IKEv2を使用したvEdgeでのサービストンネルのIPsec問題のトラブルシューティング

内容

概要

このドキュメントでは、インターネットキーエクスチェンジ(IKEv2)が設定されているサードパーティデバイスへのインターネットプロトコルセキュリティ(IPsec)トンネルに関する最も一般的な問題をトラブルシューティングする方法について説明します。Cisco SD-WANのドキュメントでは、最も一般的にサービス/トランスポートトンネルとして参照されます。また、IKEデバッグを有効にして読み取り、パケット交換に関連付けて、IPSecネゴシエーションの障害ポイントを理解する方法についても説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IKEv2
- IPsecネゴシエーション
- Cisco SD-WAN

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

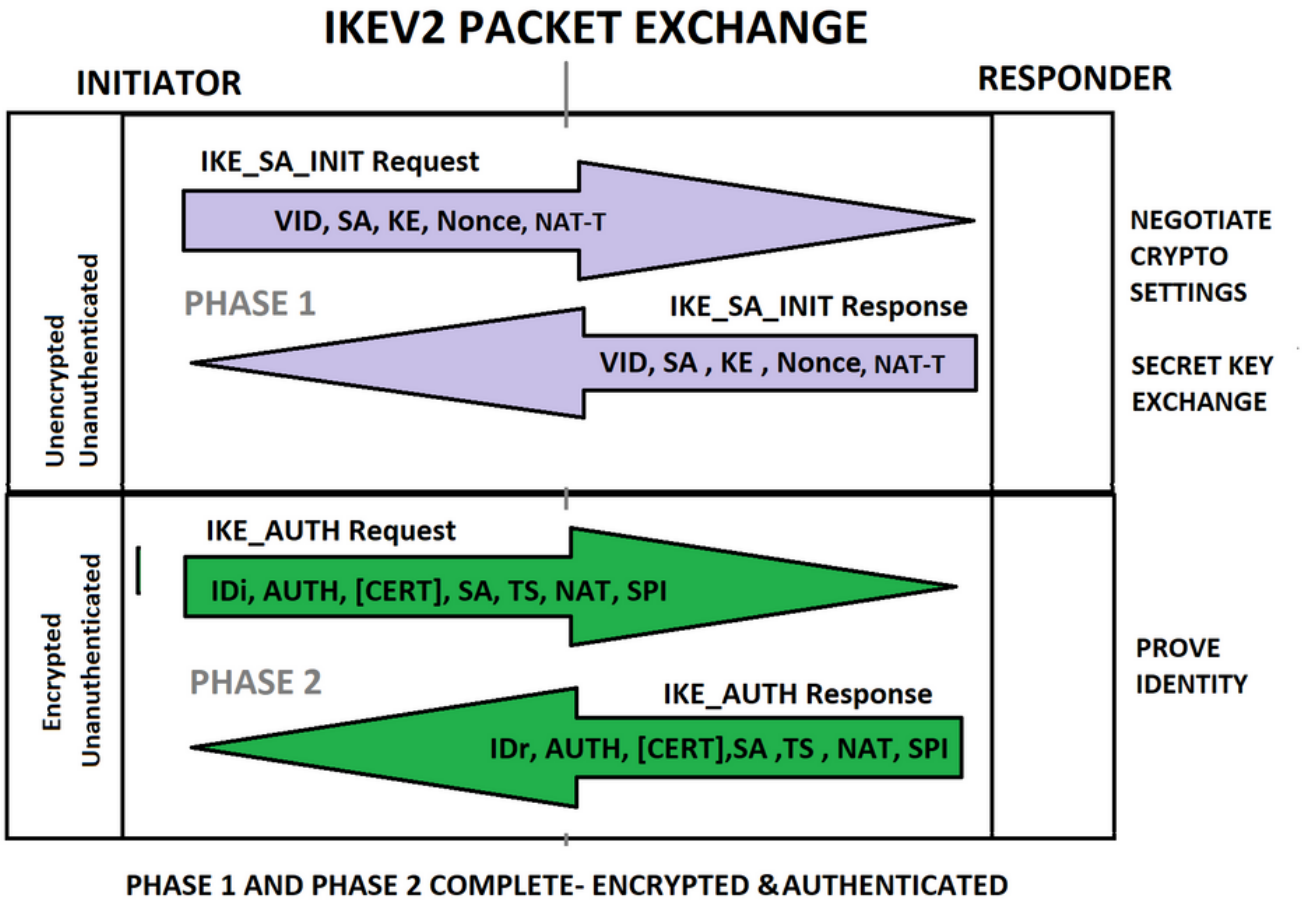
背景説明

IKE用語集

- **IPSec（Internet Protocol Security）**は、データ認証、整合性、および機密性を提供する、IPネットワーク上の2つの通信ポイント間の標準プロトコルスイートです。
- **Internet Key Exchange version 2(IKEv2)は、IPsecプロトコルスイートでセキュリティアソシエーション(SA)をセットアップするために使用されるプロトコルです。**
- セキュリ**ティアソシエーション**(SA)は、セキュアな通信をサポートするために、2つのネットワークエンティティ間で共有セキュリティ属性を確立することです。SAには、暗号化アルゴリズムやモードなどの属性を含めることができます。トラフィック暗号キー;接続を介して渡されるネットワークデータのパラメータ。
- ベンダー**ID(VID)**は、ベンダー固有の機能をサポートするために、同じベンダー実装のピアデバイスを識別するために使用されます。
- **Nonce:**ランダム性を高め、リプレイ攻撃を防ぐために、取引所で作成されるランダムな値。
- **Diffie-Hellman (**DH**)の**安全なキー交換プロセスのためのキー交換(KE)情報。
- Identity Initiator/responder(**IDi/IDr)は、ピアに認証情報を送信するために使用されます。**この情報は、共有秘密の保護の下で送信されます。
- IPSecの共有キーは、DHを使用して再度取得し、**Perfect Forward Secrecy(PFS)を保証する**か、元のDH交換から取得した共有秘密を更新することができます。
- **Diffie-Hellman (DH)キー交換は、パブリックチャネルを介して安全に暗号化アルゴリズムを交換する方法です。**
- **トラフィックセレクタ(TS)**は、暗号化されたトンネルを通過するためにIPSecネゴシエーションで交換されるプロキシIDまたはトラフィックです。

IKEv2パケット交換

各IKEパケットには、トンネル確立のためのペイロード情報が含まれます。IKE用語集では、パケット交換のペイロードコンテンツの一部として、この画像に示されている省略形について説明しています。

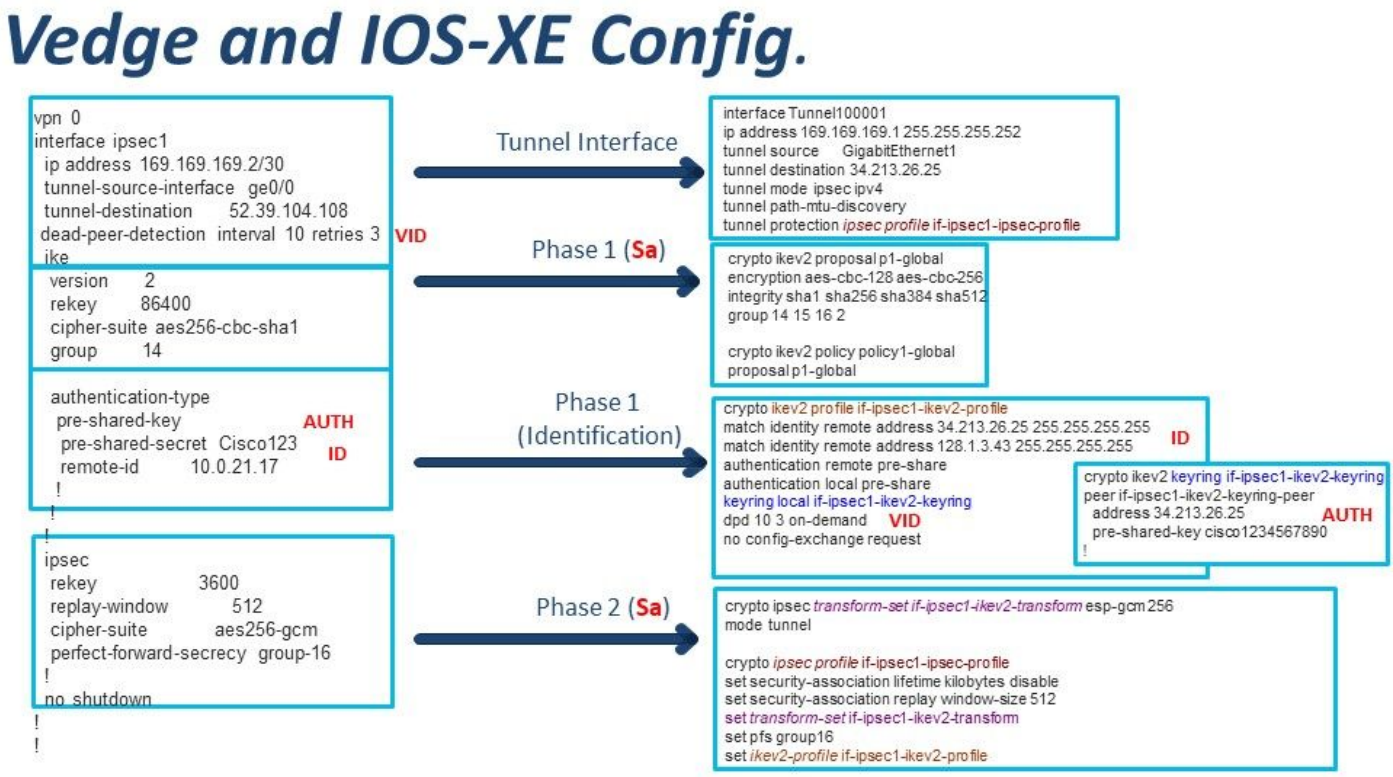


IKEV2-Exchange

注：IPSecトンネルがIKEネゴシエーションのどのパケット交換に失敗したかを確認し、問題に効果的に対処するために関係する設定をすばやく分析することが重要です。

注：このドキュメントでは、IKEv2パケット交換の詳細については説明しません。詳細については、「IKEv2 Packet Exchange」および「プロトコルレベルデバッグ」を参照してください

vEdge設定をCisco IOS® XE設定と関連付けるために必要です。また、図に示すように、IKEv2パケット交換のIPsecの概念とペイロードの内容を一致させると便利です。



注：設定の各部分は、IKEネゴシエーション交換の側面を変更します。コマンドをIPsecのプロトコルネゴシエーションに関連付けることが重要です。

トラブルシュート

IKEデバッグの有効化

vEdgesのデバッグイ**ンクを使用**すると、IKEv1またはIKEv2のいずれかのデバッグレベル情報が有効になります。

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

vshell内で現在のデバッグ情報を表示し、コマンドtail -f <debug path>を実行できます。

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

CLIでは、指定したパスの現在のログ/デバッグ情報を表示することもできます。

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

IPSec問題のトラブルシューティングプロセスを開始するためのヒント

3つの異なるIPsecシナリオを分離できます。症状を特定するには、より良いアプローチを持って始める方法を知ることが良い参照ポイントです。

1. IPsecトンネルが確立されない。
2. IPSecトンネルがダウンし、自身で再確立されました。（フラップ）

3. IPSecトンネルがダウンし、ダウン状態のままになる。

IPSecトンネルが症状を確立しない場合は、IKEネゴシエーションの現在の動作を確認するために、リアルタイムでデバッグする必要があります。

IPSecトンネルがダウンして、それ自体の症状で再確立した場合は、最も一般的にトンネルフラップと呼ばれ、根本原因分析(RCA)が必要です。トンネルがダウンした場合のタイムスタンプを知ることも、デバッグを確認する推定時間を持つことも不可欠です。

IPSecトンネルがダウンし、ダウン状態の症状が続く場合は、トンネルがダウンし、何らかの理由でトンネルがダウンした場合に、ティアダウンの理由と、トンネルが正常に確立されるのを妨げている現在の動作を知る必要があります。

トラブルシューティングを開始する前に、ポイントを特定します。

1. 問題と設定を含むIPsecトンネル（番号）。
2. トンネルがダウンしたときのタイムスタンプ（該当する場合）。
3. IPsecピアのIPアドレス（トンネルの宛先）。

すべてのデバッグと口グは/var/log/messagesファイルに保存され、現在の口グではmessagesファイルに保存されますが、この特定の症状の場合、フラップは問題の後に数時間または数日で特定できます。関連するデバッグのほとんどはmessages1、2、3..適切なメッセージファイルを確認し、IPsecトンネル関連のIKEネゴシエーションのデバッグ(chaon)を分析するためのタイムスタンプを知ることが重要です。

ほとんどのデバッグでは、IPsecトンネルの番号は出力されません。ネゴシエーションとパケットを識別する最も一般的な方法は、リモートピアのIPアドレスと、トンネルがエッジから送信されるIPアドレスです。IKEデバッグの出力例を次に示します。

```
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
```

IKE INITネゴシエーションのデバッグには、IPsecトンネル番号が表示されますが、パケット交換の後続の情報では、IPsecトンネルIPアドレスだけが使用されます。

```
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トンネル設定：

```
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 !
```

現象1. IPsecトンネルが確立されない

この問題はトンネルの最初の実装である可能性があるため、まだアップ状態ではなく、IKEデバッグが最適なオプションです。

現象2. IPSecトンネルがダウンし、自身で再確立された

前述したように、通常この症状は、トンネルがダウンした原因の根本原因を知るために取り上げられています。根本原因の分析が判明している場合、ネットワークの管理者が問題を回避することがあります。

トラブルシューティングを開始する前に、ポイントを特定します。

1. 問題と設定を含むIPsecトンネル（番号）。
2. トンネルがダウンしたときのタイムスタンプ。
3. IPsecピアのIPアドレス（トンネルの宛先）

DPD再送信

この例では、6月18日(00:31:17)にトンネルがダウンしています。

```
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
```

> **注：**IPsecトンネルダウンのログはデバッグの一部ではなく、FTMDログです。したがって、*charon*も*IKE*も*印刷*されません。

> **注：**関連するログは通常は一緒に印刷されず、同じプロセスに関連しない情報がログ間に表示されます。

ステップ1：タイムスタンプが特定され、時間とログが関連付けられた後、下から上にログのレビューを開始します。

```
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)
```

最後に成功したDPDパケット交換は、要求# 542として記述されます。

```
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 [ ]
```

ステップ2：すべての情報を正しい順序に並べます。

```
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
```

上記の例では、vEdge01が10.10.10.1からのDPDパケットを受信しないため、トンネルがダウンしています。これは、3つのDPD再送信後にIPsecピアが「lost」に設定され、トンネルがダウンすると予想されます。この動作には複数の理由があります。通常、これはパケットがパスで損失またはドロップされるISPに関連しています。問題が一度発生した場合、失われたトラフィックを追跡する方法はありませんが、問題が解決しない場合は、vEdge、リモートIPSecピア、およびISPのキャプチャを使用してパケットを追跡できます。

症状3:IPsecトンネルがダウンし、ダウン状態のままになる

この症状で前述したように、トンネルは正常に動作していましたが、何らかの理由でダウンし、トンネルが正常に確立されませんでした。このシナリオでは、ネットワークに影響があります。

トラブルシューティングを開始する前に、ポイントを特定します。

1. 問題と設定を含むIPsecトンネル（番号）。
2. トンネルがダウンしたときのタイムスタンプ。
3. IPsecピアのIPアドレス（トンネルの宛先）

PFSの不一致

この例では、トンネルがダウンしたときにタイムスタンプでトラブルシューティングが開始されません。問題が解決しない限り、IKEデバッグが最適なオプションです。

```
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
```

デバッグリンクが有効になり、ネゴシエーションが表示されます。

```
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
```

> **注：** CREATE_CHILD_SAパケットは、キー再生成または新しいSAごとに交換されます。詳細については、「IKEv2パケット交換について」を参照してください

IKEデバッグは同じ動作を示し、常に繰り返されるため、情報の一部を取得して分析することができます。

CREATE_CHILD_SAは、新しいSPISを生成してIPsecエンドポイント間で交換する目的を持つキー再生成を意味します。

- エッジは、10.10.10.1からCREATE_CHILD_SA要求パケットを受信します。
- エッジは要求を処理し、ピア10.10.10.1から送信されたプロポーザル(SA)を確認します
- エッジは、ピアから送信された受信したプロポーザルと、設定されたプロポーザルを比較します。
- 交換されたCREATE_CHILD_SAが「no acceptable proposal found」で失敗します。

この時点で、次のような問題が発生します。**トンネルが以前に動作していて、変更が行われていなかった場合、設定の不一致があるのはなぜですか。**

深く分析すると、ピアが送信していない設定済みのプロポーザルに追加フィールドがあります。

設定されたプロポーザル：ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ

受け取った提案：
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は、フェーズ2（IPsecセクション）のPFS(Perfect-forward-secrecy)に対してvedgeが設定されているDHグループ16です。

PFSは、トンネルが正常に確立できる、またはIKEネゴシエーションの発信側または応答側が誰であるかによって確立できない唯一の不一致の設定です。ただし、キー再生成が開始されると、トンネルは続行できず、この症状が発生したり、関連する可能性があります。

DELETEイベントが原因で切断された後にvEdge IPSec/Ikev2トンネルが再始動しない

この動作の詳細については、Cisco Bug ID CSCvx86427を参照してください。

この問題が発生すると、IKEデバッグが最適なオプションになります。ただし、デバッグが有効になっている場合、この特定の不具合に関して、ターミナルとメッセージファイルのどちらにも情報が表示されません。

この問題を絞り込み、vEdgeがCisco Bug ID CSCvx86427に該当するかどうかを確認するには、トンネルがダウンした瞬間を見つける必要があります。

トラブルシューティングを開始する前に、ポイントを特定します。

1. 問題と設定を含むIPsecトンネル（番号）。
2. トンネルがダウンしたときのタイムスタンプ。
3. IPsecピアのIPアドレス（トンネルの宛先）

タイムスタンプが特定され、時間とログが関連付けられた後、トンネルがダウンする直前のログを確認します。

```
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
```

> **注：** IPSecネゴシエーションには複数のDELETEパケットがあり、CHILD_SAのDELETEはREKEYプロセスに対して予期されるDELETEです。この問題は、純粋なIKE_SA DELETEパケットが特定のIPSecネゴシエーションなしで受信された時にに発生します。このDELETEによって、すべてのIPsec/IKEトンネルが削除されます。

関連情報

- KEv2パケット交換およびプロトコルレベルデバッグ
- インターネットキー交換(IKE):RFC 2409
- IKEv2:RFC 7296
- vEdgeとCisco IOS間のサイト間LAN間IPSec
- テクニカル サポートとドキュメント – Cisco Systems