Probleemoplossing voor IOS IKEv2-debugs voor site-to-site VPN met PSKâ€™s

Inhoud

Inleiding

Dit document beschrijft debuggen van Internet Key Exchange versie 2 (IKEv2) op Cisco IOS® wanneer een niet-gedeelde sleutel (PSK) wordt gebruikt.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de pakketuitwisseling voor IKEv2. Raadpleeg IKEv2 Packet Exchange en Protocolniveau debuggen voor meer informatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Internet Key Exchange, versie 2 (IKEv2)
- Cisco IOS 15.1(1)T of hoger

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 live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Dit document bevat informatie over de manier waarop bepaalde debug-regels in een configuratie moeten worden vertaald.

Belangrijkste probleem

De pakketuitwisseling in IKEv2 verschilt sterk van pakketuitwisseling in IKEv1. In IKEv1 was er een duidelijk afgebakende fase1-uitwisseling die bestond uit zes (6) pakketten met een fase 2-uitwisseling daarna die bestond uit drie (3) pakketten; de IKEv2-uitwisseling is variabel. Zie IKEv2 Packet Exchange en Protocol Level Debugging voor meer informatie over de verschillen en een uitleg van de pakketuitwisseling.

Routerconfiguratie

In deze sectie worden de configuraties weergegeven die in dit document worden gebruikt.

Router 1

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy site-pol
 proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
 peer peer1
  address 10.0.0.2 255.255.255.0
  hostname host1
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
```

```
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

Router 2

```
crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 keyring KEYRNG
 peer peer2
  address 10.0.0.1 255.255.255.0
  hostname host2
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.102 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

Problemen oplossen

Routerdebugs

Deze debug-opdrachten worden in dit document gebruikt:

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Router 1 (Initiator) Berichtbeschrijving	**Debugs**
Router 1 ontvangt een pakket dat overeenkomt met de crypto-oproep voor peer ASA 10.0.0.2. Initieert SA-creatie	*Nov 11 20:28:34.003: IKEv2:Got a packet from dispatcher *11 nov 20:28:34.003: IKEv2:Een item uit de piekwachtrij verwerken *Nov 11 19:30:34.811: IKEv2:% krijgen preshared sleutel op adres 10.0.0.2 *Nov 11 19:30:34.811: IKEv2:Voorstel PHASE1-prop aan toolkit-beleid toevoegen *11 nov 19:30:34.811: IKEv2:(1): Kies IKE-profiel IKEV2-SETUP *11 nov 19:30:34.811: IKEv2:New ikev2 als verzoek aanvaard *11 nov 19:30:34.811: IKEv2:Uitgaande onderhandelingen verhogen als tellen door één
Het eerste paar berichten is de IKE_SA_INIT uitwisseling. Deze berichten onderhandelen met cryptografische algoritmen, ruilen nonces uit en doen een Diffie-Hellman-uitwisseling. **Relevante configuratie:** `crypto ikev2 voorstel PHASE1-prop encryptie 3des aes-cbc-128 integriteit sha1 groep 2crypto ikev2 keyring KEYRING peer1-adres 10.0.0.2 255.255.255.0 hostname host1 pre-shared-key lokale Cisco pre-shared-key externe cisco`	*Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: IDLE Event: EV_INIT_SA *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_IKE_POLICY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event:**EV_SET_POLICY** *11 nov 19:30:34.811: IKEv2:(SA-id = 1):Geselecteerd beleid instellen *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_CHK_AUTH4PKI *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event:**EV_GEN_DH_KEY** *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_NO_EVENT *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_OK_RECD_DH_PUBKEY_RESP *11 nov 19:30:34.811: IKEv2:(SA ID = 1):Actie: Action_Null *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_CONFIG_MODE_MODE *Nov 11 19:30:34.811: IKEv2:IKEv2 initiator - geen configuratiegegevens om IKE_SA_INIT exch in te sturen *Nov 11 19:30:34.811: IKEv2:Geen configuratiegegevens te verzenden naar toolkit: *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_BLD_MSG *Nov 11 19:30:34.811: IKEv2:Construct Verkoper specifieke payload: Delete-ratio *Nov 11 19:30:34.811: IKEv2:Construct Vendor Specific Payload: (aangepast) *Nov 11 19:30:34.811: IKEv2:Construct Melden payload: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.811: IKEv2:Construct Melden payload: NAT_DETECTION_DESTINY_I

Initiator bouwt IKE_INIT_SA pakket. Het bevat: ISAKMP-header (SPI/version/flags), SAi1 (cryptografisch algoritme dat IKE-initiator ondersteunt), KEi (DH openbare toetswaarde van de initiator) en N (Initiator Nonce).	*Nov 11 19:30:34.811: **IKEv2:(SA ID = 1)**:Volgende lading: SA, versie: 2.0 Type uitwisseli **IKE_SA_INIT,** vlaggen: **INITIATOR** Bericht ID: 0, lengte: 344 Inhoud payload: **SA** Volgende payload: KE, gereserveerd: 0x0, lengte: 56 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 52 Voorstel: 1, Protocol id: IKE, SPI grootte: 0, #trans: 5 laatste transformatie: 0x3, gereserveer 0x0: lengte: 8 type: 1, gereserveerd: 0x0, id: 3DES laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA1 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1024_MODP/groep 2 **KE** Volgende payload: N, gereserveerd: 0x0, lengte: 136 DH groep: 2, Gereserveerd: 0x0 N Volgende payload: VID, gereserveerd: 0x0, lengte: 24 VID Volgende payload: VID, gereserveerd: 0x0, lengte: 23 VID Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 21 MELDEN(NAT_DETECTION_SOURCE_IP) Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 28 Security protocol-id: IKE, spi-grootte: 0, type: NAT_DETECTION_SOURCE_IP MELDEN(NAT_DETECTION_DESTY_IP) Volgende payload: NONE, gereserveerd: 0x0, lengte: 28 Security protocol-id: IKE, spi-grootte: 0, type: NAT_DETECTION_DESTINY_IP
	----------Initiator verzonden IKE_INIT_SA ---------->
	*Nov 11 19:30:34.814: IKEv2:Krijg een pakket van verzender *11 nov 19:30:34.814: IKEv2:Een item uit de piekwachtrij verwerken *11 nov 19:30:34.814: IKEv2:New ikev2 als verzoek aanvaard *11 nov 19:30:34.814: IKEv2:Inkomende onderhandelingen verhogen als tellen door één
	*Nov 11 19:30:34.814: IKEv2:Volgende payload: SA, versie: 2.0 Exchange type: IKE_SA_INIT, vlaggen: INITIATOR Message id: 0, lengte: 344 Inhoud payload: SA Volgende payload: KE, gereserveerd: 0x0, lengte: 56 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 52 Voorstel: 1, Protocol id: IKE, SPI grootte: 0, #trans: 5 laatste transformatie: 0x3, gereserveer 0x0: lengte: 8 type: 1, gereserveerd: 0x0, id: 3DES laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA1 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1024_MODP/groep 2 KE Volgende payload: N, gereserveerd: 0x0, lengte: 136 DH groep: 2, Gereserveerd: 0x0

	N Volgende payload: VID, gereserveerd: 0x0, lengte: 24 *Nov 11 19:30:34.814: IKEv2:Parse Leverancier-specifieke payload: Cisco-Delete-REDENS VID Volgende payload: VID, gereserveerd: 0x0, lengte: 23 *Nov 11 19:30:34.814: IKEv2:Parse Leverancier Specifieke payload: (AANGEPAST) VID Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 21 *Nov 11 19:30:34.814: IKEv2:Parse Notify payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Volgende payload: NOTIFY, gereserveerd: 0x0 lengte: 28 Security protocol-id: IKE, spi-grootte: 0, type: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.814: IKEv2:Parse Notify payload: NAT_DETECTION_DESTINATION_I NOTIFY(NAT_DETECTION_DESTINY_IP) Volgende payload: NONE, gereserveerd: 0x0, lengte: 28 Security protocol-id: IKE, spi-grootte: 0, type: NAT_DETECTION_DESTINY_IP
	*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: IDLE Event:**EV_RECV_INIT** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:**EV_VERIFY_MSG** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:**EV_INSERT_SA** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:**EV_GET_IKE_POLICY** *Nov 11 19:30:34.814: IKEv2:Toevoeging van voorstel standaard aan toolkit beleid *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:**EV_PROC_MSG** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event: EV_DEdetect_NAT *11 nov 19:30:34.814: IKEv2:(SA-id = 1):NAT-detectie van proces melden *11 nov 19:30:34.814: IKEv2:(SA ID = 1):Verwerking nat detecteren src aanmelden *11 nov 19:30:34.814: IKEv2:(SA-id = 1):Afstandsadres afgestemd *11 nov 19:30:34.814: IKEv2:(SA ID = 1):Verwerking nat detecteren dst aanmelden *11 nov 19:30:34.814: IKEv2:(SA ID = 1):Lokaal adres gekoppeld *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Geen NAT gevonden *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event: EV_CHK_CONFIG_MODE *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_SET_POLICY *nov 11 19:30:34.814: IKEv2:(SA-id = 1):**Instellen van geconfigureerd beleid** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_CHK_AUTH4PKI *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:

	EV_PKI_SESH_OPEN *11 nov 19:30:34.814: IKEv2:(SA ID = 1):Een PKI-sessie openen *Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:**EV_GEN_DH_KEY** *Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_NO_EVENT *Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:**EV_OK_RECD_DH_PUBKEY_RESP** *11 nov 19:30:34.815: IKEv2:(SA ID = 1):Actie: Action_Null *Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:**EV_GEN_DH_SECRET** *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_NO_EVENT *Nov 11 19:30:34.822: IKEv2:% **Vooraf gedeelde sleutel op adres 10.0.0.1** *Nov 11 19:30:34.822: IKEv2:Toevoeging van voorstel standaard aan toolkit beleid *11 nov 19:30:34.822: IKEv2:(2): Kies IKE-profiel IKEV2-SETUP *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_OK_RECD_DH_SECRET_RESP *11 nov 19:30:34.822: IKEv2:(SA ID = 1):Actie: Action_Null *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:**EV_GEN_SKEYID** *nov 11 19:30:34.822: IKEv2:(SA-id = 1):**Generate skeyid** *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_GET_CONFIG_MODE_MODE *Nov 11 19:30:34.822: IKEv2:IKEv2 responder - geen configuratiegegevens om IKE_SA_IN exch in te sturen *Nov 11 19:30:34.822: IKEv2:Geen configuratiegegevens te verzenden naar toolkit: *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_BLD_MSG *Nov 11 19:30:34.822: IKEv2:Construct Verkoper specifieke payload: Delete-ratio *Nov 11 19:30:34.822: IKEv2:Construct Vendor Specific Payload: (aangepast) *Nov 11 19:30:34.822: IKEv2:Construct Melden payload: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.822: IKEv2:Construct Melden payload: NAT_DETECTION_DESTINY_I *Nov 11 19:30:34.822: IKEv2:Construct Melden payload: HTTP_CERT_LOOKUP_SUPPO
	*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Volgende payload: SA, versie: 2.0 Wisseltype: **IKE_SA_INIT,** vlaggen: **RESPONDER MSG-RESPONSE** Bericht: 0, lengte: 449 Inhoud payload: **SA** Volgende payload: KE, gereserveerd: 0x0, lengte: 48 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 44 Voorstel: 1, Protocol id: IKE, SPI grootte: 0, #trans: 4 laatste transformatie: 0x3, gereserveer 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC

	laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA1 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1024_MODP/groep 2 **KE** Volgende payload: N, gereserveerd: 0x0, lengte: 136 DH groep: 2, Gereserveerd: 0x0 **N** Volgende payload: VID, gereserveerd: 0x0, lengte: 24 VID Volgende payload: VID, gereserveerd: 0x0, lengte: 23 VID Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 21 MELDEN(NAT_DETECTION_SOURCE_IP) Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 28 Security protocol-id: IKE, spi-grootte: 0, type: NAT_DETECTION_SOURCE_IP MELDEN(NAT_DETECTION_DESTY_IP) Volgende payload: CERTREQ, gereserveerd: 0x0, lengte: 28 Security protocol-id: IKE, spi-grootte: 0, type: NAT_DETECTION_DESTINY_IP CERTREQ Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 105 Snelcodering Hash en URL van PKIX MELDEN(HTTP_CERT_LOOKUP_SUPPORT) Volgende payload: NONE, gereserveerd: 0x0, lengte: 8 Security protocol-id: IKE, spi-grootte: 0, type: HTTP_CERT_LOOKUP_SUPPORT
	*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_done Event: EV_DON_DON *11 nov 19:30:34.822: IKEv2:(SA-id = 1):Cisco DeleteReason Notify is ingeschakeld *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DID Event: EV_CHK4_ROL *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DID Event:**EV_START_TMR.** *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_wait_AUTH Event: EV_NO_EVENT *11 nov 19:30:34.822: IKEv2:**Nieuw ikev2 op verzoek toegelaten** *11 nov 19:30:34.822: IKEv2: **Verhoging van uitgaande onderhandelingen als tellen door één**

<----------Responder verstuurd door IKE_INIT_SA ----------

Router 1 ontvangt het IKE_SA_INIT reactiepakket van router 2.	*Nov 11 19:30:34.823: IKEv2:Krijg een pakket van verzender *Nov 11 19:30:34.823: IKEv2:Krijg een pakket van verzender *11 nov 19:30:34.823: IKEv2:Een item uit de piekwachtrij verwerken	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R MsgID = 00000000 CurState: INIT_DID Event:**EV_START_TMR.**

Router1 verifieert en verwerkt de reactie: (1) de initiator DH geheime sleutel wordt gegevens verwerkt, en (2) initiator skeyid wordt ook geproduceerd.	*Nov 11 19:30:34.823: IKEv2:(SA ID = 1):Volgende payload: SA, versie: 2.0 Wisseltype: IKE_SA_INIT, vlaggen: **RESPONDER MSG-RESPONSE** Bericht id: 0, lengte: 449 Inhoud payload: **SA** Volgende payload: KE, gereserveerd: 0x0, lengte: 48 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 44 Voorstel: 1, Protocol id: IKE, SPI grootte: 0, #trans: 4 laatste transformatie: 0x3, gereserveer 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA1 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1024_MODP/groep 2 **KE** Volgende payload: N, gereserveerd: 0x0, lengte: 136 DH groep: 2, Gereserveerd: 0x0 **N** Volgende payload: VID, gereserveerd: 0x0, lengte: 24 *Nov 11 19:30:34.823: IKEv2:Parse Leverancier-specifieke payload: Cisco-Delete-Why VID Volgende payload: VID, gereserveerd: 0x0, lengte: 23 *Nov 11 19:30:34.823: IKEv2:Parse Leverancier Specifieke payload: (AANGEPAST) VID Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 21 *Nov 11 19:30:34.823: IKEv2:Parse Notify payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Volgende payload: NOTIFY, gereserveerd: 0x0 lengte: 28 Security protocol-id: IKE, spi-grootte: 0, type: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.824: IKEv2:Parse Notify payload: NAT_DETECTION_TARGET_IP NOTIFY(NAT_DETECTION_DESTY_IP) Volgende payload: CERTREQ, gereserveerd: 0x0 lengte: 28 Security protocol-id: IKE, spi-grootte: 0, type: NAT_DETECTION_DESTINY_IP CERTREQ Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 105 Snelcodering Hash en URL van PKIX *Nov 11 19:30:34.824: IKEv2:Parse Notify payload: HTTP_CERT_LOOKUP_SUPPORT NOTIFY(HTTP_CERT_LOOKUP_SUPPORT) Volgende payload: NONE, gereserveerd: 0x0 lengte: 8 Security protocol-id: IKE, spi-grootte: 0, type: HTTP_CERT_LOOKUP_SUPPORT *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_wait_INIT Gebeurtenis: EV_RECV_INIT *11 nov 19:30:34.824: IKEv2:(SA ID = 1):Verwerking IKE_SA_INIT bericht *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_CHK4_NOTIFY *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_VERIFY_MSG *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event:

	EV_PROC_MSG *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_DEdetect_NAT *11 nov 19:30:34.824: IKEv2:(SA-id = 1):NAT-detectie van proces melden *11 nov 19:30:34.824: IKEv2:(SA ID = 1):Verwerking nat detecteren src aanmelden *11 nov 19:30:34.824: IKEv2:(SA-id = 1):Afstandsadres afgestemd *11 nov 19:30:34.824: IKEv2:(SA ID = 1):Verwerking nat detecteren dst aanmelden *11 nov 19:30:34.824: IKEv2:(SA ID = 1):Lokaal adres gekoppeld *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Geen NAT gevonden *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_CHK_NAT_T *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_CHK_CONFIG_MODE *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DID Event:**EV_GEN_DH_SECRET** *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_done Event: EV_NO_EVENT *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DID Event: EV_OK_RECD_DH_SECRET_RESP *11 nov 19:30:34.831: IKEv2:(SA ID = 1):Actie: Action_Null *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DID Event:**EV_GEN_SKEYID** *nov 11 19:30:34.831: IKEv2:(SA-id = 1):**Generate skeyid** *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_done Event: EV_DON_DON *11 nov 19:30:34.831: IKEv2:(SA-id = 1):Cisco DeleteReason Notify is ingeschakeld *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DID Event: EV_CHK4_ROL *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_GET_CONFIG_MODE_MODE *Nov 11 19:30:34.831: IKEv2:Config-gegevens naar toolkit verzenden *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_CHK_EAP
Initiator start IKE_AUTH-uitwisseling en genereert de payload van de authenticatie. Het IKE_AUTH-pakket bevat:	*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event:**EV_GEN_AUTH** *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_CHK_AUTH_TYPE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B

ISAKMP-header (SPI/versie/vlaggen), IDi (initiator-identiteit), AUTH-payload, SAi2 (initieert de SA-soortgelijk aan de fase 2 transformatie-set-uitwisseling in IKEv1), en TSi en TSr (Initiator en Responder Traffic selectors). Ze bevatten het bron- en doeladres van de initiator en de responder voor respectievelijk het doorsturen en ontvangen van versleuteld verkeer. Het adresbereik specificeert dat al het verkeer naar en van dat bereik wordt getunneld. Als het voorstel acceptabel is voor de respondent, stuurt het identieke TS-payloads terug. Het eerste CHILD_SA wordt aangemaakt voor het proxy_ID-paar dat overeenkomt met het trigger-pakket. **Relevante configuratie:** `crypto ipsec transformatie-set TS esp-3des esp-sha-hmac crypto ipsec profiel phse2-prof set transformatie-set TS set ikev2-profiel IKEV2-SETUP`	R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_OK_AUTH_GEN *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_SEND_AUTH *Nov 11 19:30:34.831: IKEv2:Construct Vendor Specific Payload: Cisco-GRANITE *Nov 11 19:30:34.831: IKEv2:Construct Melden payload: initial_CONTACT *Nov 11 19:30:34.831: IKEv2:Construct Melden payload: SET_VENSTER_SIZE *Nov 11 19:30:34.831: IKEv2:Construct Melden payload: ESP_TFC_NO_SUPPORT *Nov 11 19:30:34.831: IKEv2:Construct Melden payload: NON_FIRST_FRAGS **Inhoud payload:** VID Volgende payload: IDi, gereserveerd: 0x0, lengte: 20 **IDi** Volgende payload: AUTH, gereserveerd: 0x0, lengte: 12 Type ID: IPv4 adres, gereserveerd: 0x0 0x0 **AUTH** Volgende payload: CFG, gereserveerd: 0x0, lengte: 28 Automatische methode PSK, gereserveerd: 0x0, gereserveerd 0x0 **CFG** Volgende payload: SA, gereserveerd: 0x0, lengte: 309 cfg type: CFG_REQUEST, gereserveerd: 0x0, gereserveerd: 0x0 *nov 11 19:30:34.831: SA Volgende lading: **TSi**, gereserveerd: 0x0, lengte: 40 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 36 Voorstel: 1, Protocol id: ESP, SPI grootte: 4, #trans: 3 laatste transformatie: 0x3, gereserveerd 0x0: lengte: 8 type: 1, gereserveerd: 0x0, id: 3DES laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 5, gereserveerd: 0x0, id: Niet gebruiken **TSi** Volgende payload: TSr, gereserveerd: 0x0, lengte: 24 Aantal TS'en: 1, gereserveerd 0x0, gereserveerd 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, lengte: 16 beginhaven: 0, eindhaven: 65535 begindatum: 0.0.0.0, einddatum: 255.255.255.255.255 **TSr** Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 24 Aantal TS'en: 1, gereserveerd 0x0, gereserveerd 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, lengte: 16 beginhaven: 0, eindhaven: 65535 begindatum: 0.0.0.0, einddatum: 255.255.255.255.255 MELDEN(INITIËLE_CONTACT) Volgende payload: MELDEN, gereserveerd: 0x0, lengte: Beveiligingsprotocol-id: IKE, spi-grootte: 0, type: INITIAL_CONTACT MELDEN(SET_VENSTER_SIZE) Volgende payload: MELDEN, gereserveerd: 0x0, lengte: Security protocol-id: IKE, spi size: 0, type: SET_VENSTER_SIZE MELDEN(ESP_TFC_NO_SUPPORT) Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 8 Security protocol-id: IKE, spi size: 0, type: ESP_TFC_NO_SUPPORT MELDEN(NON_FIRST_FRAGS) Volgende payload: NONE, gereserveerd: 0x0, lengte: 8 Beveiligingsprotocol-id: IKE, spi-grootte: 0, type: NON_FIRST_FRAGS *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Volgende lading: ENCR, versie: 2.0 Wisseltype: **IKE_AUTH**, vlaggen: **INITIATOR** Bericht ID: 1, lengte: 556 Inhoud payload: ENCR Volgende payload: VID, gereserveerd: 0x0, lengte: 528

	*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 **CurStaat: I_wait_AUTH** Gebeurtenis: EV_NO_EVENT
	----------Initiator verzonden IKE_AUTH ----------
	*Nov 11 19:30:34.832: IKEv2:Krijg een pakket van verzender *11 nov 19:30:34.832: IKEv2:Een item uit de piekwachtrij verwerken *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Verzoek heeft mess_id 1; verwacht 1 tot 1 *Nov 11 19:30:34.832: **IKEv2:(SA ID = 1)**:Volgende lading: ENCR, versie: 2.0 Wisseltype: **IKE_AUTH**, vlaggen: **INITIATOR** Bericht ID: 1, lengte: 556 Inhoud payload: *Nov 11 19:30:34.832: IKEv2:Parse Leverancier Specifieke payload: (AANGEPAST) VID Volgende payload: IDi, gereserveerd: 0x0, lengte: 20 **IDi** Volgende payload: AUTH, gereserveerd: 0x0, lengte: 12 Type ID: IPv4 adres, gereserveerd: 0x0 0x0 **AUTH** Volgende payload: CFG, gereserveerd: 0x0, lengte: 28 Automatische methode PSK, gereserveerd: 0x0, gereserveerd 0x0 **CFG** Volgende payload: SA, gereserveerd: 0x0, lengte: 309 cfg type: CFG_REQUEST, gereserveerd: 0x0, gereserveerd: 0x0 *nov 11 19:30:34.832: attrib type: interne IP4 DNS, lengte: 0 *nov 11 19:30:34.832: attrib type: interne IP4 DNS, lengte: 0 *nov 11 19:30:34.832: attribtype: interne IP4 NBNS, lengte: 0 *nov 11 19:30:34.832: attribtype: interne IP4 NBNS, lengte: 0 *nov 11 19:30:34.832: attrib type: interne IP4-subnetnummer, lengte: 0 *nov 11 19:30:34.832: attrib type: applicatie versie, lengte: 257 attrib type: Onbekend - 28675, lengte: 0 *nov 11 19:30:34.832: attrib type: Onbekend - 28672, lengte: 0 *nov 11 19:30:34.832: attrib type: Onbekend - 28692, lengte: 0 *nov 11 19:30:34.832: attrib type: Onbekend - 28681, lengte: 0 *nov 11 19:30:34.832: attrib type: Onbekend - 28674, lengte: 0 *nov 11 19:30:34.832: **SA** Volgende lading: TSi, gereserveerd: 0x0, lengte: 40 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 36 Voorstel: 1, Protocol id: ESP, SPI grootte: 4, #trans: 3 laatste transformatie: 0x3, gereserveer 0x0: lengte: 8 type: 1, gereserveerd: 0x0, id: 3DES laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 5, gereserveerd: 0x0, id: Niet gebruiken **TSi** Volgende payload: TSr, gereserveerd: 0x0, lengte: 24 Aantal TS'en: 1, gereserveerd 0x0, gereserveerd 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, lengte: 16 beginhaven: 0, eindhaven: 65535 begindatum: 0.0.0.0, einddatum: 255.255.255.255 **TSr** Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 24 Aantal TS'en: 1, gereserveerd 0x0, gereserveerd 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, lengte: 16 beginhaven: 0, eindhaven: 65535 begindatum: 0.0.0.0, einddatum: 255.255.255.255

*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_RECV_AUTH
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_CHK_NAT_T
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_PROC_ID
*11 nov 19:30:34.832: IKEv2:(SA ID = 1):Ontvangen geldige parameters in proces-id
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_CHK_IF_PEER_CERT_needs_TO_FETCHED_FOR_FOR_PROF_SEL
*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_GET_POLICY_BY_PEERID
*11 nov 19:30:34.833: IKEv2:(1): Kies IKE-profiel IKEV2-SETUP
*Nov 11 19:30:34.833: IKEv2:% krijgen preshared sleutel op adres 10.0.0.1
*Nov 11 19:30:34.833: IKEv2:% krijgen preshared sleutel op adres 10.0.0.1
*Nov 11 19:30:34.833: IKEv2:Toevoeging van voorstel standaard aan toolkit beleid
*11 nov 19:30:34.833: IKEv2:(SA-ID = 1):Gebruik van het IKEv2-profiel 'IKEV2-SETUP'
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_SET_POLICY
*11 nov 19:30:34.833: IKEv2:(SA-id = 1):Geselecteerd beleid instellen
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_VERIFY_POLICY_BY_PEERID_PEERID
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_CHK_AUTH4EAP
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_wait_AUTH Event: EV_CHK_POLREQEAP
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Gebeurtenis: EV_CHK_AUTH_TYPE_TYPE
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Gebeurtenis: EV_GET_PRESHR_KEY
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Gebeurtenis: EV_VERIFY_AUTH
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK4_IC
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK_REDIRECT
*11 nov 19:30:34.833: IKEv2:(SA ID = 1):Redirect check is niet nodig, overslaan
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_NOTIFY_AUTH_DON_DON_DON

	*11 nov 19:30:34.833: IKEv2:AAA-groepsautorisatie is niet geconfigureerd *11 nov 19:30:34.833: IKEv2:AAA-gebruikersautorisatie is niet geconfigureerd *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK_CONFIG_MODE_MODE *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Gebeurtenis: EV_SET_RECD_CONFIG_MODE *Nov 11 19:30:34.833: IKEv2:Ontvangen configuratiegegevens van toolkit: *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_PROC_SA_TS_TS *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_GET_CONFIG_MODE_MODE_MODE *Nov 11 19:30:34.833: IKEv2:Fout bij construeren van configuratie antwoord *Nov 11 19:30:34.833: IKEv2:Geen configuratiegegevens te verzenden naar toolkit: *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_MY_AUTH_method *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_GET_PRESHR_KEY *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_GEN_AUTH *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_CHK4_TEKEN *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_OK_AUTH_GEN *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_SEND_AUTH *Nov 11 19:30:34.833: IKEv2:Construct Vendor Specific Payload: Cisco-GRANITE *Nov 11 19:30:34.833: IKEv2:Construct Melden payload: SET_VENSTER_SIZE *Nov 11 19:30:34.833: IKEv2:Construct Melden payload: ESP_TFC_NO_SUPPORT *Nov 11 19:30:34.833: IKEv2:Construct Melden payload: NON_FIRST_FRAGS
	*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Volgende lading: ENCR, versie: 2.0 Wisseltype: **IKE_AUTH**, vlaggen: **RESPONDER MSG-RESPONSE** Bericht ID: 1, lengte: 252 Inhoud payload: **ENCR** Volgende payload: VID, gereserveerd: 0x0, lengte: 224 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DID Event: EV_OK *11 nov 19:30:34.833: IKEv2:(SA ID = 1):Actie: Action_Null *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DID Event: EV_PKI_SESH_CLOSE *11 nov 19:30:34.833: IKEv2:(SA-id = 1):De PKI-sessie sluiten *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B

	R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DID Event: EV_UPDATE_CAC_STATS *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DID Event:**EV_INSERT_IKE** *11 nov 19:30:34.834: IKEv2:Store mib index ikev2 1, platform 60 *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DON Event: EV_GEN_LOAD_IPLOAD_IPICS *11 nov 19:30:34.834: IKEv2:(SA-id = 1):Wachtrij voor asynchrone aanvragen *11 nov 19:30:34.834: IKEv2:(SA ID = 1): *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **AUTH_DON** Event: EV_NO_EVENT	
	<----------Responder verstuurd door IKE_AUTH----------	
Initiator ontvangt antwoord van Responder.	*Nov 11 19:30:34.834: IKEv2:Krijg een pakket van verzender *11 nov 19:30:34.834: IKEv2:Een item uit de piekwachtrij verwerken	*Nov 11 19:30:34.840: IKEv2:(S ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (F MsgID = 00000001 CurState: AUTH_DID Event: EV_OK_RECD_LOAD_IPSEC_ *11 nov 19:30:34.840: IKEv2:(S ID = 1):Actie: Action_Null *Nov 11 19:30:34.840: IKEv2:(S ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (F MsgID = 00000001 CurState: AUTH_DID Event: EV_START_ACCT *Nov 11 19:30:34.840: IKEv2:(S ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (F MsgID = 00000001 CurState: AUTH_DID Event: EV_CHECK_DUPE *Nov 11 19:30:34.840: IKEv2:(S ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (F MsgID = 00000001 CurState: AUTH_DID Event: EV_CHK4_ROL
Router 1 verifieert en verwerkt de verificatiegegevens in dit pakket. Router 1 voegt vervolgens	*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Volgende lading: ENCR, versie: 2.0 Wisseltype: **IKE_AUTH**, vlaggen: **RESPONDER MSG-RESPONSE** Berichtnummer: 1, lengte: 252 **Inhoud payload:**	

deze SA in in zijn SAD.	*Nov 11 19:30:34.834: IKEv2:Parse Leverancier Specifieke payload: (AANGEPAST) VID Volgende payload: IDr., gereserveerd: 0x0, lengte: 20 **IDr.** Volgende payload: AUTH, gereserveerd: 0x0, lengte: 12 Type ID: IPv4 adres, gereserveerd: 0x0 0x0 **AUTH** Volgende payload: SA, gereserveerd: 0x0, lengte: 28 Automatische methode PSK, gereserveerd: 0x0, gereserveerd 0x0 **SA** Volgende payload: TSi, gereserveerd: 0x0, lengte: 40 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 36 Voorstel: 1, Protocol id: ESP, SPI grootte: 4, #trans: 3 laatste transformatie: 0x3, gereservee 0x0: lengte: 8 type: 1, gereserveerd: 0x0, id: 3DES laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 5, gereserveerd: 0x0, id: Niet gebruiken **TSi** Volgende payload: TSr, gereserveerd: 0x0, lengte: 24 Aantal TS'en: 1, gereserveerd 0x0, gereserveerd 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, lengte: 16 beginhaven: 0, eindhaven: 65535 begindatum: 0.0.0.0, einddatum: 255.255.255.255 **TSr** Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 24 Aantal TS'en: 1, gereserveerd 0x0, gereserveerd 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, lengte: 16 beginhaven: 0, eindhaven: 65535 begindatum: 0.0.0.0, einddatum: 255.255.255.255 *Nov 11 19:30:34.834: IKEv2:Parseren Melden payload: SET_VENSTER_SIZE MELDEN(SET_VENSTER_SIZE) Volgende payload: MELDEN, gereserveerd: 0x0, lengte: Security protocol-id: IKE, spi size: 0, type: SET_VENSTER_SIZE *Nov 11 19:30:34.834: IKEv2:Parse Notify payload: ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) Volgende payload: NOTIFY, gereserveerd: 0x0, lengte Security protocol-id: IKE, spi size: 0, type: ESP_TFC_NO_SUPPORT *Nov 11 19:30:34.834: IKEv2:Parse Notify payload: NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) Volgende payload: NONE, gereserveerd: 0x0, lengte: 8 Beveiligingsprotocol-id: IKE, spi-grootte: 0, type: NON_FIRST_FRAGS *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_wait_AUTH Event:**EV_RECV_AUTH** *11 nov 19:30:34.834: IKEv2:(SA ID = 1):Actie: Action_Null *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK4_NOTIFY *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:**EV_PROC_MSG** *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_IF_PEER_CERT_needs_TO_BE_FETCHED_FOR_PROF_SEL *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:

EV_GET_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:Voorstel PHASE1-prop toevoegen aan toolkit beleid
*11 nov 19:30:34.834: IKEv2:(SA-ID = 1):Gebruik van het IKEv2-profiel 'IKEV2-SETUP'
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Gebeurteni
EV_VERIFY_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_GET_PRESHR_KEY
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:**EV_VERIFY_AUTH**
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_EAP
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:**EV_NOTIFY_AUTH_DON_DON**
*11 nov 19:30:34.835: IKEv2:AAA-groepsautorisatie is niet geconfigureerd
*Nov 11 19:30:34.835: IKEv2:AAA-gebruikersautorisatie is niet geconfigureerd
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK4_IC
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_IKE_ONLY
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_PROC_SA_TS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DID Event: EV_OK
*11 nov 19:30:34.835: IKEv2:(SA ID = 1):Actie: Action_Null
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DID Event: EV_PKI_SESH_CLOSE
*11 nov 19:30:34.835: IKEv2:(SA-id = 1):De PKI-sessie sluiten
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DID Event: EV_UPDATE_CAC_STATS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DID Event: EV_INSERT_IKE
*11 nov 19:30:34.835: IKEv2:Store mib index ikev2 1, platform 60
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DON Event: EV_GEN_LOAD_IPLOAD_IPICS
*11 nov 19:30:34.835: IKEv2:(SA-id = 1):Wachtrij voor asynchrone aanvragen

	*11 nov 19:30:34.835: IKEv2:(SA ID = 1): *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DID Event: EV_NO_EVENT *11 nov 19:30:34.835: IKEv2:KMI-bericht 8 verbruikt. Geen actie ondernomen. *11 nov 19:30:34.835: IKEv2:KMI-bericht 12 verbruikt. Geen actie ondernomen. *Nov 11 19:30:34.835: IKEv2:Geen gegevens om in mode configuratieset te verzenden. *11 nov 19:30:34.841: IKEv2:Toevoeging van ident handle 0x80000002 geassocieerd met SP 0x9506D414 voor sessie 8 *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DID Event: EV_OK_RECD_LOAD_IPSEC_ID *11 nov 19:30:34.841: IKEv2:(SA ID = 1):Actie: Action_Null *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DID Event: EV_START_ACCT *11 nov 19:30:34.841: IKEv2:(SA ID = 1):Financiële administratie niet vereist *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DID Event: EV_CHECK_DUPE *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: **AUTH_DON** Event: EV_CHK4_ROL	
Tunnel is omhoog op de Initiator en de status *toontBEREID*.	*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: READYEvent: EV_CHK_IKE_ONLY *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Ready Event: EV_I_OK	*****Nov 11 19:30:34.840: IKEv2:(S ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I MsgID = 00000001 CurState: **Ready** Event: EV_R_OK *Nov 11 19:30:34.840: IKEv2:(S ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I MsgID = 00000001 CurState: Ready Event: EV_NO_EVENT

CHILD_SA-debugs

Deze uitwisseling bestaat uit één verzoek/antwoordpaar en werd in IKEv1 een fase 2-uitwisseling genoemd. Het kan worden geïnitieerd tegen één van beide eind van IKE_SA nadat de aanvankelijke uitwisselingen zijn voltooid.

Router 1 CHILD_SA Berichtbeschrijving	Debugs	Router 2 CHILD_SA Berichtbeschrijving
Router 1 initieert de CHILD_SA exchange. Dit is het CREATE_CHILD_SA verzoek. Het CHILD_SA-	*Nov 11 19:31:35.873: IKEv2:Krijg een pakket van verzender	

pakket bevat doorgaans: • SA HDR (version.flags/exchange type) • Nonce Ni (optioneel): Als de CHILD_SA aangemaakt wordt als deel van de eerste uitwisseling, dan mag er geen tweede KE payload en nonce worden verstuurd. • SA-payload • KEi (Key-optional): Het CREATE_CHILD_SA-verzoek kan optioneel een KE-payload voor een extra DH-uitwisseling bevatten om sterkere garanties van voorwaartse geheimhouding voor de CHILD_SA mogelijk te maken. Als de SA-aanbiedingen verschillende DH-groepen bevatten, moet KEi een onderdeel van de groep zijn waarvan de initiatiefnemer verwacht dat de responder dit accepteert. Als het fout gist, mislukt de CREATE_CHILD_SA uitwisseling, en kan het opnieuw proberen met een andere KEi • N (Melden payload-optioneel). De Notify payload, wordt gebruikt om informatieve gegevens, zoals foutcondities en toestandsovergangen, naar een IKE-peer te verzenden. Een Notify payload kan verschijnen in een antwoordbericht (meestal geeft het aan waarom een verzoek is	*11 nov 19:31:35.873: IKEv2:Een item uit de piekwachtrij verwerken *Nov 11 19:31:35.873: IKEv2:(SA ID = 2):Verzoek heeft mess_id 3; verwacht 3 tot 7 *Nov 11 19:31:35.873: IKEv2:(SA ID = 2):Volgende payload: ENCR, versie: 2.0 **Exchange type: CREATE_CHILD_SA**, vlaggen: **INITIATOR** Message id: 3, lengte: 396 Inhoud payload: **SA** Volgende payload: N, gereserveerd: 0x0, lengte: 152 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 148 Voorstel: 1, Protocol id: IKE, SPI grootte: 8, #trans: 15 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA512 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA384 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA256 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA1 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: MD5 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA512 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA384 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA256 laatste transformatie: 0x3, gereserveerd:	

afgewezen), in een INFORMATION Exchange (om een fout te melden niet in een IKE-verzoek), of in een ander bericht om de mogelijkheden van de afzender aan te geven of om de betekenis van het verzoek te wijzigen.Als deze CREATE_CHILD_SA-uitwisseling een bestaande SA anders dan IKE_SA rekeying is, MOET de leidende N-payload van het type REKEY_SA de SA identificeren die wordt gerekeyed. Als deze CREATE_CHILD_SA uitwisseling een bestaande SA niet opnieuw bevestigt, MOET de N payload worden weggelaten.	0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: MD596 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1536_MODP/groep 5 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1024_MODP/groep 2 **N** Volgende lading: KE, gereserveerd: 0x0, lengte: 24 **KE** Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 136 DH groep: 2, Gereserveerd: 0x0 *Nov 11 19:31:35.874: IKEv2:Parse Notify payload: SET_VENSTER_SIZE **NOTIFY**(SET_VENSTER_SIZE) Volgende payload: NONE, gereserveerd: 0x0, lengte: 12 Security protocol-id: IKE, spi size: 0, type: SET_VENSTER_SIZE *Nov 11 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Ready Event: **EV_RECV_CREATE_CHILD_CHILD** *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Actie: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Event: EV_RECV_CREATE_CHILD_CHILD *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Actie: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Event: EV_VERIFY_MSG *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID =	

00000003 CurState: CHILD_R_INIT Event: EV_CHK_CC_TYPE_TYPE
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Event: **EV_REKEY_IKESA**
*11 nov 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Event: EV_GET_IKE_POLICY_POLICY
*Nov 11 19:31:35.874: IKEv2:% **Vooraf gedeelde sleutel op adres 10.0.0.2**
*Nov 11 19:31:35.874: IKEv2:% krijgen preshared sleutel op adres 10.0.0.2
*Nov 11 19:31:35.874: IKEv2:Het toevoegen van voorstel PHASE1-prop aan toolkit beleid
*11 nov 19:31:35.874: IKEv2:(SA-ID = 2):Gebruik van het IKEv2-profiel 'IKEV2-SETUP'
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Event: EV_PROC_MSG
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Event: EV_SET_POLICY
*nov 11 19:31:35.874: IKEv2:(SA-id = 2):**Configureerbaar beleid instellen**
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_GEN_DH_KEY
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_NO_EVENT
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6

R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_OK_RECD_DH_PUBKEY_RESP
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Actie: Action_Null
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event:**EV_GEN_DH_SECRET**
*Nov 11 19:31:35.881: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_NO_EVENT
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Actie: Action_Null
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_BLD_MSG
*nov 11 19:31:35.882: **IKEv2:ConstructNotify payload**: SET_VENSTER_SIZE
Inhoud payload:
SA Volgende payload: N, gereserveerd: 0x0, lengte: 56
  laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 52
  Voorstel: 1, Protocol id: IKE, SPI grootte: 8, #trans: 4 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12
    type: 1, gereserveerd: 0x0, id: AES-CBC
    laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8
    type: 2, gereserveerd: 0x0, id: SHA1
    laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8
    type: 3, gereserveerd: 0x0, id: SHA96
    laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8

	type: 4, gereserveerd: 0x0, id: DH_GROUP_1024_MODP/groep 2 **N** Volgende lading: KE, gereserveerd: 0x0, lengte: 24 **KE** Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 136 DH groep: 2, Gereserveerd: 0x0 **MELDEN** (SET_VENSTER_SIZE) Volgende payload: NONE, gereserveerd: 0x0, lengte: 12 Security protocol-id: IKE, spi size: 0, type: SET_VENSTER_SIZE	
	*Nov 11 19:31:35.869: IKEv2:(**SA ID = 2**):Volgende payload: ENCR, versie: 2.0 Wisseltype: **CREATE_CHILD_SA**, vlaggen: **INITIATOR** Bericht ID: 2, lengte: 460 Inhoud payload: ENCR Volgende payload: SA, gereserveerd: 0x0, lengte: 432 *Nov 11 19:31:35.873: IKEv2:Construct Melden payload: SET_VENSTER_SIZE Inhoud payload: **SA** Volgende payload: N, gereserveerd: 0x0, lengte: 152 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 148 Voorstel: 1, Protocol id: IKE, SPI grootte: 8, #trans: 15 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA512 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA384 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA256 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 2, gereserveerd: 0x0, id: SHA1 laatste transformatie: 0x3, gereserveerd: 0x0:	Dit pakket wordt ontvangen door router 2.

	lengte: 8 type: 2, gereserveerd: 0x0, id: MD5 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA512 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA384 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA256 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: MD596 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1536_MODP/groep 5 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1024_MODP/groep 2 **N** Volgende lading: KE, gereserveerd: 0x0, lengte: 24 **KE** Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 136 DH groep: 2, Gereserveerd: 0x0 **MELDEN** (SET_VENSTER_SIZE) Volgende payload: NONE, gereserveerd: 0x0, lengte: 12 Security protocol-id: IKE, spi size: 0, type: SET_VENSTER_SIZE	
	*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):Volgende payload: ENCR, versie: 2.0 Wisseltype: **CREATE_CHILD_SA,** vlaggen: **RESPONDER MSG-RESPONSE** Berichtnummer: 3, lengte: 300 Inhoud payload: **SA** Volgende payload: N, gereserveerd: 0x0, lengte: 56 laatste voorstel: 0x0, gereserveerd: 0x0, lengte: 52 Voorstel: 1, Protocol id: IKE, SPI grootte: 8, #trans: 4 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 12 type: 1, gereserveerd: 0x0, id: AES-CBC laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8	Router 2 bouwt nu het antwoord voor de uitwisseling CHILD_SA. Dit is het CREATE_CHILD_SA antwoord. Het CHILD_SA-pakket bevat doorgaans: • SA HDR (version.flags/exchange type) • Nonce Ni (optioneel): Als de CHILD_SA gecreëerd wordt als deel van de eerste uitwisseling, dan mag er geen tweede KE payload en nonce

	type: 2, gereserveerd: 0x0, id: SHA1 laatste transformatie: 0x3, gereserveerd: 0x0: lengte: 8 type: 3, gereserveerd: 0x0, id: SHA96 laatste transformatie: 0x0, gereserveerd: 0x0: lengte: 8 type: 4, gereserveerd: 0x0, id: DH_GROUP_1024_MODP/groep 2 **N** Volgende lading: KE, gereserveerd: 0x0, lengte: 24 **KE** Volgende payload: MELDEN, gereserveerd: 0x0, lengte: 136 DH groep: 2, Gereserveerd: 0x0 *Nov 11 19:31:35.882: IKEv2:Parse Notify payload: SET_VENSTER_SIZE **NOTIFY**(SET_VENSTER_SIZE) Volgende payload: NONE, gereserveerd: 0x0, lengte: 12 Security protocol-id: IKE, spi size: 0, type: SET_VENSTER_SIZE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_wait** Event: **EV_RECV_CREATE_CHILD_CHILD** *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Actie: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_PROC** Event: EV_CHK4_NOTIFY *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: **EV_VERIFY_MSG** *11 nov 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_PROC_MSG *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC	verstuurd worden. • SA-payload • KEi (Key-optional): Het CREATE_CHILD_SA-verzoek kan optioneel een KE-payload voor een extra DH-uitwisseling bevatten om sterkere garanties van voorwaartse geheimhouding voor de CHILD_SA mogelijk te maken. Als de SA-aanbiedingen verschillende DH-groepen bevatten, moet KEi een onderdeel van de groep zijn waarvan de initiatiefnemer verwacht dat de responder dit accepteert. Als het fout raadt, mislukt de CREATE_CHILD_SA uitwisseling, en moet het opnieuw proberen met een andere KEi. • N (Melden payload-optioneel): De Notify payload wordt gebruikt om informatieve gegevens, zoals foutcondities en toestandovergangen, naar een IKE-peer te verzenden. Een Notify payload kan verschijnen in een antwoordbericht (meestal geeft het aan waarom een verzoek is afgewezen), in een informatie-uitwisseling (om een fout te melden niet in een IKE-verzoek), of in een ander bericht om de mogelijkheden van de afzender aan te geven of om de betekenis van het verzoek te wijzigen. Als deze

	Event: EV_CHK4_PFS *11 nov 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_GEN_DH_SECRET *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_NO_EVENT *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_OK_RECD_DH_SECRET_RESP *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Actie: Action_Null *11 nov 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_CHK_IKE_REKEY *11 nov 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_GEN_SKEYID *11 nov 19:31:35.890: IKEv2:(SA ID = 2):Generate skeyid *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_DON** Event: **EV_ACTIVATE_NEW_SA** *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DID Event: EV_UPDATE_CAC_STATS *Nov 11 19:31:35.890: IKEv2:New ikev2 als aanvraag geactiveerd *11 nov 19:31:35.890: IKEv2:De telling van de uitgaande onderhandelingen is mislukt *Nov 11 19:31:35.890: IKEv2:(SA ID =	CREATE_CHILD_SA uitwisseling een bestaand SA anders dan de IKE_SA rekeying uitvoert, moet de leidende N payload van type REKEY_SA identificeren die worden gerekeyed. Als deze CREATE_CHILD_SA uitwisseling een bestaande SA niet opnieuw rekeying, moet de N payload worden weggelaten. Router 2 verstuurt de reactie en voltooit de activering van het nieuwe KIND SA.

	2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_done Event: EV_CHECK_DUPE *11 nov 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_done Event: EV_OK *11 nov 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: EXIT Event: EV_CHK_PENDING *11 nov 19:31:35.890: IKEv2:(SA ID = 2):Verwerkte reactie met bericht id 3, Verzoeken kunnen worden verzonden van bereik 4 tot 8 *11 nov 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 **CurState: EXIT** Event: EV_NO_EVENT	
Router 1 ontvangt het reactiepakket van router 2 en voltooit de activering van CHILD_SA.	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Volgende payload: ENCR, versie: 2.0 Exchange type: **CREATE_CHILD_SA**, vlaggen: **RESPONDER MSG-RESPONSE** Message id: 3, lengte: 300 Inhoud payload: ENCR Volgende payload: SA, gereserveerd: 0x0, lengte: 272 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event:**EV_CHK_IKE_REKEY** *11 nov 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_GEN_SKEYID *nov 11 19:31:35.882: IKEv2:(SA ID = 2):**Generate skeyid** *Nov 11 19:31:35.882: IKEv2:(SA ID =	

	2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_done Event:**EV_ACTIVATE_NEW_SA** *11 nov 19:31:35.882: IKEv2:Store mib index ikev2 3, platform 62 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DID Event: EV_UPDATE_CAC_STATS *Nov 11 19:31:35.882: IKEv2:New ikev2 als aanvraag geactiveerd *11 nov 19:31:35.882: IKEv2:Het tellen van de binnenkomende onderhandelingen is mislukt *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: **CHILD_R_DON** Gebeurtenis: EV_CHECK_DUPE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_done Event: EV_OK *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DID Event: EV_START_DEL_NEG_TMR. *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Actie: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: EXIT Event: EV_CHK_PENDING *11 nov 19:31:35.882: IKEv2:(SA ID = 2):Verzonden antwoord met bericht id 3, Aanvragen kunnen worden geaccepteerd van bereik 4 tot 8 *11 nov 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 **CurState: EXIT** Event:	

	EV_NO_EVENT	

Tunnelverificatie

ISAKMP

Opdracht

<#root>

show crypto ikev2 sa detailed

Router 1-uitgang

<#root>

```
Router1#
```

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote             fvrf/ivrf         Status
1         10.0.0.1/500          10.0.0.2/500       none/none         READY
      Encr: AES-CBC, keysize: 128,
         Hash: SHA96, DH Grp:2,
         Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/10 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: E58F925107F8B73F     Remote spi: AFD098F4147869DA
      Local id: 10.0.0.1
      Remote id: 10.0.0.2
      Local req msg id:  2       Remote req msg id:  0
      Local next msg id: 2       Remote next msg id: 0
      Local req queued:  2       Remote req queued:  0
      Local window:      5       Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
```

Router 2-uitgang

<#root>

```
Router2#
```

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local           Remote              fvrf/ivrf          Status
2         10.0.0.2/500    10.0.0.1/500        none/none          READY
      Encr: AES-CBC, keysize: 128, Hash: SHA96,
         DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/37 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: AFD098F4147869DA       Remote spi: E58F925107F8B73F
      Local id: 10.0.0.2
      Remote id: 10.0.0.1
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
```

IPSEC

Opdracht

<#root>

show crypto ipsec sa

> **Opmerking**: in deze output, in tegenstelling tot in IKEv1, wordt de waarde van de PFS DH groep weergegeven als "PFS (Y/N): N, DH groep: none" tijdens de eerste tunnelonderhandeling, maar na een rekey, verschijnen de juiste waarden. Dit is geen bug, hoewel het gedrag is beschreven in Cisco bug-id CSC67056. (Alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools of -informatie.)
> Het verschil tussen IKEv1 en IKEv2 is dat in het laatste geval de Child SAâ€™s worden gecreëerd als onderdeel van de AUTH-uitwisseling zelf. De DH Group geconfigureerd onder de crypto kaart zou alleen worden gebruikt tijdens rekey. Vandaar dat je 'PFS (Y/N): N, DH groep: none' ziet tot de eerste rekey.
> Met IKEv1, ziet u een ander gedrag, omdat Child SA creatie gebeurt tijdens Quick Mode, en het CREATE_CHILD_SA bericht heeft een voorziening om de Key Exchange payload te dragen die de DH parameters specificeert om een nieuw gedeeld geheim af te leiden.

Router 1-uitgang

<#root>

```
Router1#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0,
         local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt:
         10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt:
         10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.1,
         remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0xF6083ADD(4127734493)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec):
         (4276853/3592)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4276853/3592)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Router 2-uitgang

<#root>

```
Router2#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.2,
         remote crypto endpt.: 10.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x6B74CB79(1802816377)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime
         (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

```
     outbound ah sas:

     outbound pcp sas:
```

U kunt ook de uitvoer van de opdracht **show crypto sessie** op beide routers controleren; deze uitvoer toont de status van de tunnelsessie als UP-ACTIVE.

<#root>

```
Router1#
```

show crypto session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
  IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Router2#
```

show cry session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
  IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Gerelateerde informatie

- **IKEv2-pakketuitwisseling en debuggen op protocolniveau**
- **Cisco technische ondersteuning en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.