Probleemoplossing voor IPsec-problemen voor servicetunnels in vEdge met IKEv2

Inhoud

Inleiding

Dit document beschrijft hoe u de meest gebruikelijke problemen voor IPsec-tunnels (Internet Protocol Security) voor derdenapparaten kunt oplossen met geconfigureerde Internet Key Exchange versie 2 (IKEv2). Populairste talen die als Service/Transport Tunes op Cisco SD-WAN documentatie worden genoemd. Dit document legt ook uit hoe u IKE-knooppunten kunt inschakelen en lezen en hoe u deze kunt koppelen aan de pakketuitwisseling om het punt van fout bij een IPsec-onderhandeling te begrijpen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IKEv2
- IPsec-onderhandeling
- Cisco SD-WAN

Gebruikte componenten

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

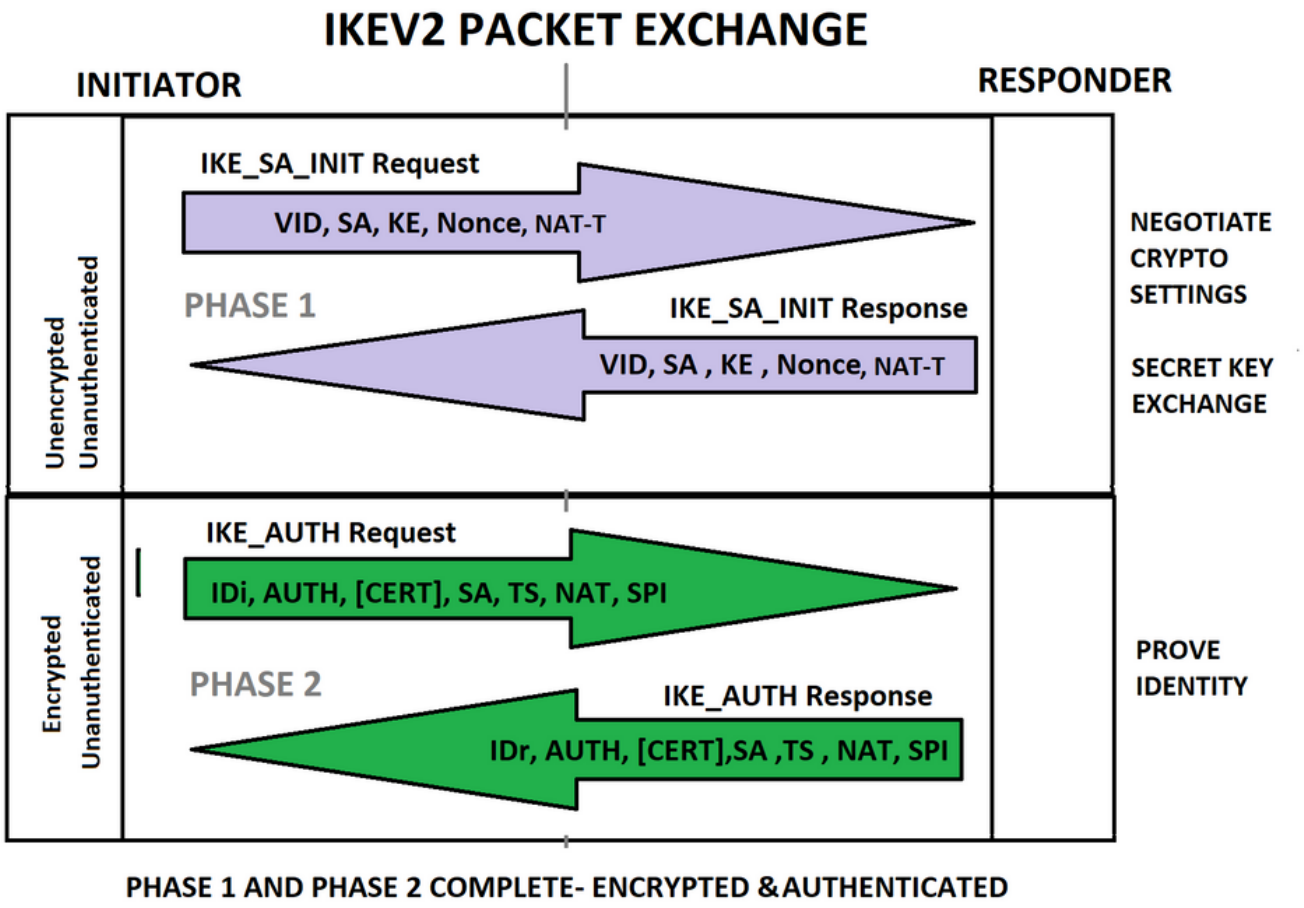
Achtergrondinformatie

IKE-woordenlijst

- **IPsec-beveiliging (Internet Protocol Security)** is een standaardreeks protocollen tussen 2 communicatiepunten over het IP-netwerk die gegevensverificatie, integriteit en vertrouwelijkheid bieden.
- **Internet Key Exchange versie 2 (IKEv2) is het protocol dat wordt gebruikt om een beveiligingsassociatie (SA) op te zetten in de IPsec-protocolreeks.**
- Een **veiligheidsorganisatie** (**SA**) is de instelling van gedeelde beveiligingskenmerken tussen twee netwerkentiteiten ter ondersteuning van beveiligde communicatie. Een SA kan eigenschappen omvatten zoals cryptografisch algoritme en -modus; Verkeersencryptiesleutel en parameters voor de netwerkgegevens die over de verbinding moeten worden doorgegeven.
- De **verkoper-ID's** (**VID**) worden gebruikt om de peer-apparaten te identificeren met dezelfde verkoper-implementatie, teneinde de verkoper-specifieke kenmerken te ondersteunen.
- **Eenmaal**: willekeurige waarden die in de uitwisseling worden gecreëerd om willekeurig toe te voegen en herhalingsaanvallen te voorkomen.
- **Key-exchange (KE)**-informatie voor het beveiligde sleuteluitwisselingsproces Diffie-Hellman (DH).
- **Identity Initiator/responder (IDi/IDr.)** wordt gebruikt om de authenticatie-informatie naar de peer te sturen. Deze informatie wordt doorgegeven onder bescherming van het gemeenschappelijk geheim.
- De gedeelde sleutel van IPSec kan met het gebruik van DH opnieuw worden afgeleid om **Perfect Forward Secundaire (PFS)** te verzekeren of met een verfrissing van het gedeelde geheim dat uit de oorspronkelijke DH-beurs is afgeleid.
- **Diffie-Hellman (DH) key exchange is een methode van beveiligde cryptografische algoritmen uitwisseling via een openbaar kanaal.**
- **Traffic Selectors (TS)** zijn de proxy-identiteiten of het verkeer dat via de IPsec-onderhandeling wordt uitgewisseld om door de tunnel versleuteld te laten passeren.

IKEv2 Packet Exchange

Elk IKE-pakket bevat payload-informatie voor de tunnelvestiging. De lijst van IKE verklaart de afkortingen die op deze afbeelding worden getoond als deel van de lading inhoud voor de pakketuitwisseling.

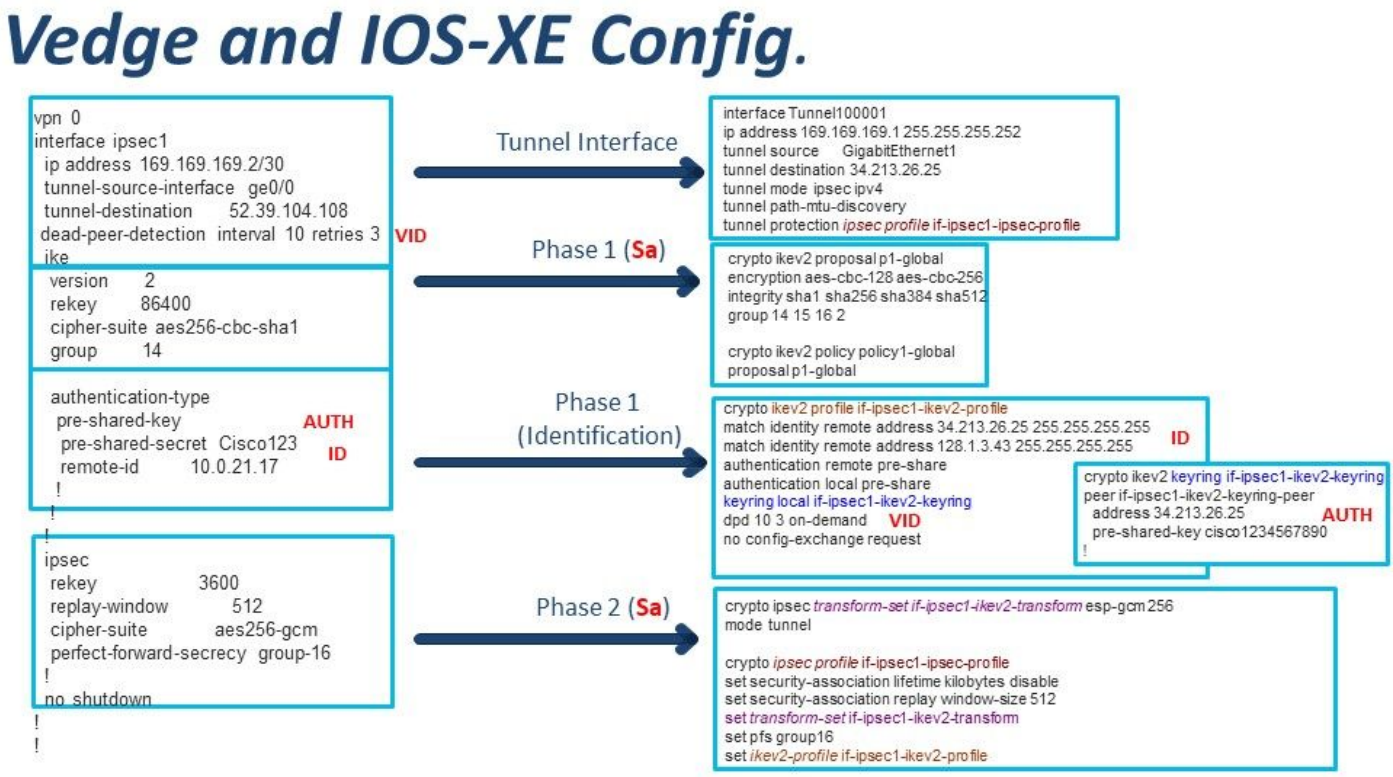


IKEV2-beurs

> **Opmerking:** Het is belangrijk om te controleren op welke pakketuitwisseling van de IKE-onderhandeling de IPsec-tunnelheid er niet in slaagt snel te analyseren welke configuratie betrokken is om het probleem effectief aan te pakken.

> **Opmerking:** Dit document beschrijft niet dieper de IKEv2 Packet exchange. Voor meer verwijzingen, navigeer naar IKEv2 Packet Exchange en Protocol Level Debugging

Het is nodig om de vEdge-configuratie te correleren met de Cisco IOS® XE configuratie. Het is ook handig om de IPsec-concepten en de payload-inhoud voor IKEv2-pakketuitwisselingen aan te passen zoals in de afbeelding.



Opmerking: Elk deel van de configuratie wijzigt een aspect van de IKE-onderhandeling. Het is belangrijk om de opdrachten te correleren met de protocolonderhandeling van IPsec.

Problemen oplossen

IKE-debugs inschakelen

Op vEdge **debug-iked** kan level-informatie worden gedebug door IKEv1 of IKEv2.

```
debug iked misc high
debug iked event high
```

Het is mogelijk om de huidige debug-informatie binnen **vshell** weer te geven en de opdracht **tail -f <debug pad>** uit te voeren.

```
vshell
tail -f /var/log/message
```

In CLI kan ook de huidige logbestanden/debug-informatie voor het opgegeven pad worden weergegeven.

```
monitor start /var/log/messages
```

Tips voor het starten van het proces voor probleemoplossing voor IPsec-problemen

Het is mogelijk om drie verschillende IPsec-scenario's te scheiden. Het is een goed referentiepunt om het symptoom te identificeren voor een betere benadering om te weten hoe te beginnen.

1. IPsec-tunnel heeft geen vestigingen.

2. IPsec-tunnel ging omlaag en werd zelf opnieuw geïnstalleerd. (Flapped)
3. IPsec-tunnel ging omlaag en blijft in een slechte staat.

Voor de IPsec-tunnel heeft geen symptomen, moet u deze in real-time debug innemen om te controleren wat het huidige gedrag bij de IKE-onderhandeling is.

Voor een daling van de IPsec-tunnel en herstel van de eigen symptomen, meestal tunnelvlakte en de grondoorzaak-analyse (RCA) is nodig. Het is absoluut noodzakelijk om de tijdstempel te kennen van de daling van de tunnel of de tijd te hebben om de debugs te bekijken.

Voor de IPsec-tunnel ging omlaag en blijft hij op neerwaartse symptomen staan. Dat betekent dat de tunnel vroeger werkte, maar om welke reden dan ook, kwam hij omlaag en we moeten weten waarom de tunnel is afgebroken en wat het huidige gedrag is dat verhindert dat de tunnel weer wordt opgezet.

Identificeer de punten voordat de probleemoplossing begint:

1. IPsec-tunnel (nummer) met problemen en configuratie.
2. De tijdstempel die werd gebruikt toen de tunnel daalde (indien van toepassing).
3. IPsec peer IP-adres (tunnelbestemming).

Alle debugs en logbestanden worden opgeslagen op **/var/log/boodschappen** bestanden. Voor de huidige logbestanden worden ze opgeslagen in een berichtenbestand, maar voor dit specifieke symptoom kan de flap uren/dagen na de uitgifte worden geïdentificeerd, wat zeer waarschijnlijk te maken heeft met debugs in de vorm van berichten1,2,3, enz. Het is belangrijk om de tijdstempel te kennen om het juiste berichtbestand te bekijken en de debugs (charon) te analyseren voor de IKE onderhandeling van het IPsec Tunnel gerelateerde bestand.

De meeste apparaten drukken het aantal van de IPsec-tunnel niet af. De meest frequente manier om de onderhandeling en pakketten te identificeren is met het IP adres van de verre peer en het IP adres waar de tunnel op de rand vandaan komt. Een paar voorbeelden van IKE-debugs:

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_IPsec2_1'
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
```

De specificaties voor de IKE INIT-onderhandeling tonen het IPsec-tunnelnummer, maar de daaropvolgende informatie voor pakketuitwisseling gebruikt alleen de IPsec-tunneladressen.

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_ipsec2_1'
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jun 18 00:31:22 vedge01 charon: 16[NET] sending packet: from 10.132.3.92[500] to 10.10.10.1[500]
(464 bytes)
Jun 18 00:31:22 vedge01 charon: 12[NET] received packet: from 10.10.10.1[500] to
10.132.3.92[500] (468 bytes)
Jun 18 00:31:22 vedge01 charon: 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(HTTP_CERT_LOOK) N(FRAG_SUP) V ]
Jun 18 00:31:22 vedge01 charon: 12[ENC] received unknown vendor ID:
4f:85:58:17:1d:21:a0:8d:69:cb:5f:60:9b:3c:06:00
Jun 18 00:31:22 vedge01 charon: 12[IKE] local host is behind NAT, sending keep alives
```

IPsec-tunnelconfiguratie:

```
interface ipsec2 ip address 192.168.1.9/30 tunnel-source 10.132.3.92 tunnel-destination
10.10.10.1 dead-peer-detection interval 30 ike version 2 rekey 86400 cipher-suite aes256-cbc-
sha1 group 14 authentication-type pre-shared-key pre-shared-secret
$8$wgrs/Cw6tX0na34yF4Fga0B62mGBpHFdOzFaRmoYfnBioWVO3s3efFPBbkaZqvoN ! ! ! ipsec rekey 3600
replay-window 512 cipher-suite aes256-gcm perfect-forward-secrecy group-14 !
```

Symptoom 1. IPsec-tunnelheid niet ingesteld

Aangezien het hier om de eerste implementatie voor de tunnel gaat, is deze nog niet gereed en zijn de IKE-debugs de beste optie.

Symptoom 2. IPsec-tunnelband werd afgebroken en zelf opnieuw geïnstalleerd

Zoals eerder vermeld, is dit symptoom gericht op het kennen van de diepere oorzaak van de daling van de tunnel. Als de analyse van de basisoorzaak bekend is, voorkomt de beheerder van het netwerk soms andere problemen.

Identificeer de punten voordat de probleemoplossing begint:

1. IPsec-tunnel (nummer) met problemen en configuratie.
2. De tijdstempel van de tunnel ging omlaag.
3. IPsec peer IP-adres (tunnelbestemming)

DPD-terugzendingen

In dit voorbeeld ging de tunnel omlaag op 18 jun om 00:31:17.

```
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-vedge01-FTMD-6-INFO-1000001: VPN 1 Interface ipsec2
DOWN
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-vedge01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"vedge01" system-ip:4.0.5.1 vpn-id:1 if-
name:"ipsec2" new-state:down
```

> **Opmerking:** De blogs voor IPsec-tunneldownloads maken geen deel uit van *FTMD*-blogs. Daarom worden *charon* noch *IKE* gedrukt.

> **Opmerking:** De bijbehorende logbestanden worden meestal niet samen afgedrukt, maar er is meer informatie tussen de logbestanden die geen verband houden met hetzelfde proces.

Stap 1. Nadat de tijdstempel is geïdentificeerd en de tijd en de logbestanden zijn gecorreleerd, start u de logbestanden van onder naar boven.

```
Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits
```

```
Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:28:22 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
```

```
Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
```

De laatste succesvolle DPD-pakketuitwisseling wordt beschreven als verzoek # 542.

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 13.51.17.190[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]
```

Stap 2. Plaats alle informatie in de juiste volgorde:

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to
10.132.3.92[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]

Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:28:22 Lvedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-FTMD-6-INFO-1000001: VPN 1 Interface
ipsec2 DOWN
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"LONDSR01" system-ip:4.0.5.1 vpn-id:1 if-
name:"ipsec2" new-state:down
```

Bijvoorbeeld, de tunnel gaat omlaag vanwege vEdge01 ontvangt de DPD-pakketten niet van 10.10.10.1. Verwacht wordt na 3 DPD-terugzendingen wordt de IPsec-peer ingesteld op "verloren" en de tunnel gaat omlaag. Er zijn meerdere redenen voor dit gedrag, meestal, is het verwant met

de ISP waar de pakketten in het pad verloren of gedaald zijn. Als de kwestie eens voorkomt is er geen manier om het verloren verkeer te volgen, echter, als de kwestie blijft voortbestaan, kan het pakket met het gebruik van Captures op vEdge, Remote IPSec peer, en de ISP worden getraceerd.

Symptoom 3. IPsec-tunneleffect werd gedempt en blijft op een downstate

Zoals eerder in dit symptoom werd gezegd, werkte de tunnel voordien prima, maar om welke reden dan ook, hij kwam naar beneden en de tunnel kon niet weer tot stand komen. In dit scenario is er een impact op het netwerk.

identificeer de punten voordat de probleemoplossing wordt gestart:

1. IPsec-tunnel (nummer) met problemen en configuratie.
2. De tijdstempel van de tunnel ging omlaag.
3. IPsec peer IP-adres (tunnelbestemming)

PFS-wanverhouding

In dit voorbeeld begint de probleemoplossing niet met de tijdstempel wanneer de tunnel omlaag gaat. Aangezien het probleem zich blijft voordoen, is het IKE-instrument de beste optie.

```
interface ipsec1 description VWAN_VPN ip address 192.168.0.101/30 tunnel-source-interface ge0/0
tunnel-destination 10.10.10.1 ike version 2 rekey 28800 cipher-suite aes256-cbc-sha1 group 2
authentication-type pre-shared-key pre-shared-secret
"$8$njK2pLLjgKWNQu0KecNtY3+fo3hbTs0/7iJy6unNtersmCGjGB38kIPjsoqqXZdVmtizLu79\naQdjt2POM242Yw=="
! ! ! ipsec rekey 3600 replay-window 512 cipher-suite aes256-cbc-sha1 perfect-forward-secrecy
group-16 ! mtu 1400 no shutdown
```

De debug-toets is ingeschakeld en de onderhandeling wordt weergegeven.

```
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (508 bytes)
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] parsed CREATE_CHILD_SA request 557 [ SA No
TSi TSr ]
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] received proposals:
ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] failed to establish CHILD_SA, keeping
IKE_SA
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] generating CREATE_CHILD_SA response 557 [
N(NO_PROP) ]
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] sending packet: from 172.28.0.36[4500] to
10.10.10.1[4500] (76 bytes)

daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (76 bytes)
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] parsed INFORMATIONAL request 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] generating INFORMATIONAL response 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] sending packet: from 172.28.0.36[4500] to
10.10.10.1[4500] (76 bytes)
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to
```

```
172.28.0.36[4500] (396 bytes)
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[ENC] parsed CREATE_CHILD_SA request 559 [ SA No
TSi TSr ]
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG] received proposals:
ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
daemon.info: Apr 27 05:12:58 Avedge01 charon: 07[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[IKE] failed to establish CHILD_SA, keeping
IKE_SA
```

> **Opmerking:** CREATE_CHILD_SA pakketten worden uitgewisseld voor elk rekey of nieuwe SA. Voor meer verwijzingen, navigeer om IKEv2 Packet Exchange te begrijpen

IKE-debugs vertonen hetzelfde gedrag en worden constant herhaald, dus is het mogelijk om een deel van de informatie te verwerken en te analyseren:

CREATE_CHILD_SA betekent een rekey, met het doel om de nieuwe SPIS te creëren en te ruilen tussen de IPsec endpoints.

- De rand ontvangt het CREATE_CHILD_SA aanvraagpakket van 10.10.10.1.
- De rand verwerkt het verzoek en verifieert de voorstellen (SA) die door peer 10.10.10.10 zijn verstuurd
- De rand vergelijkt het ontvangen voorstel dat door de peer wordt verstuurd met zijn geconfigureerde voorstellen.
- De CREATE_CHILD_SA uitgewisselde mislukking met "geen aanvaardbare voorstellen gevonden".

Op dit moment is de vraag: **Waarom is er een configuratie mismatch als de tunnel eerder werkte en er geen wijzigingen werden aangebracht?**

Diep analyseren, er is een extra veld in de geconfigureerde voorstellen dat de peer niet stuurt.

Ingevulde voorstellen: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ

Ontvangen voorstellen:
ESP:AES_GCM_16_256/NO_EXT_SEQ,
ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ

MODP_4096 is DH groep 16, die de randen heeft geconfigureerd voor PFS (perfect-voorwaarts-geheim) in fase 2 (IPsec-sectie).

PFS is de enige ongeschikte configuratie waarin de tunnel succesvol kan worden ingesteld of niet volgens wie de initiator of de responder is in de IKE-onderhandeling. Wanneer de rekey start, kan de tunnel echter niet doorgaan en kan dit symptoom worden gepresenteerd of gerelateerd aan.

vEdge IPSec/Ikev2-tunnels worden niet opnieuw geïnitieerd na omlaag te zijn gedraaid vanwege een gebeurtenis die tot wissing heeft geleid

Zie Cisco bug-ID CSCvx86427 voor meer informatie over dit gedrag.

Aangezien het probleem zich blijft voordoen, biedt IKE de beste opties. Echter, voor dit specifieke bug als debugs zijn ingeschakeld wordt er geen informatie weergegeven, noch de terminal noch het berichtbestand.

Om deze kwestie te verkleinen en te controleren of vEdge de Cisco bug-ID CSCvx86427 raakt, moet u het moment vinden dat de tunnel omlaag gaat.

identificeer de punten voordat de probleemoplossing wordt gestart:

1. IPsec-tunnel (nummer) met problemen en configuratie.
2. De tijdstempel van de tunnel ging omlaag.
3. IPsec peer IP-adres (tunnelbestemming)

Nadat de tijdstempel is geïdentificeerd en de tijd en de logboeken zijn gecorreleerd, bekijk de logbestanden net voordat de tunnel omlaag gaat.

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] received DELETE for IKE_SA ipsec1_1[217]
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between
10.16.0.5[10.16.0.5]...10.10.10.1[10.10.10.1]
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between
10.16.0.5[10.16.0.5]...10.10.10.1[10.10.10.1]
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
Apr 13 22:05:21 vedge01 charon: 12[ENC] generating INFORMATIONAL response 4586 [ ]
Apr 13 22:05:21 vedge01 charon: 12[NET] sending packet: from 10.16.0.5[4500] to 10.10.10.1[4500]
(80 bytes)
Apr 13 22:05:21 vedge01 charon: 12[KNL] Deleting SAD entry with SPI 00000e77
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-FTMD-6-INFO-1000001: VPN 1 Interface
ipsec1 DOWN
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"vedge01" system-ip:4.1.0.1 vpn-id:1 if-
name:"ipsec1" new-state:down
```

> **Opmerking:** Er zijn pakketten van meerdere DELETES op een IPsec-onderhandeling, en de DELETE voor CHILD_SA is een verwachte VERWIJDERING voor een REKEY-proces, wordt deze kwestie gezien wanneer een zuiver IKE_SA VERWIJDERINGSPakket wordt ontvangen zonder enige specifieke IPsec-onderhandeling. Hiermee verwijdert u alle IPsec/IKE-tunnel.

Gerelateerde informatie

- KEv2 Packet Exchange en Protocol-niveau
- Internet Key Exchange (IKE) - RFC 2409
- IKEv2 - RFC 7296
- Site-to-Site LAN met IPSec tussen vEdge en Cisco IOS
- Technische ondersteuning en documentatie – Cisco Systems