

# IKEv2 VRF 인식 SVTI 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[배경 정보](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[디버그 출력 샘플](#)

[참조](#)

## 소개

이 문서에서는 IKEv2(Internet Key Exchange version 2) 프로토콜을 사용하여 두 VPN(Virtual Private Network) 피어 간에 VRF(Virtual Routing and Forwarding) 인식 SVTI(Static Virtual Tunnel Interface)를 설정하는 컨피그레이션 예를 제공합니다. 이 설정에는 로컬 서브넷이 속하는 IVRF와 터널 설정이 발생하는 FVRF(Front Door VRF)가 포함됩니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IOS CLI 구성에 대한 기본 지식
- IKEv2 및 IPSEC에 대한 기본 지식

### 사용되는 구성 요소

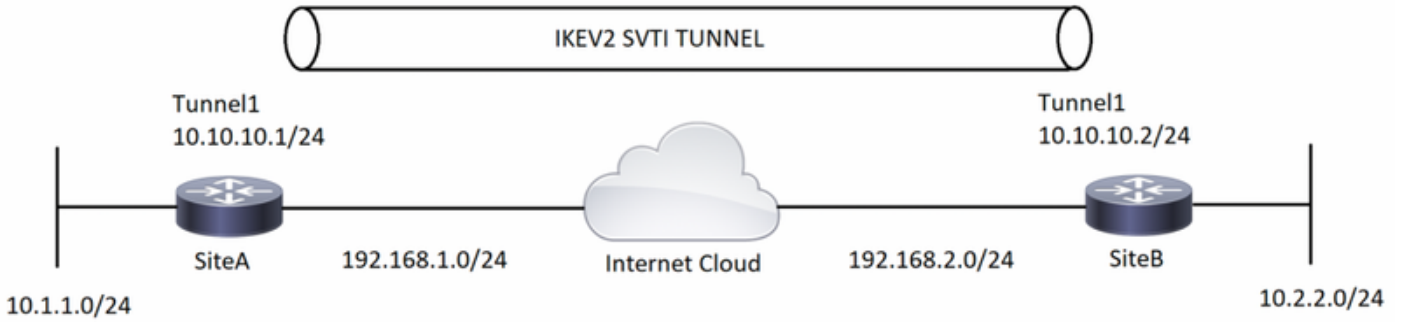
이 문서의 정보는 Cisco IOS® 소프트웨어 릴리스 15.7이 포함된 Cisco IOS 2900 Series 라우터를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 프로덕션 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

# 네트워크 다이어그램



## 배경 정보

VRF 인식 터널은 신뢰할 수 없는 다른 코어 네트워크로 분리된 고객 네트워크 또는 서로 다른 인프라로 코어 네트워크를 연결하는 데 사용됩니다. 이 설정을 사용하면 모든 VRF 테이블에 속하도록 터널의 소스 및 대상을 구성할 수 있습니다.

터널 인터페이스에서 "vrf forwarding" 명령을 사용하여 터널 인터페이스를 특정 라우팅 테이블에 배치합니다. "tunnel vrf" 명령을 사용하면 라우터가 터널 소스 및 대상 IP 주소에 대해 지정된 VRF의 라우팅 테이블을 사용하도록 지시됩니다.

이 문서에 사용된 예에서 루프백 인터페이스 VRF는 LAN 세그먼트 VRF와 같습니다. 이 인터페이스를 통해 들어오는 패킷은 이 VRF를 사용하여 라우팅됩니다. 터널을 빠져나가는 패킷은 이 VRF로 전달됩니다.

"tunnel vrf" 명령을 사용하여 터널에 구성된 VRF는 전송 VRF입니다. 캡슐화된 페이로드에 적용되며 터널 엔드포인트를 찾는 데 사용되는 VRF입니다. 이 VRF는 터널이 패킷을 전송하는 물리적 인터페이스와 연결된 VRF와 동일합니다.

## 구성

1단계. VRF를 정의합니다. 이 예에서는 LAN 및 WAN 인터페이스에 대해 각각 "local" 및 "internet"이라는 두 VRF가 정의됩니다.

SiteA :

! — Defining vrf

```
vrf definition internet
rd 2:2
address-family ipv4
exit-address-family
```

```
vrf definition local
rd 1:1
address-family ipv4
exit-address-family
```

SiteB :

! — Defining vrf

```
vrf definition internet
rd 2:2
address-family ipv4
exit-address-family
```

```
vrf definition local
rd 1:1
address-family ipv4
exit-address-family
```

2단계. IKEv2 제안서 생성 및 키링부터 시작하여 IKEv2 터널을 설정하는 데 필요한 매개변수를 구성합니다. 그런 다음 IKEv2 프로파일은 crypto keyring이 호출되는 곳에서 구성되고 crypto 컨피그레이션으로 마무리하기 위해 IPSEC 프로필에 IPSEC transform-set 및 IKEv2 프로필이 포함됩니다.

**SiteA :**

**! — IKEv2 Proposal**

```
crypto ikev2 proposal prop-1
encryption aes-cbc-256
integrity sha512
group 5
```

**! --- IKEv2 Policy**

```
crypto ikev2 policy policy-1
match fvrf internet
match address local 192.168.1.1
proposal prop-1
```

**! — IKEv2 Keyring**

```
crypto ikev2 keyring keyring-1
peer ANY
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123
```

**! — IKEv2 Profile**

```
crypto ikev2 profile IKEv2-Profile-1
match fvrf internet
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local keyring-1
```

**! — IPSEC Transform set**

```
crypto ipsec transform-set transform-1 esp-aes 256 esp-sha-hmac
mode transport
```

**! — IPSEC Profile**

```
crypto ipsec profile IPSEC-Profile-1
set transform-set transform-1
set ikev2-profile IKEv2-Profile-1
```

**SiteB :**

**! — IKEv2 Proposal**

```
crypto ikev2 proposal prop-1
  encryption aes-cbc-256
  integrity sha512
  group 5
```

**! -- IKEv2 Policy**

```
crypto ikev2 policy policy-1
match fvrfl internet
match address local 192.168.2.1
proposal prop-1 ! — IKEv2 Keyring
```

```
crypto ikev2 keyring keyring-1
  peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco123
```

**! — IKEv2 Profile**

```
crypto ikev2 profile IKEv2-Profile-1
  match fvrfl internet
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local keyring-1
```

**! — IPSEC Transform set**

```
crypto ipsec transform-set transform-1 esp-aes 256 esp-sha-hmac
mode transport
```

**! — IPSEC Profile**

```
crypto ipsec profile IPSEC-Profile-1
  set transform-set transform-1
  set ikev2-profile IKEv2-Profile-1
```

3단계. 필요한 인터페이스를 구성합니다. 이 예에서 루프백 인터페이스는 "local" VRF의 일부이며 흥미로운 트래픽으로 작동합니다. "인터넷" VRF의 일부인 물리적 인터페이스는 ISP에 연결된 WAN 인터페이스입니다. 터널 인터페이스는 IPSEC로 암호화된 GRE 캡슐화를 트리거합니다.

**SiteA :**

**! — Interface Configuration**

```
interface Loopback1
  vrf forwarding local
  ip address 10.1.1.1 255.255.255.0
```

```
interface Tunnel1
  vrf forwarding local
  ip address 10.10.10.1 255.255.255.0
  tunnel source 192.168.1.1
  tunnel destination 192.168.2.1
  tunnel key 777
  tunnel vrf internet
  tunnel protection ipsec profile IPSEC-Profile-1
```

```
interface GigabitEthernet0/0
  vrf forwarding internet
  ip address 192.168.1.1 255.255.255.0
```

SiteB :

! — Interface Configuration

```
interface Loopback1
  vrf forwarding local
  ip address 10.2.2.2 255.255.255.0

interface Tunnel1
  vrf forwarding local
  ip address 10.10.10.2 255.255.255.0
  tunnel source 192.168.2.1
  tunnel destination 192.168.1.1
  tunnel key 777
  tunnel vrf internet
  tunnel protection ipsec profile IPSEC-Profile-1

interface GigabitEthernet0/0
  vrf forwarding internet
  ip address 192.168.2.1 255.255.255.0
```

4단계:VRF 관련 경로를 구성합니다.이 설정에서는 "인터넷" VRF의 경로가 물리적 인터페이스의 next hop(또는 실제 환경의 ISP)을 가리키는 기본 경로로 구성됩니다. "local" VRF의 두 번째 경로는 터널 인터페이스를 가리키는 원격 VPN 서버넷에 대한 것입니다. 이 서버넷은 결국 트래픽이 터널 인터페이스를 통과하여 VPN을 트리거합니다.

SiteA :

! — VRF specific routes

```
ip route vrf internet 0.0.0.0 0.0.0.0 192.168.1.2
ip route vrf local 10.2.2.0 255.255.255.0 Tunnel1
```

SiteB :

! — VRF specific routes

```
ip route vrf internet 0.0.0.0 0.0.0.0 192.168.2.2
ip route vrf local 10.1.1.0 255.255.255.0 tunnel 1
```

## 다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다. [Cisco CLI Analyzer](#)는 특정 show 명령을 지원합니다.Cisco CLI Analyzer를 사용하여 show 명령 출력의 분석을 봅니다.

SiteA :

SiteA#show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

	Tunnel-id	Local	Remote	fvr/f/ivrf	Status
1	192.168.1.1/500	192.168.2.1/500	internet/local	READY	

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK  
Life/Active Time: 86400/128 sec

SiteA#show crypto ipsec sa detail

interface: Tunnell

Crypto map tag: Tunnell-head-0, local addr 192.168.1.1

protected vrf: local

**local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)**

**remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0)**

current\_peer 192.168.2.1 port 500

PERMIT, flags={origin\_is\_acl,}

**#pkts encaps: 25, #pkts encrypt: 25, #pkts digest: 25**

**#pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25**

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#pkts no sa (send) 0, #pkts invalid sa (rcv) 0

#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0

#pkts invalid prot (rcv) 0, #pkts verify failed: 0

#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0

#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0

##pkts replay failed (rcv): 0

#pkts tagged (send): 0, #pkts untagged (rcv): 0

#pkts not tagged (send): 0, #pkts not untagged (rcv): 0

#pkts internal err (send): 0, #pkts internal err (rcv) 0

**local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.2.1**

plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0

current outbound spi: 0xE0B1BF6B(3769745259)

PFS (Y/N): N, DH group: none

**inbound esp sas:**

**spi: 0xCA8E7D53(3398335827)**

transform: esp-256-aes esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2010, flow\_id: Onboard VPN:10, sibling\_flags 80000000, crypto map: Tunnell-

head-0

sa timing: remaining key lifetime (k/sec): (4368363/3461)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

**outbound esp sas:**

**spi: 0xE0B1BF6B(3769745259)**

transform: esp-256-aes esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2009, flow\_id: Onboard VPN:9, sibling\_flags 80000000, crypto map: Tunnell-head-

0

sa timing: remaining key lifetime (k/sec): (4368363/3461)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

SiteA#show crypto session remote 192.168.2.1 detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation  
X - IKE Extended Authentication, F - IKE Fragmentation  
R - IKE Auto Reconnect, U - IKE Dynamic Route Update  
S - SIP VPN

Interface: Tunnell

Profile: IKEv2-Profile-1

Uptime: 00:02:35

Session status: **UP-ACTIVE**

Peer: 192.168.2.1 port 500 fvrf: internet ivrf: local

Phase1\_id: 192.168.2.1

Desc: (none)

Session ID: 3

IKEv2 SA: local 192.168.1.1/500 remote 192.168.2.1/500 Active

Capabilities:(none) connid:1 lifetime:23:57:25

IPSEC FLOW: permit 47 host 192.168.1.1 host 192.168.2.1

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4368363/3444

Outbound: #pkts enc'ed 25 drop 0 life (KB/Sec) 4368363/3444

**SiteB :**

**SiteB#show crypto ikev2 sa**

IPv4 Crypto IKEv2 SA

	Tunnel-id	Local	Remote	fvrf/ivrf	Status
1	192.168.2.1/500	192.168.1.1/500	internet/local	READY	

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK  
Life/Active Time: 86400/90 sec

**SiteB#show crypto ipsec sa detail**

interface: Tunnell

Crypto map tag: Tunnell-head-0, local addr 192.168.2.1

protected vrf: local

**local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0)**

**remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)**

current\_peer 192.168.1.1 port 500

PERMIT, flags={origin\_is\_acl,}

**#pkts encaps: 25, #pkts encrypt: 25, #pkts digest: 25**

**#pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25**

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#pkts no sa (send) 0, #pkts invalid sa (rcv) 0

#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0

#pkts invalid prot (rcv) 0, #pkts verify failed: 0

#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0

#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0

##pkts replay failed (rcv): 0

#pkts tagged (send): 0, #pkts untagged (rcv): 0

#pkts not tagged (send): 0, #pkts not untagged (rcv): 0

#pkts internal err (send): 0, #pkts internal err (rcv) 0

**local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1**

plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0

current outbound spi: 0xCA8E7D53(3398335827)

PFS (Y/N): N, DH group: none

**inbound esp sas:**

```

spi: 0xE0B1BF6B(3769745259)
  transform: esp-256-aes esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2009, flow_id: Onboard VPN:9, sibling_flags 80000000, crypto map: Tunnel1-head-
0
  sa timing: remaining key lifetime (k/sec): (4251213/3468)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xCA8E7D53(3398335827)
  transform: esp-256-aes esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2010, flow_id: Onboard VPN:10, sibling_flags 80000000, crypto map: Tunnel1-
head-0
  sa timing: remaining key lifetime (k/sec): (4251213/3468)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

```

```

SiteB#show crypto session remote 192.168.1.1 detail
Crypto session current status

```

```

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect

```

```

Interface: Tunnel1
Profile: IKEv2-Profile-1
Uptime: 00:02:33
Session status: UP-ACTIVE
Peer: 192.168.1.1 port 500 fvrf: internet ivrf: local
  Phase1_id: 192.168.1.1
  Desc: (none)
Session ID: 4
IKEv2 SA: local 192.168.2.1/500 remote 192.168.1.1/500 Active
  Capabilities:(none) connid:1 lifetime:23:57:27
IPSEC FLOW: permit 47 host 192.168.2.1 host 192.168.1.1
  Active SAs: 2, origin: crypto map
  Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4251213/3447
  Outbound: #pkts enc'ed 25 drop 0 life (KB/Sec) 4251213/3447

```

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다. 샘플 디버그 출력도 표시됩니다.

### 문제 해결 명령

참고: debug 명령 을 사용하기 전에 [디버그 명령](#)에 대한 중요 정보를 참조하십시오. 라우터에 여러 터널이 구성된 경우 다음 조건을 사용할 수 있습니다.



- 디버그 crypto ikev2 내부
- 암호화 ikev2 패킷 디버그

## 디버그 출력 샘플

### SiteA Debugs :

```

*Jul 16 05:30:50.731: IKEv2: Got a packet from dispatcher
*Jul 16 05:30:50.731: IKEv2: Processing an item off the pak queue
*Jul 16 05:30:50.731: IKEv2-INTERNAL:% Getting preshared key by address 192.168.2.1
*Jul 16 05:30:50.731: IKEv2-INTERNAL:Adding Proposal default to toolkit policy
*Jul 16 05:30:50.731: IKEv2-INTERNAL:(1): Choosing IKE profile IKEv2-Profile-1
*Jul 16 05:30:50.731: IKEv2-INTERNAL:New ikev2 sa request admitted
*Jul 16 05:30:50.731: IKEv2-INTERNAL:Incrementing outgoing negotiating sa count by one

*Jul 16 05:30:50.731: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: IDLE Event: EV_INIT_SA
*Jul 16 05:30:50.731: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: I_BLD_INIT Event:
EV_GET_IKE_POLICY
*Jul 16 05:30:50.731: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: I_BLD_INIT Event:
EV_SET_POLICY
*Jul 16 05:30:50.731: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Setting configured policies
*Jul 16 05:30:50.731: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: I_BLD_INIT Event:
EV_CHK_AUTH4PKI
*Jul 16 05:30:50.731: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: I_BLD_INIT Event:
EV_GEN_DH_KEY
*Jul 16 05:30:50.791: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: I_BLD_INIT Event:
EV_NO_EVENT
*Jul 16 05:30:50.791: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: I_BLD_INIT Event:
EV_OK_REC'D_DH_PUBKEY_RESP
*Jul 16 05:30:50.791: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Action: Action_Null
*Jul 16 05:30:50.791: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: I_BLD_INIT Event:
EV_GET_CONFIG_MODE
*Jul 16 05:30:50.791: IKEv2-INTERNAL:No config data to send to toolkit:
*Jul 16 05:30:50.791: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=0000000000000000 (I) MsgID = 0 CurState: I_BLD_INIT Event:
EV_BLD_MSG
*Jul 16 05:30:50.791: IKEv2-INTERNAL:Construct Vendor Specific Payload: DELETE-REASON
*Jul 16 05:30:50.791: IKEv2-INTERNAL:Construct Vendor Specific Payload: CISCOVPN-REV-02
*Jul 16 05:30:50.791: IKEv2-INTERNAL:Sending DRU Handshake
*Jul 16 05:30:50.791: IKEv2-INTERNAL:(1): Sending custom vendor id : CISCO-DYNAMIC-ROUTE
*Jul 16 05:30:50.791: IKEv2-INTERNAL:Construct Vendor Specific Payload: (CUSTOM)
*Jul 16 05:30:50.791: IKEv2-INTERNAL:Construct Vendor Specific Payload: (CUSTOM)
*Jul 16 05:30:50.791: IKEv2-INTERNAL:Construct Notify Payload: NAT_DETECTION_SOURCE_IP
*Jul 16 05:30:50.791: IKEv2-INTERNAL:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP

*Jul 16 05:30:50.795: IKEv2-PAK:(SESSION ID = 3,SA ID = 1):Next payload: SA, version: 2.0
Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 550
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 144
  last proposal: 0x0, reserved: 0x0, length: 140
  Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 15      last transform: 0x3, reserved: 0x0:

```

length: 12  
type: 1, reserved: 0x0, id: AES-CBC  
last transform: 0x3, reserved: 0x0: length: 12  
type: 1, reserved: 0x0, id: AES-CBC  
last transform: 0x3, reserved: 0x0: length: 12  
type: 1, reserved: 0x0, id: AES-CBC  
last transform: 0x3, reserved: 0x0: length: 8  
type: 2, reserved: 0x0, id: SHA512  
last transform: 0x3, reserved: 0x0: length: 8  
type: 2, reserved: 0x0, id: SHA384  
last transform: 0x3, reserved: 0x0: length: 8  
type: 2, reserved: 0x0, id: SHA256  
last transform: 0x3, reserved: 0x0: length: 8  
type: 2, reserved: 0x0, id: SHA1  
last transform: 0x3, reserved: 0x0: length: 8  
type: 2, reserved: 0x0, id: MD5  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA512  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA384  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA256  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA96  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: MD596  
last transform: 0x3, reserved: 0x0: length: 8  
type: 4, reserved: 0x0, id: DH\_GROUP\_1536\_MODP/Group 5  
last transform: 0x0, reserved: 0x0: length: 8  
type: 4, reserved: 0x0, id: DH\_GROUP\_1024\_MODP/Group 2  
KE Next payload: N, reserved: 0x0, length: 200  
DH group: 5, Reserved: 0x0  
N Next payload: VID, reserved: 0x0, length: 36  
VID Next payload: VID, reserved: 0x0, length: 23  
VID Next payload: VID, reserved: 0x0, length: 19  
VID Next payload: VID, reserved: 0x0, length: 23  
VID Next payload: NOTIFY, reserved: 0x0, length: 21  
NOTIFY(NAT\_DETECTION\_SOURCE\_IP) Next payload: NOTIFY, reserved: 0x0, length: 28  
Security protocol id: Unknown - 0, spi size: 0, type: NAT\_DETECTION\_SOURCE\_IP  
NOTIFY(NAT\_DETECTION\_DESTINATION\_IP) Next payload: NONE, reserved: 0x0, length: 28  
Security protocol id: Unknown - 0, spi size: 0, type: NAT\_DETECTION\_DESTINATION\_IP

\*Jul 16 05:30:50.931: **IKEv2-INTERNAL:Got a packet from dispatcher**  
\*Jul 16 05:30:50.931: **IKEv2-INTERNAL:Processing an item off the pak queue**

\*Jul 16 05:30:50.939: **IKEv2-PAK:(SESSION ID = 3,SA ID = 1):Next payload: SA, version: 2.0**  
**Exchange type: IKE\_SA\_INIT, flags: RESPONDER MSG-RESPONSE** Message id: 0, length: 431  
**Payload contents:**  
SA Next payload: KE, reserved: 0x0, length: 48  
last proposal: 0x0, reserved: 0x0, length: 44  
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 last transform: 0x3, reserved: 0x0:  
length: 12  
type: 1, reserved: 0x0, id: AES-CBC  
last transform: 0x3, reserved: 0x0: length: 8  
type: 2, reserved: 0x0, id: SHA512  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA512  
last transform: 0x0, reserved: 0x0: length: 8  
type: 4, reserved: 0x0, id: DH\_GROUP\_1536\_MODP/Group 5  
KE Next payload: N, reserved: 0x0, length: 200  
DH group: 5, Reserved: 0x0  
N Next payload: VID, reserved: 0x0, length: 36

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:Parse Vendor Specific Payload: CISCO-DELETE-REASON  
VID Next payload: VID, reserved: 0x0, length: 23

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:Parse Vendor Specific Payload: CISCOVPN-REV VID Next  
payload: VID, reserved: 0x0, length: 19

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:Parse Vendor Specific Payload: (CUSTOM) VID Next payload:  
NOTIFY, reserved: 0x0, length: 21

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:Parse Notify Payload: NAT\_DETECTION\_SOURCE\_IP  
NOTIFY(NAT\_DETECTION\_SOURCE\_IP) Next payload: NOTIFY, reserved: 0x0, length: 28  
Security protocol id: Unknown - 0, spi size: 0, type: NAT\_DETECTION\_SOURCE\_IP

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:Parse Notify Payload: NAT\_DETECTION\_DESTINATION\_IP  
NOTIFY(NAT\_DETECTION\_DESTINATION\_IP) Next payload: NONE, reserved: 0x0, length: 28  
Security protocol id: Unknown - 0, spi size: 0, type: NAT\_DETECTION\_DESTINATION\_IP

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_WAIT\_INIT Event:  
EV\_RECV\_INIT

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Processing IKE\_SA\_INIT message

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_PROC\_INIT Event:  
EV\_CHK4\_NOTIFY

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_PROC\_INIT Event:  
EV\_VERIFY\_MSG

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_PROC\_INIT Event:  
EV\_PROC\_MSG

\*Jul 16 05:30:50.939: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_PROC\_INIT Event:  
EV\_DETECT\_NAT

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Process NAT discovery notify

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Processing nat detect src notify

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Remote address matched

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Processing nat detect dst notify

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Local address matched

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):No NAT found

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_PROC\_INIT Event:  
EV\_CHK\_NAT\_T

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_PROC\_INIT Event:  
EV\_CHK\_CONFIG\_MODE

\*Jul 16 05:30:50.943: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: INIT\_DONE Event:  
**EV\_GEN\_DH\_SECRET**

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: INIT\_DONE Event:  
EV\_NO\_EVENT

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: INIT\_DONE Event:  
EV\_OK\_REC'D\_DH\_SECRET\_RESP

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Action: Action\_Null

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: INIT\_DONE Event:  
**EV\_GEN\_SKEYID**

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):**Generate skeyid**

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: INIT\_DONE Event: EV\_DONE

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Cisco DeleteReason Notify is  
enabled

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: INIT\_DONE Event:  
EV\_CHK4\_ROLE

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_BLD\_AUTH Event:  
EV\_GET\_CONFIG\_MODE

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:Sending config data to toolkit

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_BLD\_AUTH Event:  
EV\_CHK\_EAP

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_BLD\_AUTH Event:  
**EV\_GEN\_AUTH**

\*Jul 16 05:30:51.019: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_BLD\_AUTH Event:  
EV\_CHK\_AUTH\_TYPE

\*Jul 16 05:30:51.023: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_BLD\_AUTH Event:  
EV\_OK\_AUTH\_GEN

\*Jul 16 05:30:51.023: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 0 CurState: I\_BLD\_AUTH Event:  
EV\_SEND\_AUTH

\*Jul 16 05:30:51.023: IKEv2-INTERNAL:Construct Vendor Specific Payload: CISCO-GRANITE

\*Jul 16 05:30:51.023: IKEv2-INTERNAL:Construct Notify Payload: INITIAL\_CONTACT

\*Jul 16 05:30:51.023: IKEv2-INTERNAL:Construct Notify Payload: USE\_TRANSPORT\_MODE

\*Jul 16 05:30:51.023: IKEv2-INTERNAL:Construct Notify Payload: SET\_WINDOW\_SIZE

\*Jul 16 05:30:51.023: IKEv2-INTERNAL:Construct Notify Payload: ESP\_TFC\_NO\_SUPPORT

\*Jul 16 05:30:51.023: IKEv2-INTERNAL:Construct Notify Payload: NON\_FIRST\_FRAGS

**Payload contents:**

VID Next payload: IDi, reserved: 0x0, length: 20

IDi Next payload: AUTH, reserved: 0x0, length: 12

Id type: IPv4 address, Reserved: 0x0 0x0

AUTH Next payload: CFG, reserved: 0x0, length: 72

Auth method PSK, reserved: 0x0, reserved 0x0

CFG Next payload: SA, reserved: 0x0, length: 304

cfg type: CFG\_REQUEST, reserved: 0x0, reserved: 0x0

\*Jul 16 05:30:51.023: SA Next payload: TSi, reserved: 0x0, length: 44

last proposal: 0x0, reserved: 0x0, length: 40

Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0:  
length: 12

type: 1, reserved: 0x0, id: AES-CBC

last transform: 0x3, reserved: 0x0: length: 8

type: 3, reserved: 0x0, id: SHA96

last transform: 0x0, reserved: 0x0: length: 8

type: 5, reserved: 0x0, id: Don't use ESN

TSi Next payload: TSr, reserved: 0x0, length: 24

Num of TSs: 1, reserved 0x0, reserved 0x0

TS type: TS\_IPV4\_ADDR\_RANGE, proto id: 47, length: 16

start port: 0, end port: 65535

start addr: 192.168.1.1, end addr: 192.168.1.1

TSr Next payload: NOTIFY, reserved: 0x0, length: 24

Num of TSs: 1, reserved 0x0, reserved 0x0

TS type: TS\_IPV4\_ADDR\_RANGE, proto id: 47, length: 16

start port: 0, end port: 65535

start addr: 192.168.2.1, end addr: 192.168.2.1

NOTIFY(INITIAL\_CONTACT) Next payload: NOTIFY, reserved: 0x0, length: 8

Security protocol id: Unknown - 0, spi size: 0, type: INITIAL\_CONTACT

NOTIFY(USE\_TRANSPORT\_MODE) Next payload: NOTIFY, reserved: 0x0, length: 8

Security protocol id: Unknown - 0, spi size: 0, type: USE\_TRANSPORT\_MODE

NOTIFY(SET\_WINDOW\_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12

Security protocol id: Unknown - 0, spi size: 0, type: SET\_WINDOW\_SIZE

NOTIFY(ESP\_TFC\_NO\_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8

Security protocol id: Unknown - 0, spi size: 0, type: ESP\_TFC\_NO\_SUPPORT

NOTIFY(NON\_FIRST\_FRAGS) Next payload: NONE, reserved: 0x0, length: 8

Security protocol id: Unknown - 0, spi size: 0, type: NON\_FIRST\_FRAGS

\*Jul 16 05:30:51.023: **IKEv2-PAK:(SESSION ID = 3,SA ID = 1):Next payload: ENCR, version: 2.0**

**Exchange type: IKE\_AUTH, flags: INITIATOR** Message id: 1, length: 640

**Payload contents:**

ENCR Next payload: VID, reserved: 0x0, length: 612

\*Jul 16 05:30:51.023: **IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:**

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 1 CurState: I\_WAIT\_AUTH Event:  
EV\_NO\_EVENT

\*Jul 16 05:30:51.023: **IKEv2-INTERNAL:Got a packet from dispatcher**

\*Jul 16 05:30:51.023: **IKEv2-INTERNAL:Processing an item off the pak queue**

\*Jul 16 05:30:51.107: **IKEv2-PAK:(SESSION ID = 3,SA ID = 1):Next payload: ENCR, version: 2.0**

**Exchange type: IKE\_AUTH, flags: RESPONDER MSG-RESPONSE** Message id: 1, length: 320

**Payload contents:**

\*Jul 16 05:30:51.111: **IKEv2-INTERNAL:Parse Vendor Specific Payload: (CUSTOM) VID** Next payload:  
IDr, reserved: 0x0, length: 20

IDr Next payload: AUTH, reserved: 0x0, length: 12

Id type: IPv4 address, Reserved: 0x0 0x0

AUTH Next payload: SA, reserved: 0x0, length: 72

Auth method PSK, reserved: 0x0, reserved 0x0

SA Next payload: TSi, reserved: 0x0, length: 44

last proposal: 0x0, reserved: 0x0, length: 40

Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0:  
length: 12

type: 1, reserved: 0x0, id: AES-CBC

last transform: 0x3, reserved: 0x0: length: 8

type: 3, reserved: 0x0, id: SHA96

last transform: 0x0, reserved: 0x0: length: 8

type: 5, reserved: 0x0, id: Don't use ESN

TSi Next payload: TSr, reserved: 0x0, length: 24

Num of TSs: 1, reserved 0x0, reserved 0x0

TS type: TS\_IPV4\_ADDR\_RANGE, proto id: 47, length: 16

start port: 0, end port: 65535

start addr: 192.168.1.1, end addr: 192.168.1.1

TSr Next payload: NOTIFY, reserved: 0x0, length: 24

Num of TSs: 1, reserved 0x0, reserved 0x0

TS type: TS\_IPV4\_ADDR\_RANGE, proto id: 47, length: 16

start port: 0, end port: 65535

start addr: 192.168.2.1, end addr: 192.168.2.1

\*Jul 16 05:30:51.111: **IKEv2-INTERNAL:Parse Notify Payload: USE\_TRANSPORT\_MODE**

NOTIFY(USE\_TRANSPORT\_MODE) Next payload: NOTIFY, reserved: 0x0, length: 8

Security protocol id: Unknown - 0, spi size: 0, type: USE\_TRANSPORT\_MODE

\*Jul 16 05:30:51.111: **IKEv2-INTERNAL:Parse Notify Payload: SET\_WINDOW\_SIZE**

NOTIFY(SET\_WINDOW\_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12

Security protocol id: Unknown - 0, spi size: 0, type: SET\_WINDOW\_SIZE

\*Jul 16 05:30:51.111: **IKEv2-INTERNAL:Parse Notify Payload: ESP\_TFC\_NO\_SUPPORT**

NOTIFY(ESP\_TFC\_NO\_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8

Security protocol id: Unknown - 0, spi size: 0, type: ESP\_TFC\_NO\_SUPPORT

\*Jul 16 05:30:51.111: **IKEv2-INTERNAL:Parse Notify Payload: NON\_FIRST\_FRAGS**

NOTIFY(NON\_FIRST\_FRAGS) Next payload: NONE, reserved: 0x0, length: 8

Security protocol id: Unknown - 0, spi size: 0, type: NON\_FIRST\_FRAGS

\*Jul 16 05:30:51.111: **IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:**

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 1 CurState: I\_WAIT\_AUTH Event:

**EV\_RECV\_AUTH**

\*Jul 16 05:30:51.111: **IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):Action: Action\_Null**

\*Jul 16 05:30:51.123: **IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:**

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 1 CurState: READY Event:  
EV\_CHK\_IKE\_ONLY  
\*Jul 16 05:30:51.123: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (I) MsgID = 1 CurState: READY Event: EV\_I\_OK  
\*Jul 16 05:30:52.011: SM Trace-> SA: I\_SPI=34CDD54C620910B0 R\_SPI=F1A0F4AB68B75F00 (R) MsgID = 1  
CurState: AUTH\_DONE Event: EV\_CHK4\_ROLE  
\*Jul 16 05:30:52.027: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=34CDD54C620910B0 R\_SPI=F1A0F4AB68B75F00 (R) MsgID = 1 CurState: READY Event: EV\_R\_OK  
\*Jul 16 05:30:52.027: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=34CDD54C620910B0 R\_SPI=F1A0F4AB68B75F00 (R) MsgID = 1 CurState: READY Event: EV\_NO\_E  
\*Jul 16 05:30:52.027: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=34CDD54C620910B0 R\_SPI=F1A0F4AB68B75F00 (R) MsgID = 1 CurState:I\_PROC\_AUTH: **EV\_VERIFY\_AUTH**  
\*Jul 16 05:30:52.027: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=34CDD54C620910B0 R\_SPI=F1A0F4AB68B75F00 (R) MsgID = 1 CurState:I\_PROC\_AUTH  
**EVENT:EV\_NOTIFY\_AUTH\_DONE**  
\*Jul 16 05:30:52.027: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=34CDD54C620910B0 R\_SPI=F1A0F4AB68B75F00 (R) MsgID = 1 CurState:**AUTH\_DONE** Event  
EV\_CHK4\_ROLE  
\*Jul 16 05:30:52.027: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=34CDD54C620910B0 R\_SPI=F1A0F4AB68B75F00 (R) MsgID = 1 CurState: **READY**Event:  
EV\_CHK\_IKE\_ONLY  
\*Jul 16 05:30:52.027: IKEv2-INTERNAL:(SESSION ID = 3,SA ID = 1):SM Trace-> SA:  
I\_SPI=34CDD54C620910B0 R\_SPI=F1A0F4AB68B75F00 (R) MsgID = 1 CurState: READYEvent: **EV\_I\_OK**

#### SiteB Debugs:

\*Jul 16 06:01:45.231: **IKEv2-INTERNAL:Got a packet from dispatcher**  
\*Jul 16 06:01:45.231: **IKEv2-INTERNAL:Processing an item off the pak queue**  
\*Jul 16 06:01:45.231: **IKEv2-INTERNAL:New ikev2 sa request admitted**  
\*Jul 16 06:01:45.231: **IKEv2-INTERNAL:Incrementing incoming negotiating sa count by one**  
\*Jul 16 06:01:45.231: **IKEv2-PAK:Next payload: SA, version: 2.0 Exchange type: IKE\_SA\_INIT, flags: INITIATOR** Message id: 0, length: 550  
**Payload contents:**  
SA Next payload: KE, reserved: 0x0, length: 144  
last proposal: 0x0, reserved: 0x0, length: 140  
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 15 last transform: 0x3, reserved: 0x0:  
length: 12  
type: 1, reserved: 0x0, id: AES-CBC  
last transform: 0x3, reserved: 0x0: length: 12  
type: 1, reserved: 0x0, id: AES-CBC  
last transform: 0x3, reserved: 0x0: length: 8  
type: 2, reserved: 0x0, id: SHA1  
last transform: 0x3, reserved: 0x0: length: 12  
type: 1, reserved: 0x0, id: AES-CBC  
last transform: 0x3, reserved: 0x0: 1 last transform: 0x3, reserved: 0x0: length: 8  
type: 2, reserved: 0x0, id: MD5  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA512  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA384  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA256  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: SHA96  
last transform: 0x3, reserved: 0x0: length: 8  
type: 3, reserved: 0x0, id: MD596  
last transform: 0x3, reserved: 0x0: length: 8  
type: 4, reserved: 0x0, id: DH\_GROUP\_1536\_MODP/Group 5  
type: 2, reserved: 0x0, id: SHA512  
last trans0x0, length: 23

KE Next payload: N, reserved: 0x0, length: 200

DH group: 5, Reserved: 0x0

N Next payload: VID, reserved: 0x0, length: 36

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:Parse Vendor Specific Payload: CISCOVPN-REV VID Next payload: VID, reserved: 0x0, length: 19

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: VID, reserved: 0x0, length: 23

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:form: 0x3, reserved: 0x0: length: 8

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID Next payload: VID, reserved:

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:Parse Notify Payload: NAT\_DETECTION\_SOURCE\_IP NOTIFY(NAT\_DETECTION\_SOURCE\_IP) Next payload: NOTIFY, reserved: 0x0, length: 28  
Security protocol id: Unknown - 0, spi size: 0, type: NAT\_DETECTION\_SOURCE\_IP

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:Parse Notify Payload: NAT\_DETECTION\_DESTINATION\_IP NOTIFY(NAT\_DETECTION\_DESTINATION\_IP) Next payload: NONE, reserved: 0x0, length: 28  
Security protocol id: Unknown - 0, spi size: 0, type: NAT\_DETECTION\_DESTINATION\_IP

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: IDLE Event: **EV\_RECV\_INIT**

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_INIT Event:

**EV\_VERIFY\_MSG**

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_INIT Event: **EV\_INSERT\_SA**

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_INIT Event:

**EV\_GET\_IKE\_POLICY**

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:Adding Proposal default to toolkit policy

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_INIT Event: **EV\_PROC\_MSG**

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_INIT Event:

**EV\_DETECT\_NAT**

\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Process NAT discovery notify  
\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Processing nat detect src notify  
\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Remote address matched  
\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Processing nat detect dst notify  
\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Local address matched  
\*Jul 16 06:01:45.231: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):No NAT found

\*Jul 16 06:01:45.235: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_INIT Event:

**EV\_CHK\_CONFIG\_MODE**

\*Jul 16 06:01:45.235: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:

**EV\_SET\_POLICY**

\*Jul 16 06:01:45.235: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):**Setting configured policies**

\*Jul 16 06:01:45.235: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:

**EV\_CHK\_AUTH4PKI**

\*Jul 16 06:01:45.235: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:

**EV\_GEN\_DH\_KEY**

\*Jul 16 06:01:45.295: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:

**EV\_NO\_EVENT**

\*Jul 16 06:01:45.295: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:

**EV\_OK\_REC'D\_DH\_PUBKEY\_RESP**

\*Jul 16 06:01:45.295: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Action: Action\_Null

\*Jul 16 06:01:45.295: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:  
**EV\_GEN\_DH\_SECRET**  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:  
EV\_NO\_EVENT  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:  
EV\_OK\_REC'D\_DH\_SECRET\_RESP  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Action: Action\_Null  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:  
EV\_GEN\_SKEYID  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):**Generate skeyid**  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:  
EV\_GET\_CONFIG\_MODE  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:No config data to send to toolkit:  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_BLD\_INIT Event:  
EV\_BLD\_MSG  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:Construct Vendor Specific Payload: DELETE-REASON  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:Construct Vendor Specific Payload: CISCOVPN-REV-02  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:Construct Vendor Specific Payload: (CUSTOM)  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:Construct Notify Payload: NAT\_DETECTION\_SOURCE\_IP  
\*Jul 16 06:01:45.371: IKEv2-INTERNAL:Construct Notify Payload: NAT\_DETECTION\_DESTINATION\_IP  
  
\*Jul 16 06:01:45.371: **IKEv2-PAK:(SESSION ID = 4,SA ID = 1):Next payload: SA, version: 2.0**  
**Exchange type: IKE\_SA\_INIT, flags: RESPONDER MSG-RESPONSE** Message id: 0, length: 431  
**Payload contents:**  
SA Next payload: KE, reserved: 0x0, length: 48  
    last proposal: 0x0, reserved: 0x0, length: 44  
    Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4    last transform: 0x3, reserved: 0x0:  
length: 12  
    type: 1, reserved: 0x0, id: AES-CBC  
    last transform: 0x3, reserved: 0x0: length: 8  
    type: 2, reserved: 0x0, id: SHA512  
    last transform: 0x3, reserved: 0x0: length: 8  
    type: 3, reserved: 0x0, id: SHA512  
    last transform: 0x0, reserved: 0x0: length: 8  
    type: 4, reserved: 0x0, id: DH\_GROUP\_1536\_MODP/Group 5  
KE Next payload: N, reserved: 0x0, length: 200  
    DH group: 5, Reserved: 0x0  
N Next payload: VID, reserved: 0x0, length: 36  
VID Next payload: VID, reserved: 0x0, length: 23  
VID Next payload: VID, reserved: 0x0, length: 19  
VID Next payload: NOTIFY, reserved: 0x0, length: 21  
NOTIFY(NAT\_DETECTION\_SOURCE\_IP) Next payload: NOTIFY, reserved: 0x0, length: 28  
    Security protocol id: Unknown - 0, spi size: 0, type: NAT\_DETECTION\_SOURCE\_IP  
NOTIFY(NAT\_DETECTION\_DESTINATION\_IP) Next payload: NONE, reserved: 0x0, length: 28  
    Security protocol id: Unknown - 0, spi size: 0, type: NAT\_DETECTION\_DESTINATION\_IP  
  
\*Jul 16 06:01:45.375: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: INIT\_DONE Event: EV\_DONE  
\*Jul 16 06:01:45.375: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Cisco DeleteReason Notify is  
enabled  
\*Jul 16 06:01:45.375: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: INIT\_DONE Event:  
EV\_CHK4\_ROLE  
\*Jul 16 06:01:45.375: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: INIT\_DONE Event:  
EV\_START\_TMR  
\*Jul 16 06:01:45.375: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 0 CurState: R\_WAIT\_AUTH Event:  
EV\_NO\_EVENT



\*Jul 16 06:01:45.375: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):New ikev2 sa request admitted  
\*Jul 16 06:01:45.375: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Incrementing outgoing negotiating sa count by one

\*Jul 16 06:01:45.390: **IKEv2-INTERNAL:Got a packet from dispatcher**  
\*Jul 16 06:01:45.390: **IKEv2-INTERNAL:Processing an item off the pak queue**

\*Jul 16 06:01:45.375: **IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Next payload: ENCR, version: 2.0**  
**Exchange type: IKE\_AUTH, flags: INITIATOR** Message id: 1, length: 556  
**Payload contents:**  
\*Jul 16 06:01:45.375: IKEv2-INTERNAL:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDi, reserved: 0x0, length: 20  
Payload contents:  
IDi Next payload: AUTH, reserved: 0x0, length: 12  
  Id type: IPv4 address, Reserved: 0x0 0x0  
AUTH Next payload: CFG, reserved: 0x0, length: 72  
  Auth method PSK, reserved: 0x0, reserved 0x0  
CFG Next payload: SA, reserved: 0x0, length: 304  
  cfg type: CFG\_REQUEST, reserved: 0x0, reserved: 0x0  
  SA Next payload: TSi, reserved: 0x0, length: 44  
    last proposal: 0x0, reserved: 0x0, length: 40  
Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3   last transform: 0x3, reserved: 0x0:  
length: 12  
  type: 1, reserved: 0x0, id: AES-CBC  
  last transform: 0x3, reserved: 0x0: length: 8  
  type: 3, reserved: 0x0, id: SHA96  
  last transform: 0x0, reserved: 0x0: length: 8  
  type: 5, reserved: 0x0, id: Don't use ESN  
TSi Next payload: TSr, reserved: 0x0, length: 24  
  Num of TSs: 1, reserved 0x0, reserved 0x0  
  TS type: TS\_IPV4\_ADDR\_RANGE, proto id: 47, length: 16  
  start port: 0, end port: 65535  
  start addr: 192.168.1.1, end addr: 192.168.1.1  
TSr Next payload: NOTIFY, reserved: 0x0, length: 24  
  Num of TSs: 1, reserved 0x0, reserved 0x0  
  TS type: TS\_IPV4\_ADDR\_RANGE, proto id: 47, length: 16  
  start port: 0, end port: 65535  
  start addr: 192.168.2.1, end addr: 192.168.2.1

\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
**EV\_RECV\_AUTH**  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
EV\_CHK\_NAT\_T  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
EV\_PROC\_ID  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Received valid parameteres in process id  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
EV\_CHK\_IF\_PEER\_CERT\_NEEDS\_TO\_BE\_FETCHED\_FOR\_PROF\_SEL  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
EV\_GET\_POLICY\_BY\_PEERID  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
EV\_SET\_POLICY  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Setting configured policies  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
EV\_VERIFY\_POLICY\_BY\_PEERID  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:

I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
EV\_CHK\_AUTH4EAP  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_WAIT\_AUTH Event:  
EV\_CHK\_POLREQEAP  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_CHK\_AUTH\_TYPE  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_GET\_PRESHR\_KEY  
\*Jul 16 06:01:45.463: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
**EV\_VERIFY\_AUTH**  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_CHK4\_IC  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_CHK\_REDIRECT  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Redirect check is not needed,  
skipping it  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_NOTIFY\_AUTH\_DONE  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:AAA group authorization is not configured  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:AAA user authorization is not configured  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_CHK\_CONFIG\_MODE  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_SET\_REC'D\_CONFIG\_MODE  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:Received config data from toolkit:  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_CHK\_GKM  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_CHK\_DIKE  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_PROC\_SA\_TS  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_NO\_EVENT  
\*Jul 16 06:01:45.467: IPSEC(ipsec\_get\_crypto\_session\_id): Invalid Payload Id  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:IPSEC accepted group 0  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_POLICY\_NEGOTIATED  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):Action: Action\_Null  
\*Jul 16 06:01:45.467: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_VERIFY\_AUTH Event:  
EV\_GET\_CONFIG\_MODE  
\*Jul 16 06:01:45.471: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_BLD\_AUTH Event:  
EV\_MY\_AUTH\_METHOD  
\*Jul 16 06:01:45.471: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_BLD\_AUTH Event:  
EV\_GET\_PRESHR\_KEY  
\*Jul 16 06:01:45.471: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:  
I\_SPI=AA81AF8C052B480F R\_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R\_BLD\_AUTH Event:  
**EV\_GEN\_AUTH**

```

*Jul 16 06:01:45.471: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R_BLD_AUTH Event:
EV_CHK4_SIGN
*Jul 16 06:01:45.471: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R_BLD_AUTH Event:
EV_OK_AUTH_GEN
*Jul 16 06:01:45.471: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: R_BLD_AUTH Event:
EV_SEND_AUTH
*Jul 16 06:01:45.471: IKEv2-INTERNAL:Construct Vendor Specific Payload: CISCO-GRANITE
*Jul 16 06:01:45.471: IKEv2-INTERNAL:Construct Notify Payload: USE_TRANSPORT_MODE
*Jul 16 06:01:45.471: IKEv2-INTERNAL:Construct Notify Payload: SET_WINDOW_SIZE
*Jul 16 06:01:45.471: IKEv2-INTERNAL:Construct Notify Payload: ESP_TFC_NO_SUPPORT
*Jul 16 06:01:45.471: IKEv2-INTERNAL:Construct Notify Payload: NON_FIRST_FRAGS

*Jul 16 06:01:45.471: IKEv2-PAK:(SESSION ID = 4,SA ID = 1):Next payload: ENCR, version: 2.0
Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 320
Payload contents:
VID Next payload: IDr, reserved: 0x0, length: 20
IDr Next payload: AUTH, reserved: 0x0, length: 12
    Id type: IPv4 address, Reserved: 0x0 0x0
AUTH Next payload: SA, reserved: 0x0, length: 72
    Auth method PSK, reserved: 0x0, reserved 0x0
SA Next payload: TSi, reserved: 0x0, length: 44
    last proposal: 0x0, reserved: 0x0, length: 40
    Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3    last transform: 0x3, reserved: 0x0:
length: 12
    type: 1, reserved: 0x0, id: AES-CBC
    last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA96
    last transform: 0x0, reserved: 0x0: length: 8
    type: 5, reserved: 0x0, id: Don't use ESN
TSi Next payload: TSr, reserved: 0x0, length: 24
    Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 47, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.1.1, end addr: 192.168.1.1
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
    Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 47, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.2.1, end addr: 192.168.2.1
NOTIFY(USE_TRANSPORT_MODE) Next payload: NOTIFY, reserved: 0x0, length: 8
    Security protocol id: Unknown - 0, spi size: 0, type: USE_TRANSPORT_MODE
NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
    Security protocol id: Unknown - 0, spi size: 0, type: SET_WINDOW_SIZE
NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
    Security protocol id: Unknown - 0, spi size: 0, type: ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
    Security protocol id: Unknown - 0, spi size: 0, type: NON_FIRST_FRAGS

ENCR Next payload: VID, reserved: 0x0, length: 292
*Jul 16 06:01:45.479: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: AUTH_DONE Event:
EV_CHECK_DUPE
*Jul 16 06:01:45.479: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: AUTH_DONE Event:
EV_CHK4_ROLE
*Jul 16 06:01:45.479: IKEv2-INTERNAL:(SESSION ID = 4,SA ID = 1):SM Trace-> SA:
I_SPI=AA81AF8C052B480F R_SPI=53457A4ACA42FD10 (R) MsgID = 1 CurState: READY Event: EV_R_OK

```

## 참조

<https://community.cisco.com/t5/security-documents/vrf-aware-ipsec-cheat-sheet/ta-p/3109449>  
[https://www.cisco.com/c/en/us/td/docs/ios/sec\\_secure\\_connectivity/configuration/guide/convert/sec\\_ike\\_for\\_ipsec\\_vpns\\_15\\_1\\_book/sec\\_vrf\\_aware\\_ipsec.html](https://www.cisco.com/c/en/us/td/docs/ios/sec_secure_connectivity/configuration/guide/convert/sec_ike_for_ipsec_vpns_15_1_book/sec_vrf_aware_ipsec.html)  
[https://www.cisco.com/c/en/us/td/docs/ios/sec\\_secure\\_connectivity/configuration/guide/convert/sec\\_ike\\_for\\_ipsec\\_vpns\\_15\\_1\\_book/sec\\_cfg\\_ikev2.html](https://www.cisco.com/c/en/us/td/docs/ios/sec_secure_connectivity/configuration/guide/convert/sec_ike_for_ipsec_vpns_15_1_book/sec_cfg_ikev2.html)  
[https://www.cisco.com/en/US/docs/ios-xml/ios/sec\\_conn\\_ikevpn/configuration/15-1mt/Configuring\\_Internet\\_Key\\_Exchange\\_Version\\_2.html](https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-1mt/Configuring_Internet_Key_Exchange_Version_2.html)