Identificar e Solucionar Problemas de IPsec para Túneis de Serviço em Bordas com IKEv2

Contents

Introduction

Este documento descreve como solucionar os problemas mais comuns de túneis de segurança de protocolo Internet (IPsec) para dispositivos de terceiros com Internet Key Exchange versão 2 (IKEv2) configurada. Mais comumente referenciado como Túneis de Serviço/Transporte na documentação do Cisco SD-WAN. Este documento também explica como habilitar e ler depurações de IKE e associá-las à troca de pacotes para entender o ponto de falha em uma negociação de IPsec.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- IKEv2
- negociação de IPsec
- Cisco SD-WAN

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

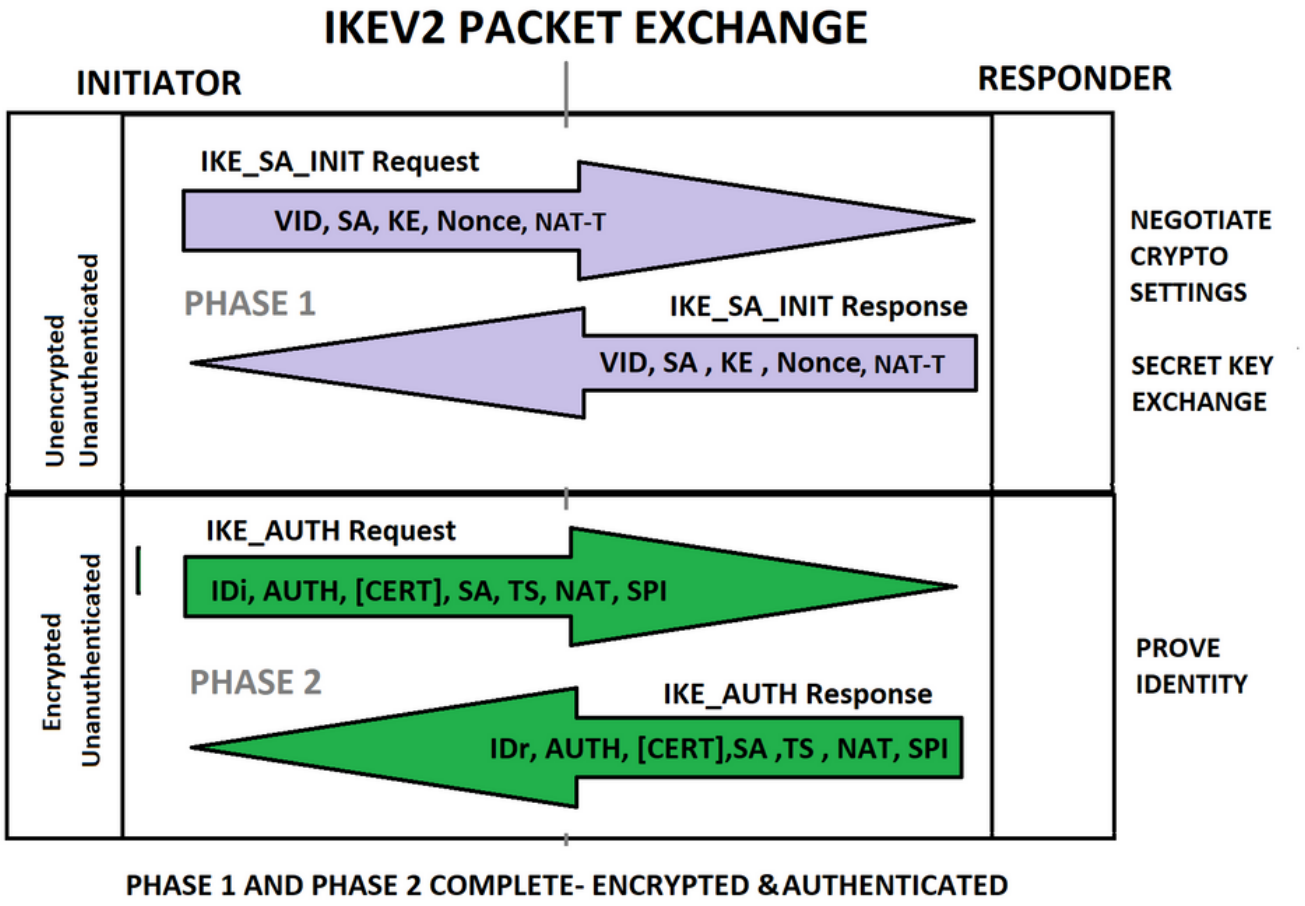
Informações de Apoio

Glossário IKE

- **Segurança de Protocolo de Internet (IPsec)** é um conjunto padrão de protocolos entre 2 pontos de comunicação na rede IP que fornece autenticação de dados, integridade e confidencialidade.
- **Internet Key Exchange versão 2 (IKEv2) é o protocolo usado para configurar uma associação de segurança (SA) no conjunto de protocolos IPsec.**
- Uma **associação de segurança** (**SA**) é o estabelecimento de atributos de segurança compartilhados entre duas entidades de rede para dar suporte à comunicação segura. Um SA pode incluir atributos como algoritmo criptográfico e modo; chave de encriptação de tráfego; e parâmetros para que os dados da rede passem pela conexão.
- As **IDs de fornecedor** (**VID**) são usadas para identificar dispositivos de mesmo nível com a mesma implementação de fornecedor para oferecer suporte a recursos específicos do fornecedor.
- **Nonce**: valores aleatórios criados na troca para adicionar aleatoriedade e impedir ataques de repetição.
- Informações **de troca de chaves (KE)** para o processo seguro de troca de chaves Diffie-Hellman (DH).
- **O Identity Initiator/responder (IDi/IDr.)** é usado para enviar informações de autenticação ao peer. Estas informações são transmitidas sob a proteção do segredo comum partilhado.
- A chave compartilhada IPSec pode ser derivada com o uso de DH novamente para garantir o **Perfect Forward Secret (PFS)** ou com uma atualização do segredo compartilhado derivado da troca DH original.
- A **troca de chaves Diffie-Hellman (DH)** é um método de troca segura de algoritmos criptográficos em um canal público.
- **Seletores de tráfego (TS)** são as identidades de proxy ou o tráfego trocado na negociação IPsec para passar pelo túnel criptografado.

Troca de pacotes IKEv2

Cada pacote IKE contém informações de payload para o estabelecimento do túnel. O glossário IKE explica as abreviações mostradas nesta imagem como parte do conteúdo da carga útil para a troca de pacotes.

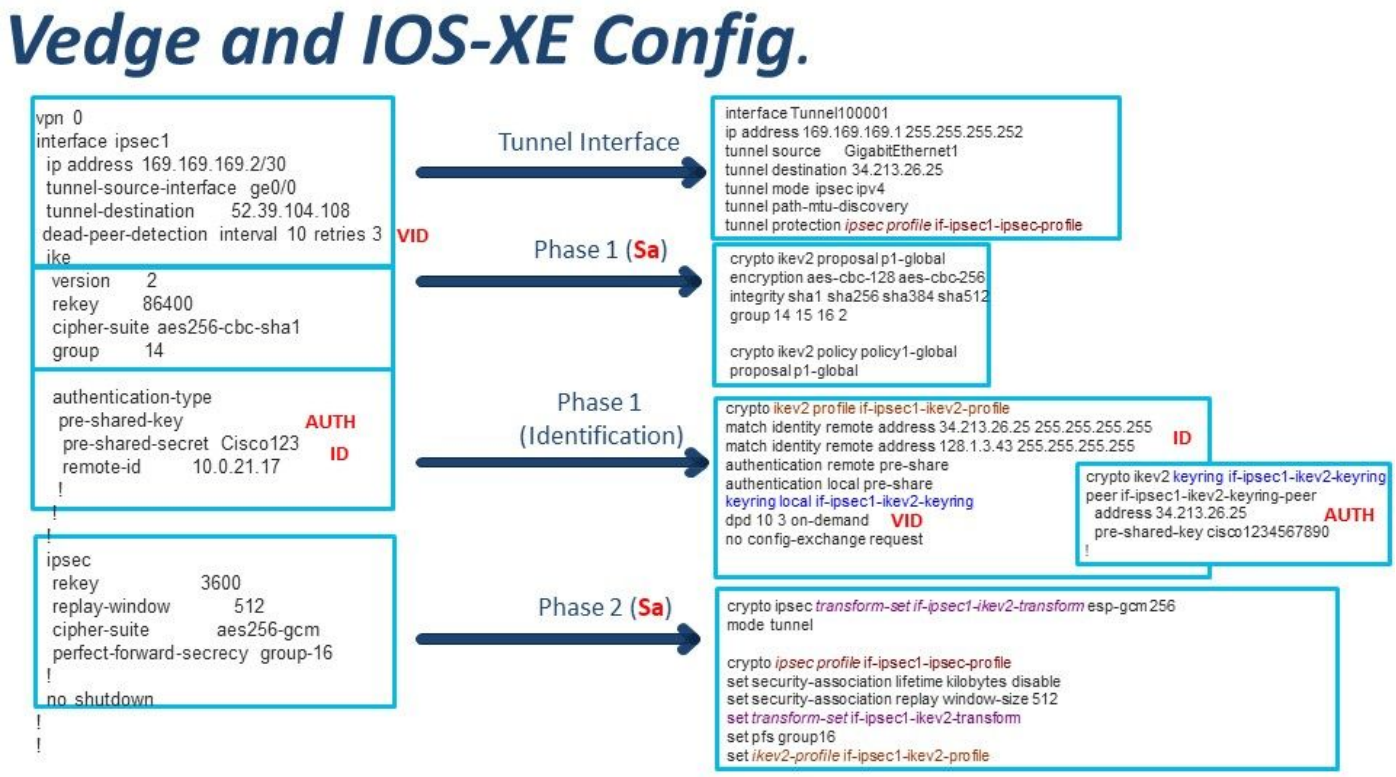


IKEV2-Exchange

> **Note**: É importante verificar em que troca de pacotes da negociação IKE o túnel IPsec não consegue analisar rapidamente qual configuração está envolvida para resolver o problema de forma eficaz.

> **Note:** Este documento não descreve mais profundamente a troca de pacotes IKEv2. Para obter mais referências, navegue até IKEv2 Packet Exchange e Protocol Level Debugging

Énecessário correlacionar a configuração do vEdge com a configuração do Cisco IOS® XE. Além disso, é útil combinar os conceitos de IPsec e o conteúdo de payload para trocas de pacotes IKEv2 como mostrado na imagem.



Note: Cada parte da configuração modifica um aspecto da troca de negociação IKE. É importante correlacionar os comandos à negociação de protocolo de IPsec.

Troubleshoot

Habilitar depurações de IKE

No vEdges **debug iked** habilita as informações de nível de depuração de IKEv1 ou IKEv2.

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

É possível exibir as informações de depuração atuais no **vshell** e executar o comando **tail -f <debug path>**.

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

Na CLI, também é possível exibir os logs/informações de depuração atuais do caminho especificado.

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

Dicas para iniciar o processo de solução de problemas de IPsec

Épossível separar três cenários IPsec diferentes. É um bom ponto de referência para identificar o sintoma para ter uma melhor abordagem para saber como começar.

1. O túnel IPsec não é estabelecido.

2. O túnel IPsec caiu e foi restabelecido sozinho. (Flapped)
3. O túnel IPsec caiu e permanece em estado inativo.

Para que o túnel IPsec não estabeleça sintomas, é necessário depurar em tempo real para verificar qual é o comportamento atual na negociação de IKE.

Para o túnel IPsec caiu e foi restabelecido em seus próprios sintomas, mais comumente conhecido como túnel Flapped e a análise da causa raiz (RCA) é necessária. É indispensável saber o timestamp quando o túnel caiu ou ter um tempo estimado para examinar as depurações.

Para o túnel IPsec desligado e permanece em sintomas de estado de inatividade, significa que o túnel funcionou antes, mas por qualquer motivo, ele desceu e precisamos saber o motivo do desligamento e o comportamento atual que impede que o túnel seja estabelecido com sucesso novamente.

Identifique os pontos antes do início da solução de problemas:

1. Túnel IPsec (Número) com problemas e configuração.
2. O carimbo de data e hora quando o túnel caiu (se aplicável).
3. IPsec peer IP address (destino do túnel).

Todas as depurações e registros são salvos em arquivos **/var/log/messages**, para os registros atuais, eles são salvos no arquivo de mensagens, mas para esse sintoma específico, o flap pode ser identificado horas/dias após o problema, provavelmente as depurações relacionadas estariam em mensagens1, 2, 3, etc. É importante saber o timestamp para examinar o arquivo de mensagem correto e analisar as depurações (charon) para a negociação IKE do túnel IPsec relacionado.

A maioria das depurações não imprime o número do túnel IPsec. A maneira mais frequente de identificar a negociação e os pacotes é com o endereço IP do peer remoto e o endereço IP onde o túnel é originado na borda. Alguns exemplos de depurações de IKE impressas:

```
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
```

As depurações da negociação IKE INIT mostram o número do túnel IPsec. Entretanto, as informações subsequentes para troca de pacotes usam apenas os endereços IP do túnel IPsec.

```
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
```

Configuração de túnel IPsec:

```
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 !
```

Sintoma 1. O túnel IPsec não é estabelecido

Como o problema pode ser a primeira implementação para o túnel, ele não foi ativado e as depurações de IKE são a melhor opção.

Sintoma 2. O túnel IPsec caiu e foi restabelecido por conta própria

Como mencionado anteriormente, geralmente esse sintoma é endereçado para saber a causa raiz do motivo pelo qual o túnel caiu. Com a análise da causa básica conhecida, às vezes, o administrador da rede evita mais problemas.

Identifique os pontos antes do início da solução de problemas:

1. Túnel IPsec (Número) com problemas e configuração.
2. O carimbo de data e hora quando o túnel caiu.
3. Endereço IP do peer IPsec (destino do túnel)

Retransmissões DPD

Neste exemplo, o túnel caiu em 18 de junho às 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
```

> **Note**: Os registros para o túnel IPsec inativo não fazem parte de depurações ligadas, são registros *FTMD*. Portanto, nem *charon* nem *IKE* seriam impressos.

> **Note**: Os registros relacionados geralmente não são impressos em conjunto, há mais informações entre eles não relacionadas ao mesmo processo.

Etapa 1. Depois que o carimbo de data/hora for identificado e a hora e os registros estiverem correlacionados, comece a revisar os registros de baixo para cima.

```
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)
```

A última troca de pacotes DPD bem-sucedida é descrita como solicitação nº 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 [ ]
```

Etapa 2. Junte todas as informações na ordem correta:

```
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
```

Para o exemplo descrito, o túnel cai devido ao vEdge01 não receber os pacotes DPD de 10.10.10.1. Ele é esperado após 3 retransmissões DPD, o peer IPsec é definido como "perdido" e o túnel é desativado. Há várias razões para esse comportamento, geralmente, ele está

relacionado ao ISP onde os pacotes são perdidos ou descartados no caminho. Se o problema ocorrer uma vez, não há como rastrear o tráfego perdido, no entanto, se o problema persistir, o pacote poderá ser rastreado com o uso de capturas no vEdge, no peer remoto de IPSec e no ISP.

Sintoma 3. O túnel IPsec caiu e permanece em estado de inatividade

Como mencionado anteriormente neste sintoma, o túnel funcionava normalmente, mas por qualquer razão, desceu e o túnel não pôde ser estabelecido novamente com sucesso. Nesse cenário, há um efeito na rede.

identifique os pontos antes do início da solução de problemas:

1. Túnel IPsec (Número) com problemas e configuração.
2. O carimbo de data e hora quando o túnel caiu.
3. Endereço IP do peer IPsec (destino do túnel)

Incompatibilidade de PFS

Neste exemplo, a solução de problemas não começa com o carimbo de data e hora quando o túnel cai. À medida que o problema persiste, as depurações de IKE são a melhor opção.

```
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
```

O campo debug iked está ativado e a negociação é exibida.

```
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
```

> **Observação:** os pacotes CREATE_CHILD_SA são trocados por cada chave nova ou SA nova. Para obter mais referências, navegue até Understanding IKEv2 Packet Exchange (Compreendendo o Intercâmbio de Pacotes IKEv2)

As depurações de IKE mostram o mesmo comportamento e são repetidas constantemente, de modo que é possível pegar uma parte das informações e analisá-las:

CREATE_CHILD_SA significa um rechaveamento, com a finalidade de que o novo SPIS seja gerado e trocado entre os endpoints IPsec.

- A borda recebe o pacote de solicitação CREATE_CHILD_SA de 10.10.10.1.
- O vedge processa a solicitação e verifica as propostas (SA) enviadas pelo peer 10.10.10.1
- A diferença compara a proposta recebida enviada pelo peer com suas propostas configuradas.
- A troca CREATE_CHILD_SA falhou com " nenhuma proposta aceitável encontrada".

Neste ponto, a questão é: **Por que há uma incompatibilidade de configuração se o túnel funcionou anteriormente e nenhuma alteração foi feita?**

Analisar profundamente, há um campo extra nas propostas configuradas que o peer não está enviando.

propostas configuradas: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ

Propostas recebidas:
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 é o grupo DH 16, que as bordas configuraram para PFS (perfeito para encaminhamento de sigilo) na fase 2 (seção IPsec).

O PFS é a única configuração de incompatibilidade na qual o túnel pode ser estabelecido com êxito ou não de acordo com quem é o iniciador ou respondente na negociação IKE. No entanto, quando a chave rekey inicia, o túnel não pode continuar e esse sintoma pode ser apresentado ou relacionado a ele.

O túnel vEdge IPSec/Ikev2 não é reiniciado após ser desligado devido a um evento de EXCLUSÃO

Consulte o bug da Cisco ID CSCvx86427 para obter mais informações sobre esse comportamento.

Conforme o problema persiste, as depurações de IKE são as melhores opções. No entanto, para esse bug específico se as depurações estiverem habilitadas, nenhuma informação será exibida nem no terminal nem no arquivo de mensagem.

Para reduzir esse problema e verificar se o vEdge atinge o bug da Cisco ID CSCvx86427, é necessário encontrar o momento em que o túnel cai.

identifique os pontos antes do início da solução de problemas:

1. Túnel IPsec (Número) com problemas e configuração.
2. O carimbo de data e hora quando o túnel caiu.
3. Endereço IP do peer IPsec (destino do túnel)

Depois que o carimbo de data/hora for identificado e o tempo e os registros estiverem correlacionados, revise os registros logo antes de quando o túnel cair.

```
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
```

> **Observação:** há vários pacotes DELETES em uma negociação IPsec e DELETE para CHILD_SA é uma DELETE esperada para um processo REKEY, esse problema é visto quando um pacote IKE_SA DELETE puro é recebido sem nenhuma negociação IPsec específica. Essa EXCLUSÃO remove todo o túnel IPsec/IKE.

Informações Relacionadas

- Intercâmbio de pacote KEv2 e depuração de nível de protocolo
- O Internet Key Exchange (IKE) - RFC 2409
- IKEv2 - RFC 7296
- IPSec de LAN para LAN entre vEdge e Cisco IOS
- Suporte Técnico e Documentação - Cisco Systems