SVTIv2 VRF configureren

Inhoud

Inleiding

Dit document biedt een configuratievoorbeeld voor het instellen van een VRF-bewust Virtual Routing and Forwarding (Virtual Routing and Forwarding) op basis van Static Virtual Tunnel Interfaces (SVTI) tussen twee VPN-peers (Virtual Private Network) door gebruik te maken van het protocol Internet Key Exchange versie 2 (IKEv2). Deze instelling omvat een IVRF waarvan het lokale net deel uitmaakt van en een Voorste Deur VRF (FVRF) waar de tunnelvestiging plaatsvindt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van IOS CLI-configuratie
- Grondkennis van IKEv2 en IPSEC

Gebruikte componenten

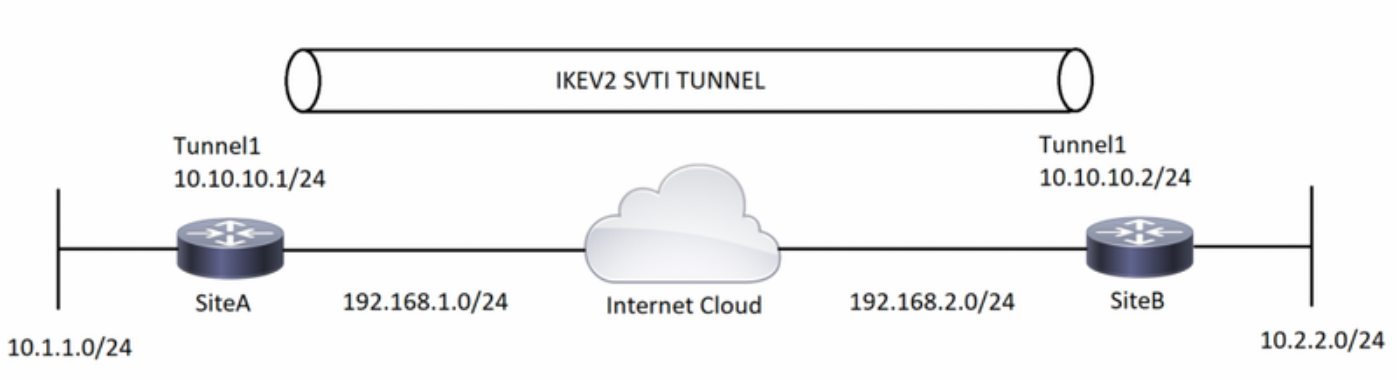
De informatie in dit document is gebaseerd op een Cisco IOS 2900 Series router met Cisco IOS® softwarerelease 15.7.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk in productie is, zorg ervoor dat u de potentiële impact van om het even welke opdracht begrijpt.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Netwerkdiagram



Achtergrondinformatie

VRF-bewuste tunnels worden gebruikt om clientnetwerken aan te sluiten die worden gescheiden door andere onvertrouwde kernnetwerken, of kernnetwerken met verschillende infrastructuur. Met deze instelling kunnen elke bron en bestemming van een tunnel worden geconfigureerd om tot een VRF-tabel te behoren.

Op een tunnelinterface, wordt "vrf forend" opdracht gebruikt om de tunnelinterface in die bepaalde routingtabel te plaatsen. Met het opdracht "tunnel vrf" is de router geïnstrueerd om de gespecificeerde VRF's routingtabel voor de tunnelbron en de IP-adressen van de bestemming te gebruiken.

In het voorbeeld dat voor dit document wordt gebruikt, is de loopback interface VRF net als een LAN-segment VRF. Packets die door deze interface worden ingevoerd, worden met deze VRF routeerd. Packets die de tunnel verlaten, worden naar deze VRF verzonden.

De VRF die op de tunnel wordt gevormd die de "tunnel vrf" opdracht gebruikt is het vervoer VRF. Het is de VRF die op de ingekapselde lading van toepassing is en gebruikt wordt om de tunneleindpunten op te zoeken. Deze VRF is het zelfde als VRF verbonden met de fysieke interface waarover de tunnel pakketten verstuurt.

Configuratie

Stap 1. Bepaal de VRF's. In dit voorbeeld, worden twee VRF's bepaald genoemd "lokaal" en "internet" respectievelijk voor LAN- en WAN-interfaces.

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
```

Stap 2. Configureer de parameters die vereist zijn om een IKEv2-tunnel op te zetten, te beginnen met de creatie van het IKEv2-voorstel en de sleutelring. Vervolgens wordt het IKEv2-profiel geconfigureerd waar de crypto-sleutelring wordt opgeroepen en om te sluiten met de crypto-configuratie, het IPSEC-profiel te configureren omvat de IPSEC-transformatie-set en het IKEv2-profiel.

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 fvrf 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 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
```

Stap 3. Configureer de gewenste interfaces. In dit voorbeeld, is de loopback interface deel van "lokaal" VRF en treedt als interessant verkeer op. De fysieke interface, een deel van "internet" VRF, is de WAN-interface die met ISP is verbonden. De tunnelinterface is de GRE-insluiting te activeren die versleuteld is met IPSEC.

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
```

Stap 4: Configureer de VRF-specifieke routes. In deze instelling wordt een route in "internet" VRF geconfigureerd als standaardroute naar volgende hop van de fysieke interface (of ISP in echte omgevingen). De tweede route in "lokaal" VRF is voor afstandsbediening van VPN die op tunnelinterface wijst wat uiteindelijk het verkeer door de tunnelinterface maakt en VPN teweegbrengt.

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
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

De Cisco CLI Analyzer ondersteunt bepaalde showopdrachten. Gebruik de Cisco CLI Analyzer om een analyse van de uitvoer van het tonen bevel te bekijken.

SiteA :

```
SiteA#show crypto ikev2 sa
IPv4 Crypto IKEv2  SA

            Tunnel-id Local                 Remote                fvrf/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: Tunnel1
    Crypto map tag: Tunnel1-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 (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 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 (recv) 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: Tunnel1-
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: Tunnel1-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: Tunnel1
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: Tunnel1
    Crypto map tag: Tunnel1-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 (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 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 (recv) 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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. Ook wordt een voorbeelduitvoer van debug-uitvoer weergegeven.

Opdrachten voor probleemoplossing

Opmerking: raadpleeg Belangrijke informatie over debug Commands voordat u debug-opdrachten gebruikt. Als er meerdere tunnels zijn ingesteld op de router, kunt u de volgende conditie gebruiken:

- **Debug crypto ikev2 interne**
- **Debug crypto ikev2-pakket**

Voorbeeld van output van foutopsporing

```
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_RECD_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_RECD_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: READYEvent:
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: l    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_SPI53457A4ACA42FD10 (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_RECD_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_RECD_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_RECD_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
```

Referenties

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_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