IKEv2를 사용하여 vEdge에서 서비스 터널에 대한 IPsec 문제 해결

목차

소개

이 문서에서는 IKEv2(Internet Key Exchange version 2)가 구성된 서드파티 디바이스로의 IPsec(Internet Protocol Security) 터널에 대한 가장 일반적인 문제를 해결하는 방법에 대해 설명합니다. Cisco SD-WAN 설명서에서 Service/Transport Tunnels로 가장 일반적으로 참조됩니다. 이 문서에서는 IKE 디버그를 활성화 및 읽고 패킷 교환에 연결하여 IPsec 협상의 장애 지점을 파악하는 방법에 대해서도 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IKEv2
- IPsec 협상
- Cisco SD-WAN

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

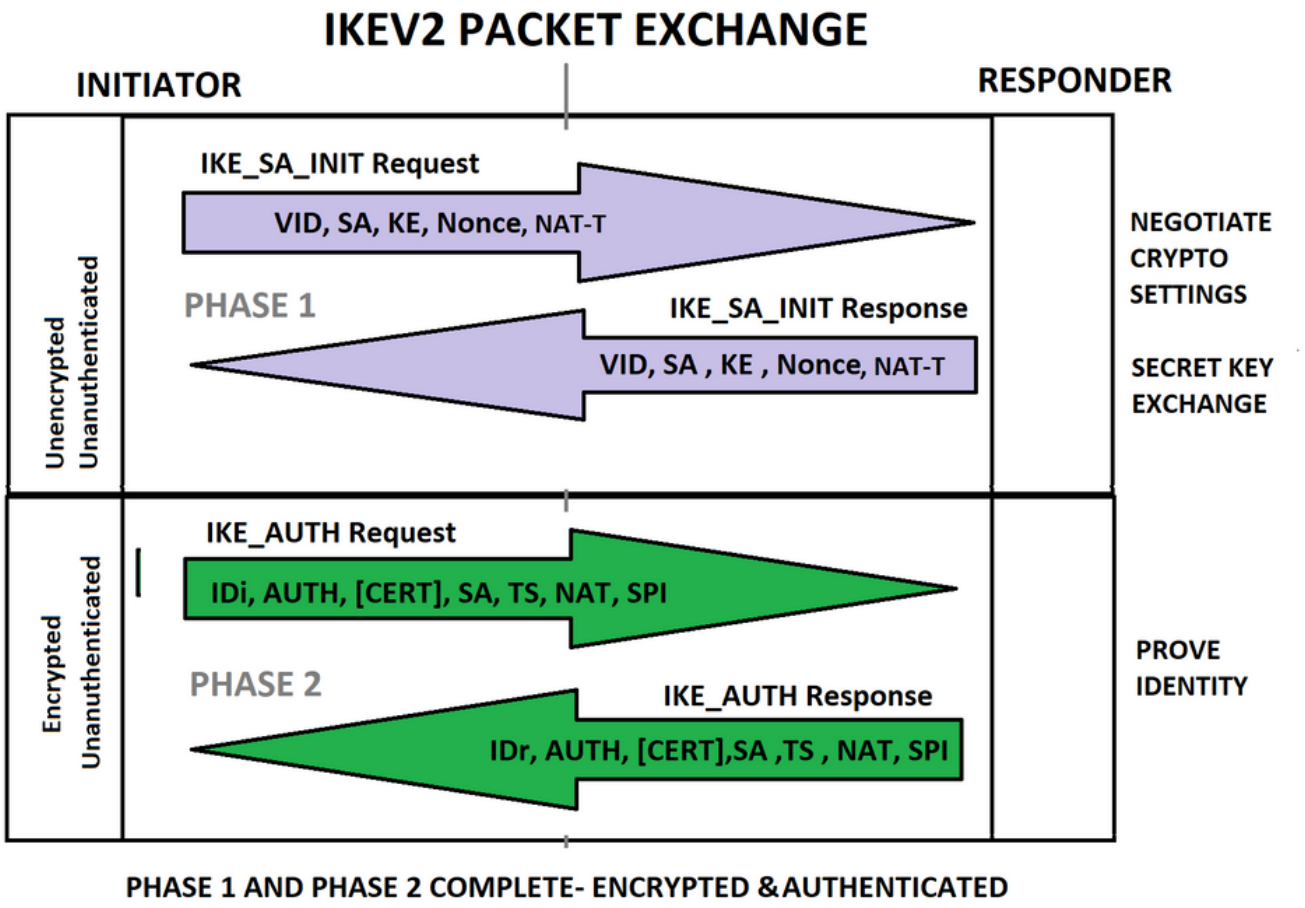
배경 정보

IKE 용어집

- **IPsec(인터넷 프로토콜 보안)** 는 데이터 인증, 무결성 및 기밀성을 제공하는 IP 네트워크 전반의 2개 통신 지점 간의 표준 프로토콜 모음입니다.
- **IKEv2(Internet Key Exchange version 2)는 IPsec 프로토콜 제품군에서 SA(Security Association)를 설정하는 데 사용되는 프로토콜입니다.**
- SA(**Security Association**)**는** 보안 통신을 지원하기 위해 두 네트워크 엔터티 간의 공유 보안 특성을 설정하는 것입니다. SA에는 암호화 알고리즘 및 모드와 같은 특성이 포함될 수 있습니다. 트래픽 암호화 키 연결을 통해 전달되는 네트워크 데이터의 매개 변수입니다.
- 공급업체 **ID**(**VID**)는 벤더별 기능을 지원하기 위해 공급업체 구현이 동일한 피어 디바이스를 식별하는 데 사용됩니다.
- **Nonce**: 임의 설정을 추가하고 재생 공격을 방지하기 위해 exchange에 생성된 임의의 값.
- **DH**(**Diffie**-Hellman) 보안 키 교환 프로세스에 대한 **KE(Key-Exchange)** 정보
- **ID Initiator/responder(IDi/IDr)**는 피어로 인증 정보를 보내는 데 사용됩니다. 이 정보는 공통 공유 비밀을 보호하여 전송됩니다.
- IPSec 공유 키는 DH를 다시 사용하여 PFS**(Perfect Forward Secrecy)**를 보장하거나 원래 DH 교환에서 파생된 공유 암호를 새로 고침하여 파생될 수 있습니다.
- **DH(Diffie-Hellman) 키 교환은 공용 채널을 통해 안전하게 암호화 알고리즘을 교환하는 방법입니다.**
- **TS(Traffic Selectors)**는 암호화된 터널을 통과하기 위해 IPsec 협상에서 교환되는 프록시 ID 또는 트래픽입니다.

IKEv2 패킷 교환

각 IKE 패킷에는 터널 설정에 대한 페이로드 정보가 포함됩니다. IKE 용어집에서는 이 이미지에 패킷 교환에 대한 페이로드 콘텐츠의 일부로 표시되는 약어를 설명합니다.

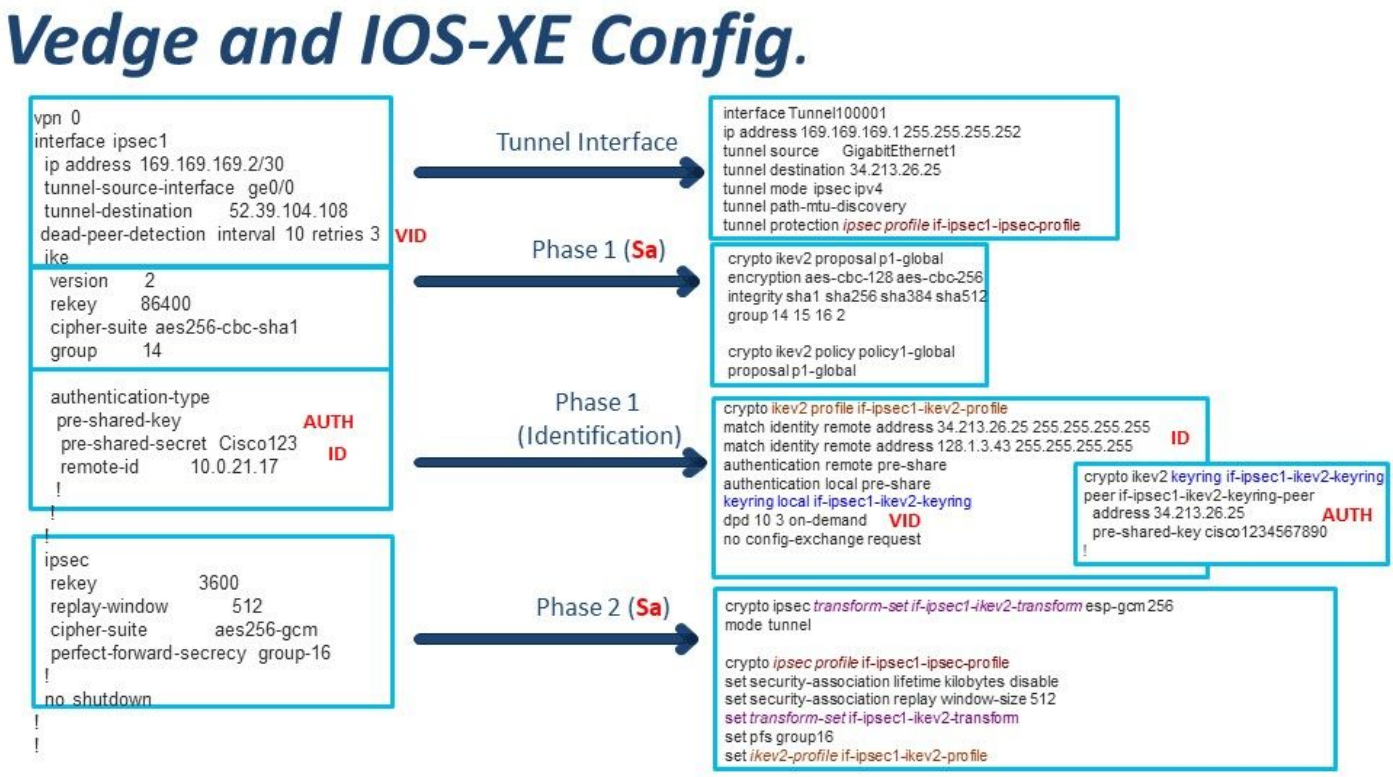


IKEV2-Exchange

> **참고:** IPsec 터널이 어떤 컨피그레이션과 관련된 컨피그레이션을 신속하게 분석하여 문제를 효과적으로 해결할 수 없는 IKE 협상의 패킷 교환을 확인해야 합니다.

> **참고:** 이 문서에서는 IKEv2 패킷 교환에 대해 자세히 설명하지 않습니다. 추가 참조를 보려면 IKEv2 Packet Exchange 및 Protocol Level Debugging으로 이동합니다.

vEdge 컨피그레이션과 Cisco IOS® XE 컨피그레이션의 상관관계를 분석해야 합니다. 또한 이미지에 표시된 대로 IKEv2 패킷 교환에 대한 IPsec 개념 및 페이로드 콘텐츠를 일치시키는 것이 유용합니다.



참고: 컨피그레이션의 각 부분은 IKE 협상 교환의 측면을 수정합니다. 이 명령을 IPsec의 프로토콜 협상에 연계하는 것이 중요합니다.

문제 해결

IKE 디버깅 사용

vEdges **debug**(vEdge **디버그**)는 IKEv1 또는 IKEv2 중 하나의 디버그 레벨 정보를 활성화합니다.

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

vshell 내에 현재 디버그 정보를 표시하고 **tail -f <debug path>** 명령을 실행할 수 있습니다.

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

CLI에서는 지정된 경로에 대한 현재 로그/디버그 정보를 표시할 수도 있습니다.

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

IPsec 문제에 대한 문제 해결 프로세스 시작 팁

3가지 IPsec 시나리오를 분리할 수 있습니다. 이는 시작하는 방법을 더 잘 알기 위해 증상을 식별하는 좋은 참조입니다.

1. IPsec 터널이 설정되지 않습니다.
2. IPsec 터널이 다운되어 자체적으로 다시 설정되었습니다. (플랩됨)
3. IPsec 터널이 다운되어 다운상태가 유지됩니다.

IPsec 터널이 증상을 설정하지 않는 경우 실시간으로 디버깅하여 IKE 협상의 현재 동작을 확인해야 합니다.

IPsec 터널이 다운되고 자체 증상에 대해 다시 설정됩니다. 터널 플랩이라고 가장 일반적으로 알려져 있고 RCA(root cause analysis)가 필요합니다. 터널이 다운되거나 디버그를 볼 수 있는 예상 시간을 갖는 타임스탬프를 알아야 합니다.

IPsec 터널이 다운되고 다운상태 증상에 머물러 있는 경우, 터널이 이전에 작동했지만 어떤 이유로든 작동이 중지되었으며 터널을 다시 정상적으로 설정할 수 없게 하는 현재 동작과 분해 사유를 알아야 합니다.

트러블슈팅을 시작하기 전에 포인트를 확인합니다.

1. 문제 및 컨피그레이션이 있는 IPsec 터널(번호)
2. 터널이 다운된 타임스탬프(해당되는 경우).
3. IPsec 피어 IP 주소(터널 대상).

모든 디버깅 및 로그는 **/var/log/messages** 파일에 저장되며 현재 로그의 경우 메시지 파일에 저장되지만 이 특정 증상의 경우 문제 발생 후 몇 시간/일 후에 플랩을 식별할 수 있습니다. 관련된 대부분의 디버그는 메시지 1,2,3.등에 있을 수 있습니다. 올바른 메시지 파일을 확인하고 관련 IPsec 터널의 IKE 협상에 대한 디버그(charon)를 분석하는 타임스탬프를 알고 있어야 합니다.

대부분의 디버그는 IPsec 터널 수를 인쇄하지 않습니다. 협상 및 패킷을 식별하는 가장 빈번한 방법은 원격 피어의 IP 주소 및 터널이 vedge에서 소싱되는 IP 주소를 사용하는 것입니다. 인쇄된 IKE 디버그의 몇 가지 예는 다음과 같습니다.

```
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 협상에 대한 디버그에는 IPsec 터널 번호가 표시되지만, 패킷 교환에 대한 후속 정보는 IPsec 터널 IP 주소만 사용합니다.

```
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 터널 구성:

```
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 !
```

증상 1. IPsec 터널이 설정되지 않음

이 문제는 터널의 첫 번째 구현일 수 있으므로 아직 작동되지 않았으며 IKE 디버그가 가장 좋은 옵션입니다.

증상 2. IPsec 터널이 다운되어 자체적으로 재설정되었습니다.

앞서 언급했듯이, 일반적으로 이 증세는 터널이 다운된 이유에 대한 근본 원인을 알기 위해 설명합니다. 근본 원인 분석이 알려지면 네트워크 관리자가 추가 문제를 방지할 수 있습니다.

트러블슈팅을 시작하기 전에 포인트를 확인합니다.

1. 문제 및 컨피그레이션이 있는 IPsec 터널(번호)
2. 터널이 다운된 타임스탬프입니다.
3. IPsec 피어 IP 주소(터널 대상)

DPD 재전송

이 예에서 터널은 6월 18일 00:31:17에 다운되었습니다.

```
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
```

> **참고:** IPsec 터널 다운에 대한 로그는 로깅된 디버그의 일부가 아니라 *FTMD* 로그입니다. 따라서 *charon*과 *IKE*는 인쇄되지 않습니다.

> **참고:** 관련 로그는 일반적으로 함께 인쇄되지 않으며, 동일한 프로세스와 관련이 없는 추가 정보가 있습니다.

1단계. 타임스탬프가 식별되고 시간 및 로그가 상관관계가 있는 후 로그를 아래에서 위로 검토하기 시작합니다.

```
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)
```

마지막으로 성공한 DPD 패킷 교환은 요청 # 542로 설명되어 있습니다.

```
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 [ ]
```

2단계. 모든 정보를 올바른 순서로 배치합니다.

```
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
```

예를 들어 vEdge01에서 10.10.10.1로부터 DPD 패킷을 수신하지 않으므로 터널이 다운됩니다. 3개의 DPD를 재전송한 후 IPsec 피어가 "lost"로 설정되고 터널이 다운될 것으로 예상됩니다. 이러한 동작에는 여러 가지 이유가 있습니다. 일반적으로 패킷이 경로에서 손실되거나 삭제된 ISP와 관련이 있습니다. 문제가 한 번 발생하면 손실된 트래픽을 추적할 수 있는 방법은 없지만 문제가 계속되면 vEdge, 원격 IPSec 피어 및 ISP에서 캡처를 사용하여 패킷을 추적할 수 있습니다.

증상 3. IPsec 터널이 다운되어 다운상태에 있음

이 증상에 앞서 언급했듯이 터널은 이전에 정상적으로 작동했지만 어떤 이유로든 터널이 다운되어

터널이 다시 정상적으로 설정되지 않았습니다. 이 시나리오에서는 네트워크에 영향을 미칩니다.

트러블슈팅이 시작되기 전에 점을 확인합니다.

1. 문제 및 컨피그레이션이 있는 IPsec 터널(번호)
2. 터널이 다운된 타임스탬프입니다.
3. IPsec 피어 IP 주소(터널 대상)

PFS 불일치

이 예에서는 터널이 다운될 때 타임스탬프로 트러블슈팅이 시작되지 않습니다. 문제가 계속되면 IKE 디버그가 가장 좋습니다.

```
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
```

디버그 링크가 활성화되고 협상이 표시됩니다.

```
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

> **참고:** CREATE_CHILD_SA 패킷은 모든 키 재설정 또는 새 SA에 대해 교환됩니다. 추가 참조를 보려면 Understanding IKEv2 Packet Exchange(IKEv2 패킷 교환 이해)로 이동합니다.

IKE 디버그는 동일한 동작을 보여주며 지속적으로 반복되므로 정보의 일부를 가져와 분석할 수 있습니다.

CREATE_CHILD_SA는 IPsec 엔드포인트 간에 새 SPIS를 생성하고 교환할 목적으로 키 재설정을 의미합니다.

- vedge는 10.10.10.1에서 CREATE_CHILD_SA 요청 패킷을 수신합니다.
- vedge는 요청을 처리하고 피어 10.10.10.1에서 보낸 제안(SA)을 확인합니다.
- vedge는 피어가 보낸 수신한 제안을 구성된 제안과 비교합니다.
- 교환된 CREATE_CHILD_SA가 " 허용 가능한 제안서를 찾을 수 없음"으로 실패합니다.

이 시점에서 질문은 다음과 같습니다. **터널이 이전에 작동했지만 변경 사항이 없는 경우 컨피그레이션이 일치하지 않는 이유는 무엇입니까?**

심층적으로 분석하면 피어가 전송하지 않는 구성된 제안서에 추가 필드가 있습니다.

구성된 제안: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ

받은 제안:
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_4096은 IPsec 섹션 2단계에서 PFS(Perfect-forward-secrecy)에 대해 vEdge가 구성된 DH 그룹 16입니다.

PFS는 터널이 성공적으로 설정되거나 IKE 협상에서 initiator 또는 responder인 사용자에 따라 설정되지 않는 유일한 불일치 컨피그레이션입니다. 그러나 키 재설정이 시작되면 터널을 계속할 수 없으며 이 증상과 관련될 수 있습니다.

vEdge IPSec/ikev2 터널이 DELETE 이벤트로 인해 중단된 후 다시 시작되지 않음

이 동작에 대한 자세한 내용은 Cisco 버그 ID CSCvx86427을 참조하십시오.

문제가 지속되는 만큼 IKE 디버그가 가장 좋은 옵션입니다. 그러나 디버그가 활성화된 경우 이 특정 버그의 경우 터미널이나 메시지 파일 중 어떤 정보도 표시되지 않습니다.

이 문제를 줄이고 vEdge가 Cisco 버그 ID CSCvx86427에 도달했는지 확인하려면 터널이 다운되는 시점을 찾아야 합니다.

트러블슈팅이 시작되기 전에 점을 확인합니다.

1. 문제 및 컨피그레이션이 있는 IPsec 터널(번호)
2. 터널이 다운된 타임스탬프입니다.

3. IPsec 피어 IP 주소(터널 대상)

타임스탬프가 식별되고 시간 및 로그가 상관관계가 파악되면 터널이 중단되기 직전에 로그를 검토합니다.

```
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
```

> **참고:** IPsec 협상에 DELETE 패킷이 여러 개 있으며 CHILD_SA에 대한 DELETE는 REKEY 프로세스에 대한 예상 DELETE입니다. 이 문제는 특정 IPsec 협상 없이 순수 IKE_SA DELETE 패킷을 수신할 때 발생합니다. 이 DELETE는 모든 IPsec/IKE 터널을 제거합니다.

관련 정보

- KEv2 패킷 교환 및 프로토콜 수준 디버깅
- IKE(Internet Key Exchange) - RFC 2409
- IKEv2 - RFC 7296
- vEdge와 Cisco IOS 간 사이트 간 LAN-LAN IPSec
- 기술 지원 및 문서 – Cisco Systems