Fehlerbehebung bei IPsec-Problemen für Service Tunnels auf vEdges mit IKEv2

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die häufigsten Probleme bei IPsec-Tunneln (Internet Protocol Security) zu Geräten von Drittanbietern beheben, für die Internet Key Exchange Version 2 (IKEv2) konfiguriert wurde. Wird in der Cisco SD-WAN-Dokumentation häufig als Service-/Transport-Tunnel bezeichnet. In diesem Dokument wird auch erläutert, wie IKE-Debugger aktiviert und gelesen und dem Paketaustausch zugewiesen werden, um den Fehlerpunkt bei einer IPsec-Aushandlung zu verstehen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IKEv2
- IPsec-Aushandlung
- Cisco SD-WAN

Verwendete Komponenten

Die Informationen in diesem Dokument wurden von den Geräten in einer spezifischen Laborumgebung auf der Basis von vEdge-Routern erstellt. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

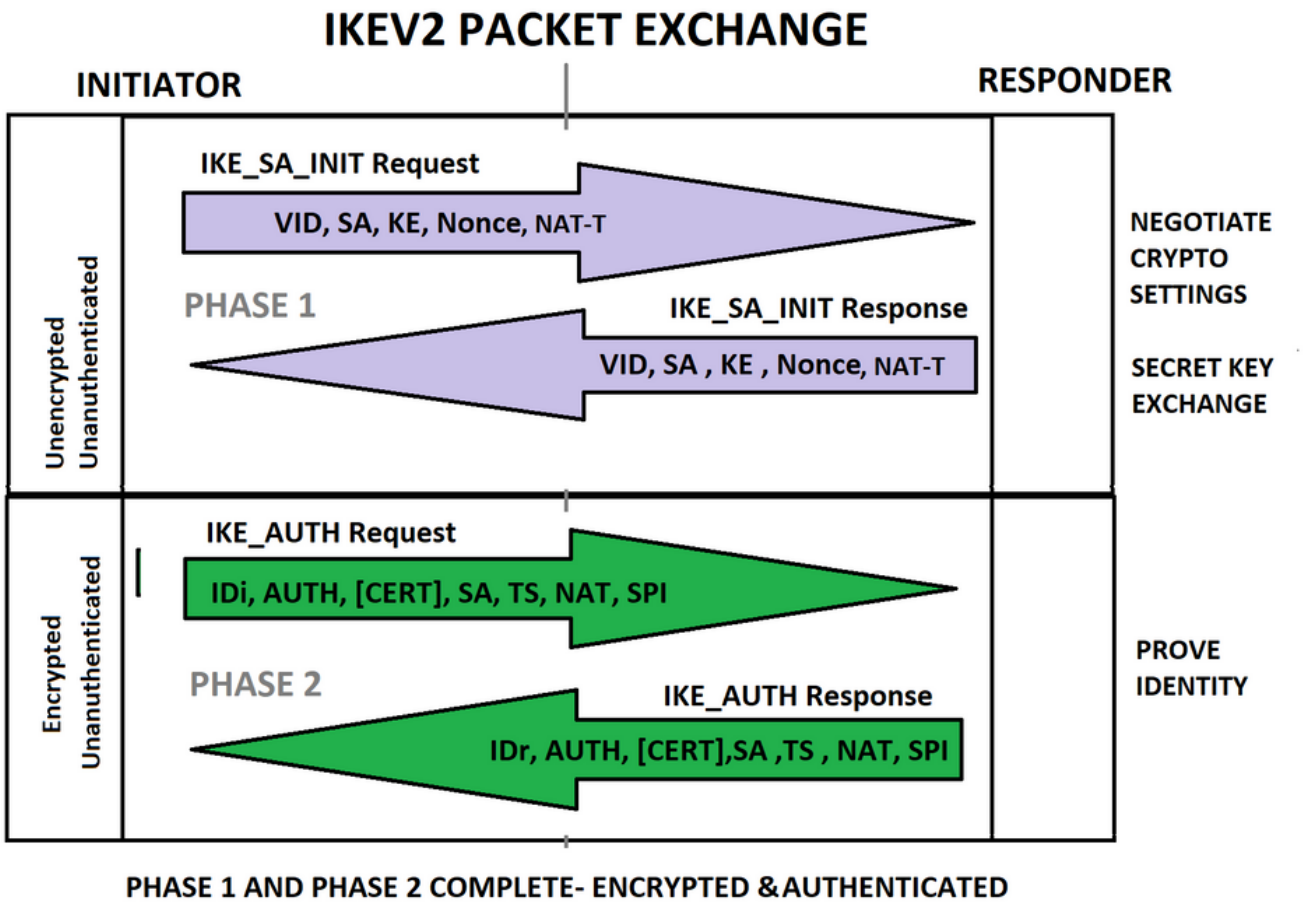
Hintergrundinformationen

IKE-Glossar

- **Internet Protocol Security (IPsec)** ist eine Standardsuite von Protokollen zwischen zwei Kommunikationspunkten im IP-Netzwerk, die Datenauthentifizierung, -integrität und -vertraulichkeit bieten.
- **Internet Key Exchange Version 2 (IKEv2) ist das Protokoll zum Einrichten einer Sicherheitszuordnung (Security Association, SA) in der IPsec-Protokoll-Suite.**
- Eine **Sicherheitszuordnung** (**SA**) ist die Einrichtung gemeinsamer Sicherheitsattribute zwischen zwei Netzwerkentitäten zur Unterstützung der sicheren Kommunikation. Ein SA kann Attribute wie Verschlüsselungsalgorithmus und -modus enthalten. Verschlüsselungsschlüssel für den Datenverkehr; und Parameter für die Netzwerkdaten, die über die Verbindung weitergegeben werden sollen.
- Die **Anbieter-IDs** (**VID**) werden verarbeitet, um festzustellen, ob der Peer die Funktion NAT-Traversal, Dead Peer Detection, Fragmentation usw. unterstützt.
- **Einmal**: eine zufällig generierte Nummer, die der Initiator sendet. Diese wird zusammen mit den anderen Artikeln mit dem vereinbarten Schlüssel gehasht und zurückgesendet. Der Initiator überprüft das Cookie und die Nonce und lehnt alle Nachrichten ab, die nicht einmal das Recht haben. Dies hilft, eine Wiederholung zu verhindern, da kein Dritter vorhersagen kann, was die Zufallsgenerierung ist.
- **Key-Exchange (KE)**-Informationen für den sicheren Schlüsselaustauschprozess Diffie-Hellman (DH).
- **Identitätsinitiator/-Responder (IDi/IDr.)** wird verwendet, um Authentifizierungsinformationen an den Peer zu senden. Diese Informationen werden unter dem Schutz des gemeinsamen geheimen Geheimnisses übermittelt.
- Der gemeinsam genutzte IPSec-Schlüssel kann mit der Verwendung von DH erneut abgeleitet werden, um **Perfect Forward Secrecy (PFS)** oder eine Aktualisierung des vom ursprünglichen DH-Austausch abgeleiteten gemeinsamen geheimen Codes sicherzustellen.
- **Der Diffie-Hellman (DH)-Schlüsselaustausch ist eine Methode zum sicheren Austausch kryptografischer Algorithmen über einen öffentlichen Kanal.**
- **Datenverkehrsauswahl (TS)** sind die Proxy-Identitäten oder der Datenverkehr, der bei der IPsec-Aushandlung ausgetauscht wird, um den Tunnel verschlüsselt zu durchlaufen.

IKEv2-Paketaustausch

Jedes IKE-Paket enthält Payload-Informationen für die Tunneleinrichtung. Im IKE-Glossar werden die Abkürzungen erläutert, die auf diesem Bild als Teil des Payload-Inhalts für den Paketaustausch angezeigt werden.

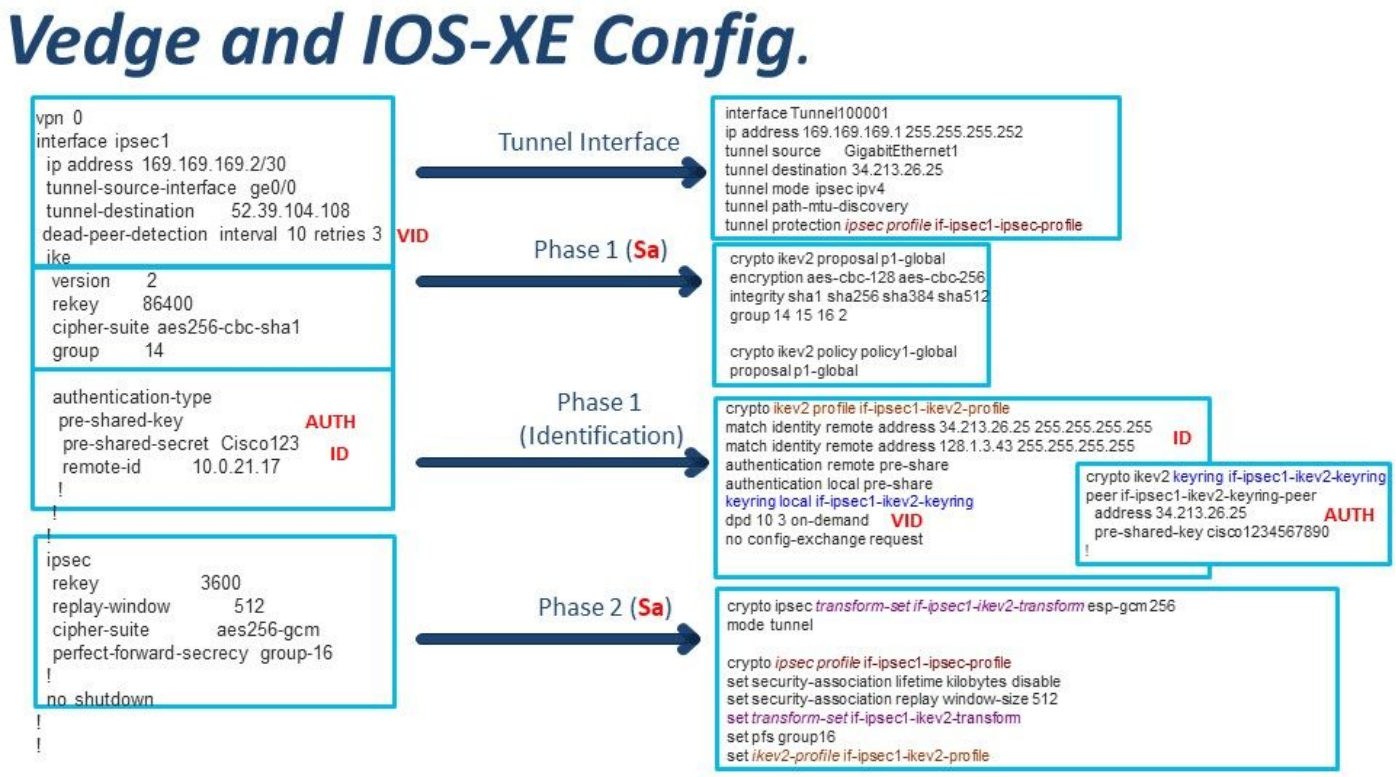


PHASE 1 AND PHASE 2 COMPLETE- ENCRYPTED &AUTHENTICATED

Anmerkung: Es ist wichtig zu überprüfen, welche Paketaustauschverbindungen der IKE-Aushandlung der IPsec-Tunnel nicht schnell analysieren kann, um das Problem wirksam zu beheben.

Anmerkung: In diesem Dokument wird der IKEv2-Paketaustausch nicht genauer beschrieben. Weitere Referenzen finden Sie unter Debuggen auf IKEv2-Paketaustausch und Protokollebene.

Es ist erforderlich, die vEdge-Konfiguration mit der Cisco IOS® XE-Konfiguration zu korrelieren. Außerdem ist es hilfreich, die IPsec-Konzepte und den Payload-Inhalt für den IKEv2-Paketaustausch, wie im Bild gezeigt, aufeinander abzustimmen.



Anmerkung: Jeder Teil der Konfiguration ändert einen Aspekt des IKE-Verhandlungs-Austauschs. Es ist wichtig, die Befehle mit der Protokollaushandlung von IPsec zu korrelieren.

Fehlerbehebung

IKE-Debuggen aktivieren

Auf vEdges ermöglicht **Debug** Debugging-Informationen entweder IKEv1 oder IKEv2.

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

Es ist möglich, die aktuellen Debuginformationen in **vshell** anzuzeigen und den Befehl **tail -f**<debug path> auszuführen.

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

In CLI können auch die aktuellen Protokolle/Debuginformationen für den angegebenen Pfad angezeigt werden.

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

Tipps zum Starten des Fehlerbehebungsprozesses bei IPsec-Problemen

Es ist möglich, drei verschiedene IPsec-Szenarien zu trennen. Es ist ein guter Bezugspunkt, um das Symptom zu identifizieren, um einen besseren Ansatz zu wissen, wie man beginnt.

1. IPsec-Tunnel wird nicht eingerichtet.
2. Der IPsec-Tunnel ist ausgefallen, und er wird von alleine wiederhergestellt. (Flapping)
3. Der IPsec-Tunnel ist ausgefallen, und er bleibt in einem Downstate.

Da der IPsec-Tunnel keine Symptome feststellt, muss das Debuggen in Echtzeit durchgeführt werden, um das aktuelle Verhalten bei der IKE-Aushandlung zu überprüfen.

Für den IPsec-Tunnel ging ein Ausfall ein und setzte sich auf eigene Symptome wieder ein, die meist als Tunnel-Flapped bezeichnet werden und die Ursachenanalyse (Root Cause Analysis, RCA) erforderlich ist. Es ist unerlässlich, den Zeitstempel zu kennen, wenn der Tunnel ausgefallen ist, oder über eine veranschlagte Zeit zu verfügen, um sich die Debuggen anzusehen.

Da der IPsec-Tunnel ausgefallen ist und weiterhin Downstate-Symptome aufweist, bedeutet dies, dass der Tunnel zuvor funktioniert hat, aber aus irgendeinem Grund ist er heruntergefallen, und wir müssen den Grund für die Entfernung und das aktuelle Verhalten kennen, das verhindert, dass der Tunnel wieder erfolgreich hergestellt wird.

Identifizieren Sie die Punkte, bevor die Fehlerbehebung beginnt:

1. IPsec-Tunnel (Nummer) mit Problemen und Konfiguration.
2. Der Zeitstempel, wenn der Tunnel ausfällt (falls zutreffend).
3. IPsec-Peer-IP-Adresse (Tunnelziel).

Alle Debug- und Protokolldateien werden in Dateien mit **/var/log/messages** gespeichert, für die aktuellen Protokolle werden sie in der Nachrichtendatei gespeichert, aber für dieses spezielle Symptom könnte die Flapping Stunden/Tage nach dem Problem identifiziert werden, höchstwahrscheinlich betreffen Debug-Probleme Nachrichten1,2,3..usw. Es ist wichtig, den Zeitstempel zu kennen, um die richtige Nachrichtendatei anzuzeigen und die Debug-(Charon-)Dateien für die IKE-Aushandlung des IPsec-Tunnels zu analysieren.

Die meisten Debugger drucken die Anzahl des IPsec-Tunnels nicht. Die häufigste Methode zur Identifizierung der Aushandlung und Pakete ist die IP-Adresse des Remote-Peers und die IP-Adresse, von der der Tunnel am Vedge stammt. Einige Beispiele für gedruckte IKE-Debuggen:

```
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
```

Die Debug für die IKE-INIT-Aushandlung zeigt die IPsec-Tunnelnummer an. Die nachfolgenden Informationen für den Paketaustausch verwenden jedoch nur die IP-Adressen des IPsec-Tunnels.

```
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-Tunnelkonfiguration:

```
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 !
```

Symptom 1. IPsec-Tunnel wird nicht eingerichtet

Da das Problem die erste Implementierung für den Tunnel sein kann, ist er nicht aktiv, und die IKE-Debuggen sind die beste Option.

Symptom 2. Der IPsec-Tunnel ging herunter und wurde wieder aufgebaut

Wie bereits erwähnt, wird dieses Symptom in der Regel angesprochen, um die Ursache für den Tunnelausfall zu ermitteln. Da die Ursachenanalyse bekannt ist, verhindert der Administrator des Netzwerks manchmal weitere Probleme.

Identifizieren Sie die Punkte, bevor die Fehlerbehebung beginnt:

1. IPsec-Tunnel (Nummer) mit Problemen und Konfiguration.
2. Der Zeitstempel, als der Tunnel ausfiel.
3. IPsec-Peer-IP-Adresse (Tunnelziel)

DPD-Neuübertragungen

In diesem Beispiel ging der Tunnel am 18. Juni um 00:31:17 herunter.

```
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
```

> **Anmerkung:** Die Protokolle für den Ausfall von IPsec-Tunneln sind nicht Teil von iked debugs, sondern *FTMD*-Protokolle. Daher würden weder *Charon* noch *IKE* gedruckt.

> **Anmerkung:** Die zugehörigen Protokolle werden in der Regel nicht zusammen gedruckt, es gibt mehr Informationen zwischen ihnen, die nicht mit dem gleichen Prozess zusammenhängen.

Schritt 1: Nachdem der Zeitstempel identifiziert und die Uhrzeit und die Protokolle korreliert wurden, können Sie die Protokolle von unten nach oben überprüfen.

```
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)
```

Der letzte erfolgreiche DPD-Paketaustausch wird als Anforderung Nr. 542 beschrieben.

```
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 [ ]
```

Schritt 2: Stellen Sie alle Informationen in der richtigen Reihenfolge zusammen:

```
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
```

Im beschriebenen Beispiel wird der Tunnel aufgrund von vEdge01 ausfallen, da die DPD-Pakete nicht von 10.10.10.1 empfangen werden. Es wird erwartet, dass der IPsec-Peer nach 3 erneuten DPD-Übertragungen als "Locked" (Verloren) festgelegt wird und der Tunnel ausfällt. Für dieses Verhalten gibt es mehrere Gründe, die in der Regel mit dem ISP zusammenhängen, bei dem die Pakete im Pfad verloren gehen oder verworfen werden. Wenn das Problem einmal auftritt, gibt es keine Möglichkeit, den verlorenen Datenverkehr zu verfolgen. Wenn das Problem jedoch weiterhin besteht, kann das Paket mithilfe von Captures auf vEdge, Remote-IPSec-Peer und dem ISP nachverfolgt werden.

Symptom 3. Der IPsec-Tunnel ist ausgefallen und hält sich in einem Downstate auf

Wie bereits in diesem Symptom erwähnt, funktionierte der Tunnel vorher gut, aber aus jedem Grund kam er runter und der Tunnel konnte nicht wieder hergestellt werden. In diesem Szenario hat dies eine Auswirkung auf das Netzwerk.

Identifizieren Sie die Punkte, bevor die Fehlerbehebung beginnt:

1. IPsec-Tunnel (Nummer) mit Problemen und Konfiguration.
2. Der Zeitstempel, als der Tunnel ausfiel.
3. IPsec-Peer-IP-Adresse (Tunnelziel)

PFS-Nichtübereinstimmung

In diesem Beispiel beginnt die Fehlerbehebung nicht mit dem Zeitstempel, wenn der Tunnel ausfällt. Da das Problem weiterhin besteht, sind die IKE-Debugge die beste Option.

```
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

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
```

> **Hinweis:** CREATE_CHILD_SA-Pakete werden für jeden Schlüssel oder neue SA ausgetauscht. Weitere Referenzen finden Sie unter https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/115936-understanding-ikev2-packet-exch-debug.html

IKE-Debugger zeigen dasselbe Verhalten und werden fortlaufend wiederholt, sodass es möglich ist, einen Teil der Informationen zu übernehmen und zu analysieren:

CREATE_CHILD_SA ist ein Schlüssel, der dazu dient, das neue SPIS zu generieren und zwischen den IPsec-Endpunkten auszutauschen.

- Das vedge empfängt das CREATE_CHILD_SA-Anforderungspaket von 10.10.10.1.
- Der vEdge verarbeitet die Anfrage und verifiziert die vom Peer 10.10.10.1 gesendeten Vorschläge (SA).
- Der Vedge vergleicht das vom Peer gesendete erhaltene Angebot mit den konfigurierten Vorschlägen.
- Die ausgetauschte CREATE_CHILD_SA schlägt fehl, wenn "keine akzeptablen Vorschläge gefunden wurden".

An dieser Stelle stellt sich folgende Frage: **Warum besteht eine Konfigurationsungleichheit, wenn der Tunnel zuvor funktioniert hat und keine Änderungen vorgenommen wurden?**

Tief analysieren, gibt es ein zusätzliches Feld auf die konfigurierten Vorschläge, die der Peer nicht sendet.

konfigurierte Angebote: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_FF

Empfangene Angebote:
ESP:AES_GCM_16_256/NO_EXT_FF,
ESP: AES_CBC_256/HMAC_SHA1_96/NO_EXT_FF,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_FF,
ESP: AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_FF,
ESP: AES_CBC_128/HMAC_SHA1_96/NO_EXT_FF,
ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_FF

MODP_4096 ist die DH-Gruppe 16, die Vecken für PFS (Perfect-forward-Secrecy) in Phase 2 (IPsec-Abschnitt) konfiguriert hat.

PFS ist die einzige nicht übereinstimmende Konfiguration, in der der Tunnel erfolgreich

eingerichtet werden kann oder nicht, je nachdem, wer der Initiator oder der Responder in der IKE-Aushandlung ist. Wenn der Schlüssel startet, kann der Tunnel jedoch nicht weitergeführt werden, und dieses Symptom kann angezeigt oder in Zusammenhang damit stehen.

vEdge IPSec/IKEV2-Tunnel wird nach Abschaltung aufgrund eines DELETE-Ereignisses nicht erneut initiiert

Weitere Informationen zu diesem Verhalten finden Sie unter Cisco Bug ID CSCvx86427.

Da das Problem weiterhin besteht, sind die IKE-Debugs die besten Optionen. Für diesen speziellen Fehler, wenn Debug aktiviert ist, werden jedoch weder das Terminal noch die Nachrichtendatei angezeigt.

Um dieses Problem einzugrenzen und zu überprüfen, ob vEdge die Cisco Bug-ID CSCvx86427 trifft, muss der Zeitpunkt ermittelt werden, an dem der Tunnel ausfällt.

Identifizieren Sie die Punkte, bevor die Fehlerbehebung beginnt:

1. IPsec-Tunnel (Nummer) mit Problemen und Konfiguration.
2. Der Zeitstempel, als der Tunnel ausfiel.
3. IPsec-Peer-IP-Adresse (Tunnelziel)

Nachdem der Zeitstempel identifiziert und Zeit und Protokolle korreliert wurden, überprüfen Sie die Protokolle kurz bevor der Tunnel ausfällt.

```
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
```

> **Hinweis:** Bei einer IPsec-Aushandlung gibt es mehrere DELETES-Pakete, und die DELETE für CHILD_SA ist eine erwartete DELETE für einen REKEY-Prozess. Dieses Problem wird angezeigt, wenn ein reines IKE_SA DELETE-Paket ohne eine bestimmte IPsec-Aushandlung empfangen wird. Diese LÖSCHUNG entfernt den gesamten IPsec/IKE-Tunnel.