IKEv2を使用したvEdge上のサービストンネルに関するIPSec問題のトラブルシューティング

内容

はじめに

このドキュメントでは、Internet Key Exchange version 2(IKEv2)が設定された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に関するドキュメントでは、サービス/トランスポートトンネルと呼ばれることが最も一般的です。また、IPsecネゴシエーションの障害ポイント(POP)を理解するために、IKEデバッグをイネーブルにして読み取り、デバッグをパケット交換に関連付け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、クリアな（デフォルト）設定で作業を開始しています。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。

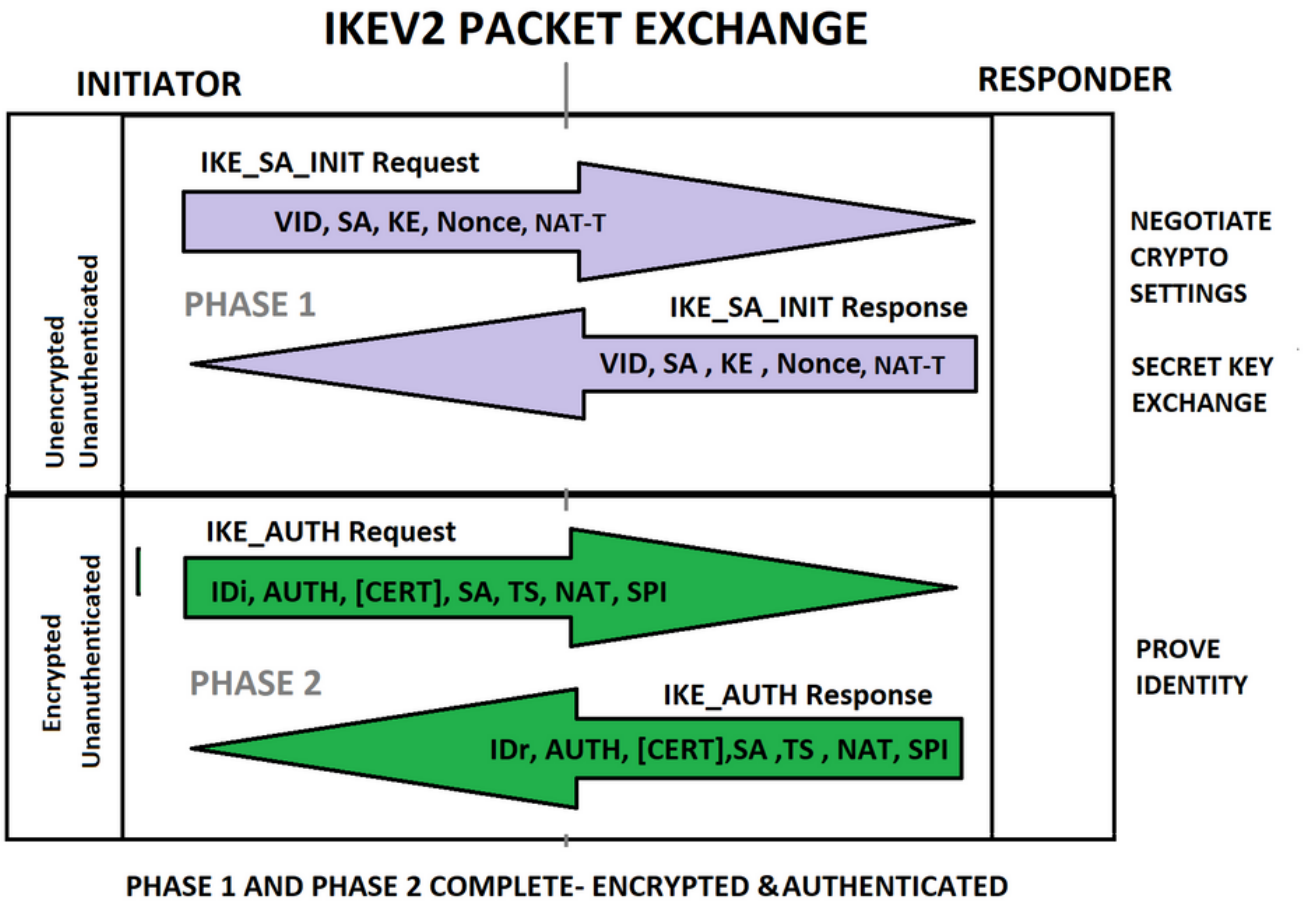
背景説明

IKE用語集

- インターネットプロトコルセキュリティ(IPsec)は、IPネットワーク上の2つの通信ポイント間でデータの認証、整合性、機密性を提供するプロトコルの標準スイートです。
- インターネットキーエクスチェンジバージョン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される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暗号化モード、トラフィック暗号化キー、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などの属性を含めることができます。
- 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、同じベンダー実装を持つピアデバイスを識別するために使用されます。
- ナンス：ランダム性を付加し、リプレイアタックを防止するために交換で作成されるランダムな値。
- Diffie-Hellman(DH)セキュア鍵交換プロセスの鍵交換(KE)情報。
- ピアに認証情報を送信するために、IDイニシエータ/レスポンダ(IDi/IDr)が使用されます。この情報は、共通共有秘密の保護の下で送信されます。
- IPSec共有キーは、DHを再度使用してPerfect Forward Secrecy(PFS)を確保するか、元のDH交換から取得した共有シークレットを更新することで取得できます。
- Diffie-Hellman(DH)鍵交換は、公衆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、トンネルを確立するためのペイロード情報が含まれています。IKE用語集では、パケット交換のペイロードの内容の一部として、この図に示されている省略形について説明します。



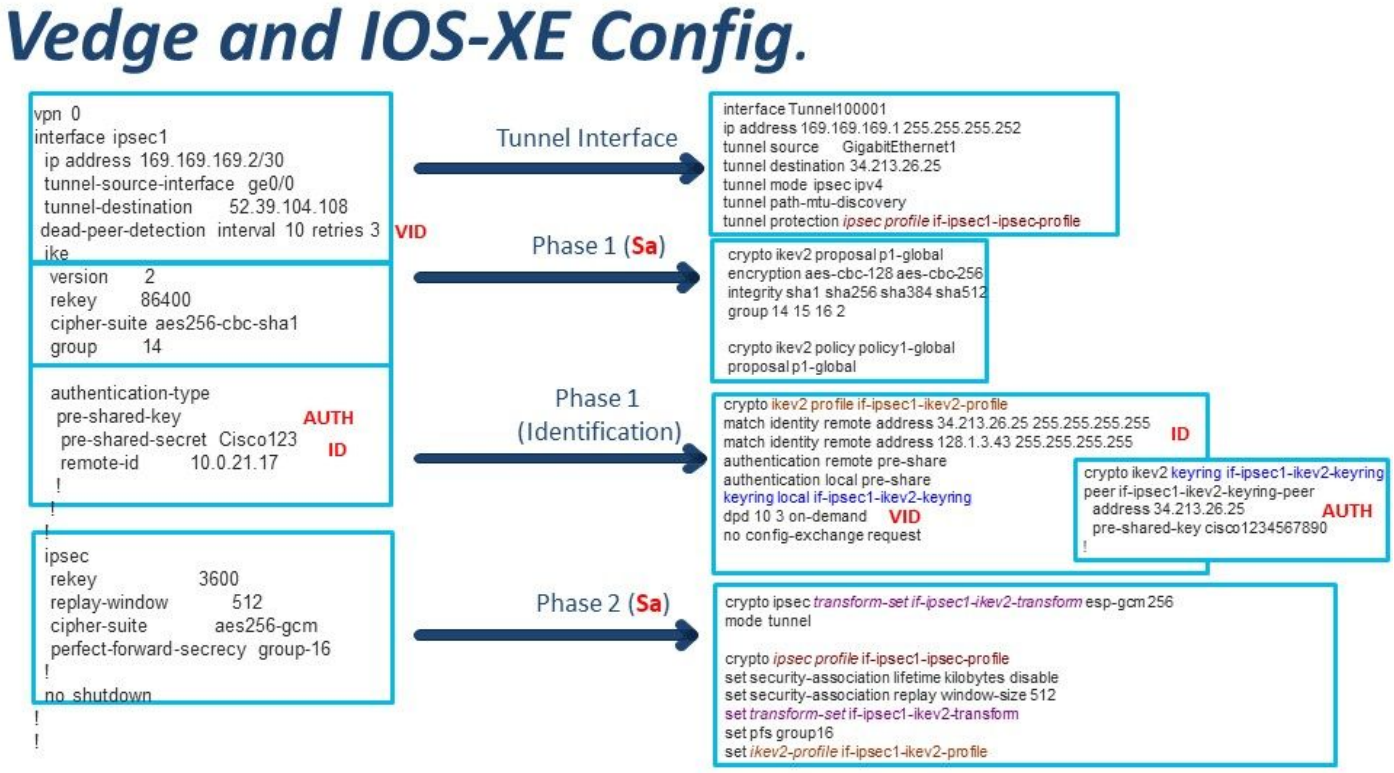
IKEV2交換

注:IKEネゴシエーションのパケット交換について、問題に効果的に対処するためにどの設定が関係しているかをIPSecトンネルが迅速に分析していないことを確認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ていません。詳細については、「IKEv2のパケット交換と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設定に関連付ける必要があります。また、図に示すように、IPsecの概念とIKEv2パケット交換のペイロードの内容を照合することも有効です。



注：設定の各部分では、IKEネゴシエーション交換の側面が変更されます。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では、debug ikedにより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>を実行することができます。

```
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に関する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シナリオを分離することができます。症状を特定する上で、より適切な方法で始める方法を知ることは、良い参照点となります。

1. IPSecトンネルが確立されない。
2. IPSecトンネルがダウンし、自動的に再確立されました。（フラップ）
3. IPSecトンネルがダウンしても、ダウン状態のままである。

IPSecトンネルで症状が確立されない場合、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、それ自体の症状で再確立された場合、最も一般的に知られているのはトンネルフラップで、根本原因分析(RCA)が必要です。トンネルがダウンした時点のタイムスタンプを知るか、デバッグを確認する推定時間を知ることは不可欠です。

IPSecトンネルがダウンして「down」状態のままである場合、これはトンネルが以前は稼働していたことを意味しますが、何らかの理由でダウンした場合は、ダウンの理由と、トンネルが再度正常に確立されない現在の動作を把握する必要があります。

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. 問題と設定があるIPsecトンネル（番号）。
2. トンネルがダウンした時点のタイムスタンプ（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ており、現在の口グの場合はmessagesファイルに保存されていますが、この特定の症状の場合は、問題が発生した数時間後または数日後にフラップが特定される可能性があります。関連するデバッグのほとんどは、messages1、2、3などで発生します。タイムスタンプを知ることは、正しいメッセージファイルを参照し、関連するIPSecトンネルのIKEネゴシエーションのデバッグ(charon)を分析するために重要です。

ほとんどのデバッグでは、IPSecトンネルの番号は表示されません。ネゴシエーションとパケットを特定する最も一般的な方法は、リモートピアのIPアドレスと、トンネルの発信元であるvedge上のIPアドレスを使用する方法です。IKEデバッグの出力例の一部を次に示します。

```
<#root>

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では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。

<#root>

```
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
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_
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
Jun 18 00:31:22 vedge01 charon: 12[IKE] local host is behind NAT, sending keep alives
```

IPSecトンネルの設定：

```
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/Cw6tXOna34yF4FgaOB62mGBpHFdOzFaRmoYfnBioWVO3s3efFPBbkaZqvoN
    !
   !
  !
  ipsec
   rekey                    3600
   replay-window            512
   cipher-suite             aes256-gcm
   perfect-forward-secrecy group-14
  !
```

症状1. IPSecトンネルが確立されない

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。

症状2:IPSecトンネルがダウンし、トンネル自体が再確立された

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特定するために対処します。根本原因の分析が判明している場合は、ネットワークの管理者がそれ以上の問題を防ぐことがあります。

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. 問題と設定がある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日の00:31:17にトンネルがダウンしています。

<#root>

```
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
```

注:IPSecトンネルダウンのログはikedデバッグのログではなく、FTMDログです。したがって、charonとIKEのどちらも出力されません。

注：関連するログは通常一緒に出力されません。同じプロセスに関連しない詳細な情報がログ間にあります。

ステップ 1：タイムスタンプが特定され、時刻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
```

```
<#root>

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
```

```
<#root>

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
```

```
<#root>

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
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3, timeout=3
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

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。

```
<#root>

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
```

```
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 13.51.17.190[4500] to 10.10.10.1[4500] (7
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まとめます。

```
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
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to 10.132.3.92[4500] (76
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
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3, timeout=3
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76

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

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

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-stat
```

この例では、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ます。3つのDPDが再送信された後、IPsecピアが「lost」に設定され、トンネルがダウンすることが予想されます。この動作には複数の原因があり、通常は、パケットがパスで失われたりドロップされたりするISPに関連しています。問題が1回発生すると、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。

現象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、トンネルは以前は正常に動作していましたが、何らかの理由でダウンしてしまい、トンネルを再確立できませんでした。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. 問題と設定がある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際のタイムスタンプではトラブルシューティングが開始されません。問題が解決しない場合は、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 "$8$njK2pLLjgKWNQuOKecNtY3+fo3hbTsO/7iJy6unNtersmCGjGB38kIPjsoqqXZdVmtizLu79\naQ
    !
   !
  !
  ipsec
   rekey                    3600
   replay-window            512
   cipher-suite             aes256-cbc-sha1
   perfect-forward-secrecy group-16
  !
  mtu                      1400
  no shutdown
```

デバッグキーが有効になり、ネゴシエーションが表示されます。

<#root>

```
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] received packet: from 10.10.10.1[4500] to 172.28.0
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,
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96
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_PRO
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] sending packet: from 172.28.0.36[4500] to 10.10.10

daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] received packet: from 10.10.10.1[4500] to 172.28.0
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
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to 172.28.0
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

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、キー再生成ごとまたは新しい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はキー再生成を意味し、IPSecエンドポイント間で新しいSPIが生成され、交換されることを目的としています。

- vedgeが10.10.10.1からCREATE_CHILD_SA要求パケットを受信します。
- vedgeは要求を処理し、ピア10.10.10.1によって送信されたプロポーザル(SA)を確認します。
- vedgeは、ピアから送信された受信したプロポーザルを、自身に設定されているプロポーザルと比較します。
- 交換されたCREATE_CHILD_SAが「no acceptable proposals found」で失敗する。

この時点で問題になるのは、以前にトンネルが動作していて、変更が行われていないときに、設定の不一致が発生している理由です。

詳細な分析を行うと、設定されたプロポーザルに対して、ピアから送信されていないフィールドが余分に存在することになります。

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DHグループ16であり、vedgeがフェーズ2（IPsecセクション）でPFS(perfect-forward-secrecy)を設定しています。

PFSは、IKEネゴシエーションの発信側または応答側に基づいてトンネルを正常に確立できるかどうかが決まる、唯一の不一致設定です。ただし、キー再生成が開始されるとトンネルを続行できなくなり、この症状が発生するか、関連している可能性があります。

DELETEイベントによるティアダウン後に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。

この問題が解決しない場合は、IKEデバッグが最適なオプションです。ただし、この特定のバグに対してデバッグが有効になっている場合、ターミナルもメッセージファイルも情報は表示されません。

この問題を絞り込み、vEdgeがCisco Bug ID CSCvx86427に一致するかどうかを確認するには、トンネルがダウンする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. 問題と設定がある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、時刻とログが関連付けられた後、トンネルがダウンする直前にログを確認します。

<#root>

```
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
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
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 by
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
```

注：IPSecネゴシエーション上には複数のDELETEパケットが存在し、CHILD_SAに対するDELETEはキー再生成プロセスで想定されるDELETEです。この問題は、特定のIPSecネゴシエーションが行われずに純粋なIKE_SA DELETEパケットが受信された場合に発生します。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パケット交換とプロトコルレベルデバッグ
- インターネットキーエクスチェンジ(IKE):RFC 2409
- IKEv2 - RFC 7296

- vEdgeとCisco IOS間のサイト間LAN-to-LAN IPSec
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。