                        (FastEthernet0/0), len 108, rcvd 3
*Mar 1 00:38:43.735:     UDP src=4500, dst=4500
*Mar 1 00:38:48.863: IP: s=192.168.1.3 (FastEthernet0/0), d=10.100.100.1,
                        len 60, rcvd 4
*Mar 1 00:38:48.863:     ICMP type=8, code=0
*Mar 1 00:38:48.863: ICMP: echo reply sent, src 10.100.100.1, dst 192.168.1.3
*Mar 1 00:38:48.867: IP: s=10.100.100.1 (local), d=192.168.1.3 (FastEthernet0/0),
                        len 60, sending
*Mar 1 00:38:48.867:     ICMP type=0, code=0
*Mar 1 00:38:49.863: IP: s=192.168.1.3 (FastEthernet0/0), d=10.100.100.1,
                        len 60, rcvd 4
*Mar 1 00:38:49.863:     ICMP type=8, code=0
*Mar 1 00:38:49.863: ICMP: echo reply sent, src 10.100.100.1, dst 192.168.1.3
*Mar 1 00:38:49.863: IP: s=10.100.100.1 (local), d=192.168.1.3 (FastEthernet0/0),
                        len 60, sending
*Mar 1 00:38:49.867:     ICMP type=0, code=0
*Mar 1 00:38:50.863: IP: s=192.168.1.3 (FastEthernet0/0), d=10.100.100.1,
                        len 60, rcvd 4
*Mar 1 00:38:50.867:     ICMP type=8, code=0
*Mar 1 00:38:50.867: ICMP: echo reply sent, src 10.100.100.1, dst 192.168.1.3
*Mar 1 00:38:50.867: IP: s=10.100.100.1 (local), d=192.168.1.3 (FastEthernet0/0),
                        len 60, sending
*Mar 1 00:38:50.867:     ICMP type=0, code=0
*Mar 1 00:38:51.867: IP: s=192.168.1.3 (FastEthernet0/0), d=10.100.100.1,
                        len 60, rcvd 4
*Mar 1 00:38:51.867:     ICMP type=8, code=0
*Mar 1 00:38:51.867: ICMP: echo reply sent, src 10.100.100.1, dst 192.168.1.3

```

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.

- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.

- **debug crypto engine** - 암호화된 트래픽을 표시합니다.

```

2621#
2621#
2621#
2621#

```

```

*Mar 1 00:27:54.735: ISAKMP (0:0): received packet from 171.69.89.82 dport
                        500 sport 500 Global (N) NEW SA
*Mar 1 00:27:54.739: ISAKMP: Created a peer struct for 171.69.89.82, peer port 500
*Mar 1 00:27:54.739: ISAKMP: Locking peer struct 0x82C88D44, IKE refcount

```



```
1 for crypto_ikmp_config_initialize_sa
*Mar 1 00:27:54.739: ISAKMP (0:0): Setting client config settings 82A819DC
*Mar 1 00:27:54.739: ISAKMP (0:0): (Re)Setting client xauth list and state
*Mar 1 00:27:54.739: ISAKMP: local port 500, remote port 500
*Mar 1 00:27:54.743: ISAKMP: Find a dup sa in the avl tree during calling
    isadb_insert sa = 82443410
*Mar 1 00:27:54.743: ISAKMP (0:4): processing SA payload. message ID = 0
*Mar 1 00:27:54.743: ISAKMP (0:4): processing ID payload. message ID = 0
*Mar 1 00:27:54.743: ISAKMP (0:4): peer matches *none* of the profiles
*Mar 1 00:27:54.743: ISAKMP (0:4): processing vendor id payload
*Mar 1 00:27:54.743: ISAKMP (0:4): vendor ID seems Unity/DPD but major 215 mismatch
*Mar 1 00:27:54.747: ISAKMP (0:4): vendor ID is XAUTH
*Mar 1 00:27:54.747: ISAKMP (0:4): processing vendor id payload
*Mar 1 00:27:54.747: ISAKMP (0:4): vendor ID is DPD
*Mar 1 00:27:54.747: ISAKMP (0:4): processing vendor id payload
*Mar 1 00:27:54.747: ISAKMP (0:4): vendor ID seems Unity/DPD but major 123 mismatch
*Mar 1 00:27:54.747: ISAKMP (0:4): vendor ID is NAT-T v2
*Mar 1 00:27:54.747: ISAKMP (0:4): processing vendor id payload
*Mar 1 00:27:54.747: ISAKMP (0:4): vendor ID seems Unity/DPD but major 194 mismatch
*Mar 1 00:27:54.751: ISAKMP (0:4): processing vendor id payload
*Mar 1 00:27:54.751: ISAKMP (0:4): vendor ID is Unity
*Mar 1 00:27:54.751: ISAKMP (0:4): Authentication by xauth preshared
*Mar 1 00:27:54.751: ISAKMP (0:4): Checking ISAKMP transform 1 against
    priority 20 policy
*Mar 1 00:27:54.751: ISAKMP: encryption AES-CBC
*Mar 1 00:27:54.751: ISAKMP: hash SHA
*Mar 1 00:27:54.751: ISAKMP: default group 2
*Mar 1 00:27:54.751: ISAKMP: auth XAUTHInitPreShared
*Mar 1 00:27:54.751: ISAKMP: life type in seconds
*Mar 1 00:27:54.751: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.755: ISAKMP: keylength of 256
*Mar 1 00:27:54.755: ISAKMP (0:4): Encryption algorithm offered does not
    match policy!
*Mar 1 00:27:54.755: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.755: ISAKMP (0:4): Checking ISAKMP transform 2 against
    priority 20 policy
*Mar 1 00:27:54.755: ISAKMP: encryption AES-CBC
*Mar 1 00:27:54.755: ISAKMP: hash MD5
*Mar 1 00:27:54.755: ISAKMP: default group 2
*Mar 1 00:27:54.755: ISAKMP: auth XAUTHInitPreShared
*Mar 1 00:27:54.755: ISAKMP: life type in seconds
*Mar 1 00:27:54.755: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.759: ISAKMP: keylength of 256
*Mar 1 00:27:54.759: ISAKMP (0:4): Encryption algorithm offered does not
    match policy!
*Mar 1 00:27:54.759: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.759: ISAKMP (0:4): Checking ISAKMP transform 3 against
    priority 20 policy
*Mar 1 00:27:54.759: ISAKMP: encryption AES-CBC
*Mar 1 00:27:54.759: ISAKMP: hash SHA
*Mar 1 00:27:54.759: ISAKMP: default group 2
*Mar 1 00:27:54.759: ISAKMP: auth pre-share
*Mar 1 00:27:54.759: ISAKMP: life type in seconds
*Mar 1 00:27:54.759: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.759: ISAKMP: keylength of 256
*Mar 1 00:27:54.763: ISAKMP (0:4): Encryption algorithm offered does not match
    policy!
*Mar 1 00:27:54.763: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.763: ISAKMP (0:4): Checking ISAKMP transform 4 against priority
    20 policy
*Mar 1 00:27:54.763: ISAKMP: encryption AES-CBC
*Mar 1 00:27:54.763: ISAKMP: hash MD5
*Mar 1 00:27:54.763: ISAKMP: default group 2
*Mar 1 00:27:54.763: ISAKMP: auth pre-share
```

*Mar 1 00:27:54.763: ISAKMP: life type in seconds
*Mar 1 00:27:54.763: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.763: ISAKMP: keylength of 256
*Mar 1 00:27:54.763: ISAKMP (0:4): Encryption algorithm offered does not match policy!
*Mar 1 00:27:54.767: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.767: ISAKMP (0:4): Checking ISAKMP transform 5 against priority 20 policy
*Mar 1 00:27:54.767: ISAKMP: encryption AES-CBC
*Mar 1 00:27:54.767: ISAKMP: hash SHA
*Mar 1 00:27:54.767: ISAKMP: default group 2
*Mar 1 00:27:54.767: ISAKMP: auth XAUTHInitPreShared
*Mar 1 00:27:54.767: ISAKMP: life type in seconds
*Mar 1 00:27:54.767: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.767: ISAKMP: keylength of 192
*Mar 1 00:27:54.767: ISAKMP (0:4): Encryption algorithm offered does not match policy!
*Mar 1 00:27:54.771: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.771: ISAKMP (0:4): Checking ISAKMP transform 6 against priority 20 policy
*Mar 1 00:27:54.771: ISAKMP: encryption AES-CBC
*Mar 1 00:27:54.771: ISAKMP: hash MD5
*Mar 1 00:27:54.771: ISAKMP: default group 2
*Mar 1 00:27:54.771: ISAKMP: auth XAUTHInitPreShared
*Mar 1 00:27:54.771: ISAKMP: life type in seconds
*Mar 1 00:27:54.771: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.771: ISAKMP: keylength of 192
*Mar 1 00:27:54.771: ISAKMP (0:4): Encryption algorithm offered does not match policy!
*Mar 1 00:27:54.771: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.775: ISAKMP (0:4): Checking ISAKMP transform 7 against priority 20 policy
*Mar 1 00:27:54.775: ISAKMP: encryption AES-CBC
*Mar 1 00:27:54.775: ISAKMP: hash SHA
*Mar 1 00:27:54.775: ISAKMP: default group 2
*Mar 1 00:27:54.775: ISAKMP: auth pre-share
*Mar 1 00:27:54.775: ISAKMP: life type in seconds
*Mar 1 00:27:54.775: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.775: ISAKMP: keylength of 192
*Mar 1 00:27:54.775: ISAKMP (0:4): Encryption algorithm 1 00:27:54.783: ISAKMP: hash SHA offered does not match policy!
*Mar 1 00:27:54.775: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.775: ISAKMP (0:4): Checking ISAKMP transform 8 against priority 20 policy
*Mar 1 00:27:54.779: ISAKMP: encryption AES-CBC
*Mar 1 00:27:54.779: ISAKMP: hash MD5
*Mar 1 00:27:54.779: ISAKMP: default group 2
*Mar 1 00:27:54.779: ISAKMP: auth pre-share
*Mar 1 00:27:54.779: ISAKMP: life type in seconds
*Mar 1 00:27:54.779: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.779: ISAKMP: keylength of 192
*Mar 1 00:27:54.779: ISAKMP (0:4): Encryption algorithm offered does not match policy!
*Mar 1 00:27:54.779: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.779: ISAKMP (0:4): Checking ISAKMP transform 9 against priority 20 policy
*Mar 1 00:27:54.783: ISAKMP: encryption AES-CBC
*Mar
*Mar 1 00:27:54.783: ISAKMP: default group 2
*Mar 1 00:27:54.783: ISAKMP: auth XAUTHInitPreShared
*Mar 1 00:27:54.783: ISAKMP: life type in seconds
*Mar 1 00:27:54.783: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.783: ISAKMP: keylength of 128
*Mar 1 00:27:54.783: ISAKMP (0:4): Encryption algorithm offered does not match

```

                                policy!
*Mar 1 00:27:54.783: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.783: ISAKMP (0:4): Checking ISAKMP transform 10 against
                                priority 20 policy
*Mar 1 00:27:54.783: ISAKMP:      encryption AES-CBC
*Mar 1 00:27:54.787: ISAKMP:      hash MD5
*Mar 1 00:27:54.787: ISAKMP:      default group 2
*Mar 1 00:27:54.787: ISAKMP:      auth XAUTHInitPreShared
*Mar 1 00:27:54.787: ISAKMP:      life type in seconds
*Mar 1 00:27:54.787: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.787: ISAKMP:      keylength of 128
*Mar 1 00:27:54.787: ISAKMP (0:4): Encryption algorithm offered does not match
                                policy!
*Mar 1 00:27:54.787: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.787: ISAKMP (0:4): Checking ISAKMP transform 11 against
                                priority 20 policy
*Mar 1 00:27:54.787: ISAKMP:      encryption AES-CBC
*Mar 1 00:27:54.787: ISAKMP:      hash SHA
*Mar 1 00:27:54.791: ISAKMP:      default group 2
*Mar 1 00:27:54.791: ISAKMP:      auth pre-share
*Mar 1 00:27:54.791: ISAKMP:      life type in seconds
*Mar 1 00:27:54.791: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.791: ISAKMP:      keylength of 128
*Mar 1 00:27:54.791: ISAKMP (0:4): Encryption algorithm offered does not
                                match policy!
*Mar 1 00:27:54.791: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.791: ISAKMP (0:4): Checking ISAKMP transform 12 against
                                priority 20 policy
*Mar 1 00:27:54.791: ISAKMP:      encryption AES-CBC
*Mar 1 00:27:54.791: ISAKMP:      hash MD5
*Mar 1 00:27:54.791: ISAKMP:      default group 2
*Mar 1 00:27:54.795: ISAKMP:      auth pre-share
*Mar 1 00:27:54.795: ISAKMP:      life type in seconds
*Mar 1 00:27:54.795: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.795: ISAKMP:      keylength of 128
*Mar 1 00:27:54.795: ISAKMP (0:4): Encryption algorithm offered does not
                                match policy!
*Mar 1 00:27:54.795: ISAKMP (0:4): atts are not acceptable. Next payload
                                7:54.795: ISAKMP:      hash SHA is 3
*Mar 1 00:27:54.795: ISAKMP (0:4): Checking ISAKMP transform 13 against
                                priority 20 policy
*Mar 1 00:27:54.795: ISAKMP:      encryption 3DES-CBC
*Mar 1 00:2
*Mar 1 00:27:54.795: ISAKMP:      default group 2
*Mar 1 00:27:54.795: ISAKMP:      auth XAUTHInitPreShared
*Mar 1 00:27:54.799: ISAKMP:      life type in seconds
*Mar 1 00:27:54.799: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.799: ISAKMP (0:4): Hash algorithm offered does not match policy!
*Mar 1 00:27:54.799: ISAKMP (0:4): atts are not acceptable. Next payload is 3
*Mar 1 00:27:54.799: ISAKMP (0:4): Checking ISAKMP transform 14 against
                                priority 20 policy
*Mar 1 00:27:54.799: ISAKMP:      encryption 3DES-CBC
*Mar 1 00:27:54.799: ISAKMP:      hash MD5
*Mar 1 00:27:54.799: ISAKMP:      default group 2
*Mar 1 00:27:54.799: ISAKMP:      auth XAUTHInitPreShared
*Mar 1 00:27:54.799: ISAKMP:      life type in seconds
*Mar 1 00:27:54.803: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Mar 1 00:27:54.803: ISAKMP (0:4): atts are acceptable. Next payload is 3
*Mar 1 00:27:55.015: ISAKMP (0:4): processing KE payload. message ID = 0
*Mar 1 00:27:55.287: ISAKMP (0:4): processing NONCE payload. message ID = 0
*Mar 1 00:27:55.287: ISAKMP (0:4): vendor ID is NAT-T v2
*Mar 1 00:27:55.287: ISAKMP (0:4): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
*Mar 1 00:27:55.291: ISAKMP (0:4): Old State = IKE_READY New State =
                                IKE_R_AM_AAA_AWAIT

```

*Mar 1 00:27:55.291: ISAKMP: got callback 1
*Mar 1 00:27:55.295: ISAKMP (0:4): SKEYID state generated
*Mar 1 00:27:55.299: ISAKMP (0:4): constructed NAT-T vendor-02 ID
*Mar 1 00:27:55.299: ISAKMP (0:4): SA is doing pre-shared key authentication
plus XAUTH using id type ID_IPV4_ADDR
*Mar 1 00:27:55.299: ISAKMP (4): ID payload
next-payload : 10
type : 1
addr : 172.16.142.191
protocol : 17
port : 0
length : 8
*Mar 1 00:27:55.299: ISAKMP (4): Total payload length: 12
*Mar 1 00:27:55.303: ISAKMP (0:4): constructed HIS NAT-D
*Mar 1 00:27:55.303: ISAKMP (0:4): constructed MINE NAT-D
*Mar 1 00:27:55.303: ISAKMP (0:4): sending packet to 171.69.89.82
my_port 500 peer_port 500 (R) AG_INIT_EXCH
*Mar 1 00:27:55.303: ISAKMP (0:4): Input = IKE_MSG_FROM_AAA,
PRESHARED_KEY_REPLY
*Mar 1 00:27:55.303: ISAKMP (0:4): Old State = IKE_R_AM_AAA_AWAIT
New State = IKE_R_AM2

*Mar 1 00:27:55.391: ISAKMP (0:4): received packet from 171.69.89.82
dport 4500 sport 4500 Global (R) AG_INIT_EXCH
*Mar 1 00:27:55.395: ISAKMP (0:4): processing HASH payload. message ID = 0
*Mar 1 00:27:55.395: ISAKMP (0:4): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 82443410
*Mar 1 00:27:55.399: ISAKMP (0:4): Process initial contact,
bring down existing phase 1 and 2 SA's with local 172.16.142.191
remote 171.69.89.82 remote port 4500
*Mar 1 00:27:55.399: ISAKMP (0:4): returning IP addr to the address pool
*Mar 1 00:27:55.399: ISAKMP:received payload type 17
*Mar 1 00:27:55.399: ISAKMP (0:4): Detected NAT-D payload
*Mar 1 00:27:55.399: ISAKMP (0:4): recalc my hash for NAT-D
*Mar 1 00:27:55.399: ISAKMP (0:4): NAT match MINE hash
*Mar 1 00:27:55.399: ISAKMP:received payload type 17
*Mar 1 00:27:55.399: ISAKMP (0:4): Detected NAT-D payload
*Mar 1 00:27:55.399: ISAKMP (0:4): recalc his hash for NAT-D
*Mar 1 00:27:55.403: ISAKMP (0:4): NAT does not match HIS hash
*Mar 1 00:27:55.403: hash received: 93 31 EB 5E 30 E2 A0 C4 D3 6F 3E B1 B7
F AE C3
*Mar 1 00:27:55.403: his nat hash : 14 64 77 EC E8 DC 78 B9 F9 DC 2B 46
CB E8 1D 4
*Mar 1 00:27:55.403: ISAKMP (0:4): SA has been authenticated with 171.69.89.82
*Mar 1 00:27:55.407: ISAKMP (0:4): Detected port floating to port = 4500
*Mar 1 00:27:55.407: ISAKMP: Trying to insert a peer 171.69.89.82/4500/,
and inserted successfully.
*Mar 1 00:27:55.407: ISAKMP (0:4): IKE_DPD is enabled, initializing timers
*Mar 1 00:27:55.407: ISAKMP: set new node 772423690 to CONF_XAUTH
*Mar 1 00:27:55.411: ISAKMP (0:4): sending packet to 171.69.89.82 my_port
4500 peer_port 4500 (R) QM_IDLE
*Mar 1 00:27:55.411: ISAKMP (0:4): purging node 772423690
*Mar 1 00:27:55.411: ISAKMP: Sending phase 1 responder lifetime 86400

*Mar 1 00:27:55.411: ISAKMP (0:4): peer matches *none* of the profiles
*Mar 1 00:27:55.411: ISAKMP (0:4): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
*Mar 1 00:27:55.411: ISAKMP (0:4): Old State = IKE_R_AM2 New State =
IKE_P1_COMPLETE

*Mar 1 00:27:55.415: IPSEC(key_engine): got a queue event...
*Mar 1 00:27:55.415: ISAKMP (0:4): Need XAUTH
*Mar 1 00:27:55.415: ISAKMP (0:4): Input = IKE_MSG_INTERNAL,
IKE_PHASE1_COMPLETE

*Mar 1 00:27:55.415: ISAKMP (0:4): Old State = IKE_P1_COMPLETE
New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

*Mar 1 00:27:55.419: ISAKMP: got callback 1

*Mar 1 00:27:55.419: ISAKMP: set new node -266369278 to CONF_XAUTH

*Mar 1 00:27:55.419: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2

*Mar 1 00:27:55.419: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2

*Mar 1 00:27:55.419: ISAKMP (0:4): initiating peer config to 171.69.89.82.
ID = -266369278

*Mar 1 00:27:55.423: ISAKMP (0:4): sending packet to 171.69.89.82 my_port
4500 peer_port 4500 (R) CONF_XAUTH

*Mar 1 00:27:55.423: ISAKMP (0:4): Input = IKE_MESG_FROM_AAA,
IKE_AAA_START_LOGIN

*Mar 1 00:27:55.423: ISAKMP (0:4): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
New State = IKE_XAUTH_REQ_SENT

*Mar 1 00:27:55.959: ISAKMP (0:3): purging node 1153289263

*Mar 1 00:28:00.423: ISAKMP (0:4): retransmitting phase 2 CONF_XAUTH
-266369278 ...

*Mar 1 00:28:00.423: ISAKMP (0:4): incrementing error counter on sa:
retransmit phase 2

*Mar 1 00:28:00.423: ISAKMP (0:4): incrementing error counter on sa:
retransmit phase 2

*Mar 1 00:28:00.423: ISAKMP (0:4): retransmitting phase 2 -266369278 CONF_XAUTH

*Mar 1 00:28:00.423: ISAKMP (0:4): sending packet to 171.69.89.82 my_port
4500 peer_port 4500 (R) CONF_XAUTH

*Mar 1 00:28:02.635: ISAKMP (0:4): received packet from 171.69.89.82 dport
4500 sport 4500 Global (R) CONF_XAUTH

*Mar 1 00:28:02.635: ISAKMP (0:4): processing transaction payload from
171.69.89.82. message ID = -266369278

*Mar 1 00:28:02.639: ISAKMP: Config payload REPLY

*Mar 1 00:28:02.639: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2

*Mar 1 00:28:02.639: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2

*Mar 1 00:28:02.639: ISAKMP (0:4): deleting node -266369278 error FALSE
reason "done with xauth request/reply exchange"

*Mar 1 00:28:02.639: ISAKMP (0:4): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY

*Mar 1 00:28:02.639: ISAKMP (0:4): Old State = IKE_XAUTH_REQ_SENT
New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

*Mar 1 00:28:02.643: ISAKMP: got callback 1

*Mar 1 00:28:02.643: ISAKMP: set new node -1548124746 to CONF_XAUTH

*Mar 1 00:28:02.643: ISAKMP (0:4): initiating peer config to 171.69.89.82.
ID = -1548124746

*Mar 1 00:28:02.647: ISAKMP (0:4): sending packet to 171.69.89.82 my_port
4500 peer_port 4500 (R) CONF_XAUTH

*Mar 1 00:28:02.647: ISAKMP (0:4): Input = IKE_MESG_FROM_AAA,
IKE_AAA_CONT_LOGIN

*Mar 1 00:28:02.647: ISAKMP (0:4): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
New State = IKE_XAUTH_SET_SENT

*Mar 1 00:28:02.663: ISAKMP (0:4): received packet from 171.69.89.82 dport
4500 sport 4500 Global (R) CONF_XAUTH

*Mar 1 00:28:02.663: ISAKMP (0:4): processing transaction payload from
171.69.89.82. message ID = -1548124746

*Mar 1 00:28:02.663: ISAKMP: Config payload ACK

*Mar 1 00:28:02.663: ISAKMP (0:4): XAUTH ACK Processed

*Mar 1 00:28:02.667: ISAKMP (0:4): deleting node -1548124746 error FALSE
reason "done with transaction"

*Mar 1 00:28:02.667: ISAKMP (0:4): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK

*Mar 1 00:28:02.667: ISAKMP (0:4): Old State = IKE_XAUTH_SET_SENT
New State = IKE_P1_COMPLETE

*Mar 1 00:28:02.667: ISAKMP (0:4): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE

```

*Mar 1 00:28:02.667: ISAKMP (0:4): Old State = IKE_P1_COMPLETE
                                New State = IKE_P1_COMPLETE

*Mar 1 00:28:02.675: ISAKMP (0:4): received packet from 171.69.89.82
                                dport 4500 sport 4500 Global (R) QM_IDLE
*Mar 1 00:28:02.675: ISAKMP: set new node 1973520613 to QM_IDLE
*Mar 1 00:28:02.679: ISAKMP (0:4): processing transaction payload from
                                171.69.89.82. message ID = 1973520613
*Mar 1 00:28:02.679: ISAKMP: Config payload REQUEST
*Mar 1 00:28:02.679: ISAKMP (0:4): checking request:
*Mar 1 00:28:02.679: ISAKMP: IP4_ADDRESS
*Mar 1 00:28:02.679: ISAKMP: IP4_NETMASK
*Mar 1 00:28:02.679: ISAKMP: IP4_DNS
*Mar 1 00:28:02.683: ISAKMP: IP4_NBNS
*Mar 1 00:28:02.683: ISAKMP: ADDRESS_EXPIRY
*Mar 1 00:28:02.683: ISAKMP: APPLICATION_VERSION
*Mar 1 00:28:02.683: ISAKMP: UNKNOWN Unknown Attr: 0x7000
*Mar 1 00:28:02.683: ISAKMP: UNKNOWN Unknown Attr: 0x7001
*Mar 1 00:28:02.683: ISAKMP: DEFAULT_DOMAIN
*Mar 1 00:28:02.683: ISAKMP: SPLIT_INCLUDE
*Mar 1 00:28:02.683: ISAKMP: UNKNOWN Unknown Attr: 0x7003
*Mar 1 00:28:02.683: ISAKMP: UNKNOWN Unknown Attr: 0x7007
*Mar 1 00:28:02.683: ISAKMP: UNKNOWN Unknown Attr: 0x7008
*Mar 1 00:28:02.683: ISAKMP: UNKNOWN Unknown Attr: 0x7009
*Mar 1 00:28:02.687: ISAKMP: UNKNOWN Unknown Attr: 0x700A
*Mar 1 00:28:02.687: ISAKMP (0:4): Input = IKE_MESG_FROM_PEER,
                                IKE_CFG_REQUEST
*Mar 1 00:28:02.687: ISAKMP (0:4): Old State = IKE_P1_COMPLETE
                                New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

*Mar 1 00:28:02.691: ISAKMP: got callback 1
*Mar 1 00:28:02.695: ISAKMP (0:4): attributes sent in message:
*Mar 1 00:28:02.695: Address: 0.2.0.0
*Mar 1 00:28:02.695: ISAKMP (0:4): allocating address 192.168.1.3
*Mar 1 00:28:02.695: ISAKMP: Sending private address: 192.168.1.3
*Mar 1 00:28:02.695: ISAKMP: Sending ADDRESS_EXPIRY seconds left to
                                use the address: 86392
*Mar 1 00:28:02.695: ISAKMP: Sending APPLICATION_VERSION string:
                                Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK903S3-M), Version 12.2(13.7)T1,
                                MAINTENANCE INTERIM SOFTWARE

TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 21-Dec-02 14:10 by ccai
*Mar 1 00:28:02.699: ISAKMP (0/4): Unknown Attr: UNKNOWN (0x7000)
*Mar 1 00:28:02.699: ISAKMP (0/4): Unknown Attr: UNKNOWN (0x7001)
*Mar 1 00:28:02.699: ISAKMP: Sending split include name 120 network
                                10.100.100.0 mask 255.255.255.0 protocol 0,
                                src port 0, dst port 0

*Mar 1 00:28:02.699: ISAKMP (0/4): Unknown Attr: UNKNOWN (0x7003)
*Mar 1 00:28:02.699: ISAKMP (0/4): Unknown Attr: UNKNOWN (0x7007)
*Mar 1 00:28:02.699: ISAKMP (0/4): Unknown Attr: UNKNOWN (0x7008)
*Mar 1 00:28:02.699: ISAKMP (0/4): Unknown Attr: UNKNOWN (0x7009)
*Mar 1 00:28:02.699: ISAKMP (0/4): Unknown Attr: UNKNOWN (0x700A)
*Mar 1 00:28:02.703: ISAKMP (0:4): responding to peer config from
                                171.69.89.82. ID = 1973520613
*Mar 1 00:28:02.703: ISAKMP (0:4): sending packet to 171.69.89.82 my_port
                                4500 peer_port 4500 (R) CONF_ADDR
*Mar 1 00:28:02.707: ISAKMP (0:4): deleting node 1973520613 error FALSE
                                reason ""
*Mar 1 00:28:02.707: ISAKMP (0:4): Input = IKE_MESG_FROM_AAA,
                                IKE_AAA_GROUP_ATTR
*Mar 1 00:28:02.707: ISAKMP (0:4): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT

```

New State = IKE_P1_COMPLETE

```
*Mar 1 00:28:02.775: ISAKMP (0:4): received packet from 171.69.89.82
                                dport 4500 sport 4500 Global (R) QM_IDLE
*Mar 1 00:28:02.775: ISAKMP: set new node 1783469429 to QM_IDLE
*Mar 1 00:28:02.787: ISAKMP (0:4): processing HASH payload. message
                                ID = 1783469429
*Mar 1 00:28:02.787: ISAKMP (0:4): processing SA payload. message
                                ID = 1783469429
*Mar 1 00:28:02.787: ISAKMP (0:4): Checking IPsec proposal 1
*Mar 1 00:28:02.787: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:02.787: ISAKMP:   attributes in transform:
*Mar 1 00:28:02.787: ISAKMP:     authenticator is HMAC-MD5
*Mar 1 00:28:02.787: ISAKMP:     encaps is 61443
*Mar 1 00:28:02.791: ISAKMP:     key length is 256
*Mar 1 00:28:02.791: ISAKMP:     SA life type in seconds
*Mar 1 00:28:02.791: ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Mar 1 00:28:02.791: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.791: ISAKMP (0:4): Checking IPsec proposal 1
*Mar 1 00:28:02.791: ISAKMP (0:4): transform 1, IPPCP LZS
*Mar 1 00:28:02.791: ISAKMP:   attributes in transform:
*Mar 1 00:28:02.791: ISAKMP:     encaps is 61443
*Mar 1 00:28:02.795: ISAKMP:     SA life type in seconds
*Mar 1 00:28:02.795: ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Mar 1 00:28:02.795: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.795: IPSEC(validate_proposal_request): proposal part #1,
    (key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
    local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
    remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes 256 esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x400
*Mar 1 00:28:02.799: IPSEC(validate_proposal_request): proposal part #2,
    (key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
    local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
    remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
    protocol= PCP, transform= comp-lzs ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400
*Mar 1 00:28:02.799: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.799: IPSEC(validate_transform_proposal): no IPSEC cryptomap
    exists for local address 172.16.142.191
*Mar 1 00:28:02.799: ISAKMP (0:4): IPsec policy invalidated proposal
*Mar 1 00:28:02.803: ISAKMP (0:4): Checking IPsec proposal 2
*Mar 1 00:28:02.803: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:02.803: ISAKMP:   attributes in transform:
*Mar 1 00:28:02.803: ISAKMP:     authenticator is HMAC-SHA
*Mar 1 00:28:02.803: ISAKMP:     encaps is 61443
*Mar 1 00:28:02.803: ISAKMP:     key length is 256
*Mar 1 00:28:02.803: ISAKMP:     SA life type in seconds
*Mar 1 00:28:02.803: ISAKMP:     SA life duration (VPI) of  0x0
                                0x20 0xC4 0x9B
*Mar 1 00:28:02.803: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.807: ISAKMP (0:4): Checking IPsec proposal 2
*Mar 1 00:28:02.807: ISAKMP (0:4): transform 1, IPPCP LZS
*Mar 1 00:28:02.807: ISAKMP:   attributes in transform:
*Mar 1 00:28:02.807: ISAKMP:     encaps is 61443
*Mar 1 00:28:02.807: ISAKMP:     SA life type in seconds
*Mar 1 00:28:02.807: ISAKMP:     SA life duration (VPI) of  0x0
                                0x20 0xC4 0x9B
*Mar 1 00:28:02.807: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.807: IPSEC(validate_proposal_request): proposal part #1,
    (key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
    local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
```

```
remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x400
*Mar 1 00:28:02.811: IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400
*Mar 1 00:28:02.815: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.815: IPSEC(validate_transform_proposal): no IPSEC
cryptomap exists for local address 172.16.142.191
*Mar 1 00:28:02.815: ISAKMP (0:4): IPsec policy invalidated proposal
*Mar 1 00:28:02.815: ISAKMP (0:4): Checking IPsec proposal 3
*Mar 1 00:28:02.815: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:02.815: ISAKMP: attributes in transform:
*Mar 1 00:28:02.815: ISAKMP: authenticator is HMAC-MD5
*Mar 1 00:28:02.815: ISAKMP: encaps is 61443
*Mar 1 00:28:02.815: ISAKMP: key length is 128
*Mar 1 00:28:02.819: ISAKMP: SA life type in seconds
*Mar 1 00:28:02.819: ISAKMP: SA life duration (VPI) of 0x0 0x20
0xC4 0x9B
*Mar 1 00:28:02.819: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.819: ISAKMP (0:4): Checking IPsec proposal 3
*Mar 1 00:28:02.819: ISAKMP (0:4): transform 1, IPPCP LZS
*Mar 1 00:28:02.819: ISAKMP: attributes in transform:
*Mar 1 00:28:02.819: ISAKMP: encaps is 61443
*Mar 1 00:28:02.819: ISAKMP: SA life type in seconds
*Mar 1 00:28:02.823: ISAKMP: SA life duration (VPI) of 0x0 0x20
0xC4 0x9B
*Mar 1 00:28:02.823: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.823: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x400
*Mar 1 00:28:02.827: IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400
*Mar 1 00:28:02.827: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.827: IPSEC(validate_transform_proposal): no IPSEC
cryptomap exists for local address 172.16.142.191
*Mar 1 00:28:02.827: ISAKMP (0:4): IPsec policy invalidated proposal
*Mar 1 00:28:02.831: ISAKMP (0:4): Checking IPsec proposal 4
*Mar 1 00:28:02.831: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:02.831: ISAKMP: attributes in transform:
*Mar 1 00:28:02.831: ISAKMP: authenticator is HMAC-SHA
*Mar 1 00:28:02.831: ISAKMP: encaps is 61443
*Mar 1 00:28:02.831: ISAKMP: key length is 128
*Mar 1 00:28:02.831: ISAKMP: SA life type in seconds
*Mar 1 00:28:02.831: ISAKMP: SA life duration (VPI) of 0x0
0x20 0xC4 0x9B
*Mar 1 00:28:02.831: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.835: ISAKMP (0:4): Checking IPsec proposal 4
*Mar 1 00:28:02.835: ISAKMP (0:4): transform 1, IPPCP LZS
*Mar 1 00:28:02.835: ISAKMP: attributes in transform:
```



```

*Mar 1 00:28:02.835: ISAKMP:      encaps is 61443
*Mar 1 00:28:02.835: ISAKMP:      SA life type in seconds
*Mar 1 00:28:02.835: ISAKMP:      SA life duration (VPI) of  0x0 0x20
                                0xC4 0x9B
*Mar 1 00:28:02.835: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.835: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
  local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
  remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-aes esp-sha-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x400
*Mar 1 00:28:02.839: IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
  local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
  remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
  protocol= PCP, transform= comp-lzs ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400
*Mar 1 00:28:02.843: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.843: IPSEC(validate_transform_proposal): no IPSEC
                                cryptomap exists for local address 172.16.142.191
*Mar 1 00:28:02.843: ISAKMP (0:4): IPSec policy invalidated proposal
*Mar 1 00:28:02.843: ISAKMP (0:4): Checking IPSec proposal 5
*Mar 1 00:28:02.843: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:02.843: ISAKMP:      attributes in transform:
*Mar 1 00:28:02.843: ISAKMP:      authenticator is HMAC-MD5
*Mar 1 00:28:02.843: ISAKMP:      encaps is 61443
*Mar 1 00:28:02.843: ISAKMP:      key length is 256
*Mar 1 00:28:02.847: ISAKMP:      SA life type in seconds
*Mar 1 00:28:02.847: ISAKMP:      SA life duration (VPI) of  0x0
                                0x20 0xC4 0x9B
*Mar 1 00:28:02.847: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.847: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
  local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
  remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-aes 256 esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x400
*Mar 1 00:28:02.851: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.851: IPSEC(validate_transform_proposal): no IPSEC
                                cryptomap exists for local address 172.16.142.191
*Mar 1 00:28:02.851: ISAKMP (0:4): IPSec policy invalidated proposal
*Mar 1 00:28:02.851: ISAKMP (0:4): Checking IPSec proposal 6
*Mar 1 00:28:02.851: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:02.851: ISAKMP:      attributes in transform:
*Mar 1 00:28:02.851: ISAKMP:      authenticator is HMAC-SHA
*Mar 1 00:28:02.855: ISAKMP:      encaps is 61443
*Mar 1 00:28:02.855: ISAKMP:      key length is 256
*Mar 1 00:28:02.855: ISAKMP:      SA life type in seconds
*Mar 1 00:28:02.855: ISAKMP:      SA life duration (VPI) of  0x0
                                0x20 0xC4 0x9B
*Mar 1 00:28:02.855: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.855: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
  local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
  remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-aes 256 esp-sha-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x400
*Mar 1 00:28:02.859: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.859: IPSEC(validate_transform_proposal): no IPSEC
                                cryptomap exists for local address 172.16.142.191

```

```

*Mar 1 00:28:02.859: ISAKMP (0:4): IPsec policy invalidated proposal
*Mar 1 00:28:02.859: ISAKMP (0:4): Checking IPsec proposal 7
*Mar 1 00:28:02.859: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:02.863: ISAKMP:   attributes in transform:
*Mar 1 00:28:02.863: ISAKMP:       authenticator is HMAC-MD5
*Mar 1 00:28:02.863: ISAKMP:       encaps is 61443
*Mar 1 00:28:02.863: ISAKMP:       key length is 128
*Mar 1 00:28:02.863: ISAKMP:       SA life type in seconds
*Mar 1 00:28:02.863: ISAKMP:       SA life duration (VPI) of   0x0 0x20
                                0xC4 0x9B
*Mar 1 00:28:02.863: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.863: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
  local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
  remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-aes esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x400
*Mar 1 00:28:02.867: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.867: IPSEC(validate_transform_proposal): no IPSEC
                                cryptomap exists for local address 172.16.142.191
*Mar 1 00:28:02.867: ISAKMP (0:4): IPsec policy invalidated proposal
*Mar 1 00:28:02.867: ISAKMP (0:4): Checking IPsec proposal 8
*Mar 1 00:28:02.871: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:02.871: ISAKMP:   attributes in transform:
*Mar 1 00:28:02.871: ISAKMP:       authenticator is HMAC-SHA
*Mar 1 00:28:02.871: ISAKMP:       encaps is 61443
*Mar 1 00:28:02.871: ISAKMP:       key length is 128
*Mar 1 00:28:02.871: ISAKMP:       SA life type in seconds
*Mar 1 00:28:02.871: ISAKMP:       SA life duration (VPI) of   0x0
                                0x20 0xC4 0x9B
*Mar 1 00:28:02.871: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.875: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
  local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
  remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-aes esp-sha-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x400
*Mar 1 00:28:02.875: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.875: IPSEC(validate_transform_proposal): no IPSEC
                                cryptomap exists for local address 172.16.142.191
*Mar 1 00:28:02.879: ISAKMP (0:4): IPsec policy invalidated proposal
*Mar 1 00:28:02.879: ISAKMP (0:4): Checking IPsec proposal 9
*Mar 1 00:28:02.879: ISAKMP: transform 1, ESP_3DES
*Mar 1 00:28:02.879: ISAKMP:   attributes in transform:
*Mar 1 00:28:02.879: ISAKMP:       authenticator is HMAC-MD5
*Mar 1 00:28:02.879: ISAKMP:       encaps is 61443
*Mar 1 00:28:02.879: ISAKMP:       SA life type in seconds
*Mar 1 00:28:02.879: ISAKMP:       SA life duration (VPI) of   0x0 0x20
                                0xC4 0x9B
*Mar 1 00:28:02.879: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.883: ISAKMP (0:4): Checking IPsec proposal 9
*Mar 1 00:28:02.883: ISAKMP (0:4): transform 1, IPPCP LZS
*Mar 1 00:28:02.883: ISAKMP:   attributes in transform:
*Mar 1 00:28:02.883: ISAKMP:       encaps is 61443
*Mar 1 00:28:02.883: ISAKMP:       SA life type in seconds
*Mar 1 00:28:02.883: ISAKMP:       SA life duration (VPI) of   0x0 0x20
                                0xC4 0x9B
*Mar 1 00:28:02.883: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.883: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
  local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
  remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),

```

```

protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400
*Mar 1 00:28:02.887: IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400
*Mar 1 00:28:02.891: IPSEC(kei_proxy): head = test, map->ivrf = , kei->ivrf =
*Mar 1 00:28:02.891: IPSEC(validate_transform_proposal): no IPSEC
cryptomap exists for local address 172.16.142.191
*Mar 1 00:28:02.891: ISAKMP (0:4): IPsec policy invalidated proposal
*Mar 1 00:28:02.891: ISAKMP (0:4): Checking IPsec proposal 10
*Mar 1 00:28:02.891: ISAKMP: transform 1, ESP_3DES
*Mar 1 00:28:02.891: ISAKMP: attributes in transform:
*Mar 1 00:28:02.891: ISAKMP: authenticator is HMAC-SHA
*Mar 1 00:28:02.891: ISAKMP: encaps is 61443
*Mar 1 00:28:02.891: ISAKMP: SA life type in seconds
*Mar 1 00:28:02.891: ISAKMP: SA life duration (VPI) of 0x0 0x20
0xC4 0x9B
*Mar 1 00:28:02.895: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.895: ISAKMP (0:4): Checking IPsec proposal 10
*Mar 1 00:28:02.895: ISAKMP (0:4): transform 1, IPPCP LZS
*Mar 1 00:28:02.895: ISAKMP: attributes in transform:
*Mar 1 00:28:02.895: ISAKMP: encaps is 61443
*Mar 1 00:28:02.895: ISAKMP: SA life type in seconds
*Mar 1 00:28:02.895: ISAKMP: SA life duration (VPI) of 0x0 0x20
0xC4 0x9B
*Mar 1 00:28:02.899: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:02.899: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.142.191, remote= 171.69.89.82,
local_proxy= 172.16.142.191/255.255.255.255/0/0 (type=1),
remote_proxy= 192.168.1.3/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400
*Mar 1 00:28:02.899: IPSEC(validate_proposal_request): proposal part #2
*Mar 1 00:28:02.923: ISAKMP (0:4): asking for 1 spis from ipsec
*Mar 1 00:28:02.923: ISAKMP (0:4): Node 1783469429, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Mar 1 00:28:02.923: ISAKMP (0:4): Old State = IKE_QM_READY New State =
IKE_QM_SPI_STARVE
*Mar 1 00:28:02.923: IPSEC(key_engine): got a queue event...
*Mar 1 00:28:02.923: IPSEC(spi_response): getting spi 514603422 for SA
from 172.16.142.191 to 171.69.89.82 for prot 3
*Mar 1 00:28:02.927: ISAKMP: received ke message (2/1)
*Mar 1 00:28:03.175: ISAKMP (0:4): sending packet to 171.69.89.82 my_port
4500 peer_port 4500 (R) QM_IDLE
*Mar 1 00:28:03.179: ISAKMP (0:4): Node 1783469429, Input =
IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
*Mar 1 00:28:03.179: ISAKMP (0:4): Old State = IKE_QM_SPI_STARVE
New State = IKE_QM_R_QM2
*Mar 1 00:28:03.239: ISAKMP (0:4): received packet from 171.69.89.82
dport 4500 sport 4500 Global (R) QM_IDLE
*Mar 1 00:28:03.247: ISAKMP: Locking peer struct 0x82C88D44, IPSEC
refcount 1 for for stuff_ke
*Mar 1 00:28:03.247: ISAKMP (0:4): Creating IPsec SAs
*Mar 1 00:28:03.251: inbound SA from 171.69.89.82 to 172.16.142.191
(f/i) 0/ 0
(proxy 192.168.1.3 to 172.16.142.191)
*Mar 1 00:28:03.251: has spi 0x1EAC399E and conn_id 2000 and

```

flags 400

```
*Mar 1 00:28:03.263: IPSEC(create_sa): sa created,
(sa) sa_dest= 171.69.89.82, sa_prot= 50,
sa_spi= 0x1CD14C06(483478534),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001
*Mar 1 00:28:06.675: ISAKMP (0:4): received packet from 171.69.89.82
dport 4500 sport 4500 Global (R) QM_IDLE
*Mar 1 00:28:06.679: ISAKMP: set new node -2064779316 to QM_IDLE
*Mar 1 00:28:06.687: ISAKMP (0:4): processing HASH payload. message
ID = -2064779316
*Mar 1 00:28:06.687: ISAKMP (0:4): processing SA payload. message
ID = -2064779316
*Mar 1 00:28:06.687: ISAKMP (0:4): Checking IPsec proposal 1
*Mar 1 00:28:06.687: ISAKMP: transform 1, ESP_AES
*Mar 1 00:28:06.687: ISAKMP: attributes in transform:
*Mar 1 00:28:06.691: ISAKMP: authenticator is HMAC-MD5
*Mar 1 00:28:06.691: ISAKMP: encaps is 61443
*Mar 1 00:28:06.691: ISAKMP: key length is 256
*Mar 1 00:28:06.691: ISAKMP: SA life type in seconds
*Mar 1 00:28:06.691: ISAKMP: SA life duration (VPI) of 0x0 0x20
0xC4 0x9B
*Mar 1 00:28:06.691: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:06.691: ISAKMP (0:4): Checking IPsec proposal 1
*Mar 1 00:28:06.691: ISAKMP (0:4): transform 1, IPPCP LZS
*Mar 1 00:28:06.691: ISAKMP: attributes in transform:
*Mar 1 00:28:06.695: ISAKMP: encaps is 61443
*Mar 1 00:28:06.695: ISAKMP: SA life type in seconds
*Mar 1 00:28:06.695: ISAKMP: SA life duration (VPI) of 0x0 0x20
0xC4 0x9B
*Mar 1 00:28:06.695: ISAKMP (0:4): atts are acceptable.
*Mar 1 00:28:06.835: IPSEC(spi_response): getting spi 3561761534 for SA
from 172.16.142.191 to 171.69.89.82 for prot 3
*Mar 1 00:28:06.835: ISAKMP: received ke message (2/1)
*Mar 1 00:28:07.127: ISAKMP (0:4): sending packet to 171.69.89.82
my_port 4500 peer_port 4500 (R) QM_IDLE
*Mar 1 00:28:07.127: ISAKMP (0:4): Node -2064779316, Input =
IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
*Mar 1 00:28:07.127: ISAKMP (0:4): Old State = IKE_QM_SPI_STARVE
New State = IKE_QM_R_QM2
*Mar 1 00:28:07.143: ISAKMP (0:4): received packet from 171.69.89.82
dport 4500 sport 4500 Global (R) QM_IDLE
*Mar 1 00:28:07.151: ISAKMP: Locking peer struct 0x82C88D44, IPSEC
refcount 2 for for stuff_ke
*Mar 1 00:28:07.151: ISAKMP (0:4): Creating IPsec SAs
*Mar 1 00:28:07.151: inbound SA from 171.69.89.82 to
172.16.142.191 (f/i) 0/ 0
(proxy 192.168.1.3 to 10.100.100.0)
*Mar 1 00:28:07.151: has spi 0xD44C2AFE and conn_id 2002
and flags 400
*Mar 1 00:28:07.151: lifetime of 2147483 seconds
*Mar 1 00:28:07.151: has client flags 0x10
*Mar 1 00:28:07.151: outbound SA from 172.16.142.191 to
171.69.89.82 (f/i) 0/ 0 (proxy 10.100.100.0
to 192.168.1.3 ),
(sa) sa_dest= 171.69.89.82, sa_prot= 50,
sa_spi= 0x9A12903F(2584907839),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2003
*Mar 1 00:28:15.983: ISAKMP (0:3): purging node -457362469
*Mar 1 00:28:22.863: ISAKMP (0:4): received packet from 171.69.89.82
dport 4500 sport 4500 Global (R) QM_IDLE
*Mar 1 00:28:22.863: ISAKMP: set new node 442126453 to QM_IDLE
*Mar 1 00:28:22.867: ISAKMP (0:4): processing HASH payload. message
ID = 442126453
*Mar 1 00:28:22.867: ISAKMP (0:4): processing NOTIFY unknown protocol 1
```


관련 정보

- [Cisco VPN 클라이언트 지원 페이지](#)
- [IPsec 협상/IKE 프로토콜](#)
- [기술 지원 및 문서 - Cisco Systems](#)