PSK가 있는 Site-to-Site VPN용 IOS IKEv2 디버그 문제 해결 TechNote

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[핵심 문제](#)
[라우터 컨피그레이션](#)
[문제 해결](#)
[라우터 디버그](#)
[CHILD_SA 디버그](#)
[터널 확인](#)
[ISAKMP](#)
[IPsec](#)
[관련 정보](#)

소개

이 문서에서는 PSK(사전 공유 키)를 사용할 때 Cisco IOS®의 IKEv2(Internet Key Exchange version 2) 디버깅에 대해 설명합니다.또한 이 문서에서는 구성의 특정 디버그 행을 변환하는 방법에 대한 정보를 제공합니다.

사전 요구 사항

요구 사항

Cisco에서는 IKEv2에 대한 패킷 교환에 대해 알고 있는 것이 좋습니다. 자세한 내용은 IKEv2 패킷 교환 및 프로토콜 수준 디버깅을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IKEv2(Internet Key Exchange Version 2)

- Cisco IOS 15.1(1)T 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

핵심 문제

IKEv2의 패킷 교환은 IKEv1의 패킷 교환과 근본적으로 다릅니다. IKEv1에서는 6개의 패킷으로 구성된 명확한 경계 1단계 교환이 있었고 그 뒤에 3개의 패킷으로 구성된 2단계 교환이 있었습니다 .IKEv2 교환은 변수입니다.패킷 교환의 차이와 설명에 대한 자세한 내용은 IKEv2 패킷 교환 및 프로토콜 수준 디버깅을 참조하십시오.

라우터 컨피그레이션

이 섹션에서는 이 문서에서 사용되는 구성을 나열합니다.

라우터 1

```
interface Loopback0
ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
ip address 172.16.0.101 255.255.255.0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel destination 10.0.0.2
tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2
!
crypto ikev2 policy site-pol
proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
peer peer1
address 10.0.0.2 255.255.255.0
hostname host1
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile IKEV2-SETUP
match identity remote address 0.0.0.0
```

```
authentication remote pre-share
authentication local pre-share
keyring local KEYRNG
lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

라우터 2

```
crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2
!
crypto ikev2 keyring KEYRNG
peer peer2
address 10.0.0.1 255.255.255.0
hostname host2
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile IKEV2-SETUP
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local KEYRNG
lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
!
interface Loopback0
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
ip address 172.16.0.102 255.255.255.0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel destination 10.0.0.1
tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

문제 해결

라우터 디버그

이 문서에서는 다음과 같은 debug 명령을 사용합니다.

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

라우터 1(개시자) 메시지 설명	디버깅	라우터 2(Responder) 메시지 설명
라우터 1은 피어 ASA 10.0.0.2에 대한 암호화 ACL과 일치하는 패킷을 수신합니다. SA 생성을 시작합니다.	*11월 11일 20:28:34.003:IKEv2:디스패처에서 패킷 가져오기 *11월 11일 20:28:34.003:IKEv2:pak 큐에서 항목 처리 *11월 11일 19:30:34.811:IKEv2:% 주소별 사전 공유 키 가져오기 10.0.0.2 *11월 11일 19:30:34.811:IKEv2:제안서 PHASE1-prop to toolkit policy 추가 *11월 11일 19:30:34.811:IKEv2:(1):IKE 프로필 IKEV2-SETUP 선택 *11월 11일 19:30:34.811:IKEv2:새 ikev2 sa 요청이 승인됨 *11월 11일 19:30:34.811:IKEv2:발신 협상 sa 수를 1씩 증가 *11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000(I) MsgID = 00000000000000Cur상태:IDLE 이벤트:EV_INIT_SA	
첫 번째 메시지 쌍은 IKE_SA_INIT 교환입니다.이러한 메시지는 암호화 알고리즘을 협상하고, 비품을 교환하며, Diffie-Hellman 교환을 수행합니다. **관련 구성:** `crypto ikev2 PHASE1-prop encryption 3des aes-cbc-128 integrity sha1 group 2 crypto ikev2 keyring KEYRNG peer1 address 10.0.0.2 255.255.255.0 hostname host1 pre-shared-key local cisco pre-shared-key remote cisco`	*11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000(I) MsgID = 00000000000000Cur상태:I_BLD_INIT 이벤트 :EV_GET_IKE_POLICY *11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000(I) MsgID = 00000000000000Cur상태:I_BLD_INIT 이벤트 :**EV_SET_POLICY** *11월 11일 19:30:34.811:IKEv2:(SA ID = 1):구성된 정책 설정 *11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000(I) MsgID = 00000000000000Cur상태:I_BLD_INIT 이벤트 :EV_CHK_AUTH4PKI *11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000(I) MsgID = 00000000000000Cur상태:I_BLD_INIT 이벤트 :**EV_GEN_DH_KEY** *11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000(I) MsgID = 00000000000000Cur상태:I_BLD_INIT 이벤트:EV_NO_이벤트 *11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace->	

SA:I_SPI=F074D8BBD5A59F0B
R_SPI=000000000000000(I) MsgID =
00000000000000Cur상태:I_BLD_INIT 이벤트
:EV_OK_RECD_DH_PUBKEY_RESP
*11월 11일 19:30:34.811:IKEv2:(SA ID = 1):작업:작업_Null
*11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=000000000000000(I) MsgID =
00000000000000Cur상태:I_BLD_INIT 이벤트
:EV_GET_CONFIG_MODE
*11월 11일 19:30:34.811:IKEv2:IKEv2 initiator -
IKE_SA_INIT exch에서 전송할 구성 데이터가 없습니다.
*11월 11일 19:30:34.811:IKEv2: 툴킷에 전송할 구성 데이터
가 없습니다.
*11월 11일 19:30:34.811:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=000000000000000(I) MsgID =
00000000000000Cur상태:I_BLD_INIT 이벤트
:EV_BLD_MSG
*11월 11일 19:30:34.811:IKEv2:공급업체별 페이로드 구성
:삭제 사유
*11월 11일 19:30:34.811:IKEv2:공급업체별 페이로드 구성
:(사용자 지정)
*11월 11일 19:30:34.811:IKEv2:구성 알림 페이로드
:NAT_DETECTION_SOURCE_IP
*11월 11일 19:30:34.811:IKEv2:구성 알림 페이로드
:NAT_DETECTION_DESTINATION_IP
*11월 11일 19:30:34.811: **IKEv2:(SA ID = 1)**:다음 페이로드
:SA, 버전:2.0 Exchange 유형: **IKE_SA_INIT,** 플래그:
INITIATOR 메시지 ID:0, 길이:344
페이로드 내용:
SA 다음 페이로드:KE, 예약됨:0x0, 길이:56
마지막 제안:0x0, 예약됨:0x0, 길이:52
제안:1, 프로토콜 ID:IKE, SPI 크기:0, #trans:마지막 변환
:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:3DES
마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
KE 다음 페이로드:N, 예약됨:0x0, 길이:136
DH 그룹:2, 예약됨:0x0
N 다음 페이로드:VID, 예약됨:0x0, 길이:24
VID 다음 페이로드:VID, 예약됨:0x0, 길이:23
VID 다음 페이로드:알림, 예약됨:0x0, 길이:21
NOTIFY(NAT_DETECTION_SOURCE_IP) 다음 페이로드
:알림, 예약됨:0x0, 길이:28
보안 프로토콜 ID:IKE, spi 크기:0, 유형
:NAT_DETECTION_SOURCE_IP

IKE_INIT_SA 패킷을 빌드하는 개시자입니다.여기에는 다음이 포함됩니다 .ISAKMP 헤더(SPI/version/flags), SAi1(IKE 이니시에이터가 지원하는 암호화 알고리즘), KEi(개시자의 DH 공개 키 값) 및 N(Initiator Nonce).

NOTIFY(NAT_DETECTION_DESTINATION_IP) 다음 페이로드:없음, 예약됨:0x0, 길이:28
보안 프로토콜 ID:IKE, spi 크기:0, 유형:NAT_DETECTION_DESTINATION_IP
*11월 11일 19:30:34.814:IKEv2:디스패처에서 패킷 가져오기
*11월 11일 19:30:34.814:IKEv2:pak 큐에서 항목 처리
*11월 11일 19:30:34.814:IKEv2:새 ikev2 sa 요청이 승인됨
*11월 11일 19:30:34.814:IKEv2:수신 협상 SA 수를 하나씩 증가
*11월 11일 19:30:34.814:IKEv2:다음 페이로드:SA, 버전:2.0 Exchange 유형:IKE_SA_INIT, 플래그:INITIATOR 메시지 ID:0, 길이:344
페이로드 내용:
SA 다음 페이로드:KE, 예약됨:0x0, 길이:56
마지막 제안:0x0, 예약됨:0x0, 길이:52
제안:1, 프로토콜 ID:IKE, SPI 크기:0, #trans:마지막 변환:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:3DES
마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
KE 다음 페이로드:N, 예약됨:0x0, 길이:136
DH 그룹:2, 예약됨:0x0
N 다음 페이로드:VID, 예약됨:0x0, 길이:24

응답자가 IKE_INIT_SA를 수신합니다.

Responder가 해당 피어에 대한 SA 생성을 시작합니다.

*11월 11일 19:30:34.814:IKEv2:공급업체별 페이로드 구문 분석:CISCO-DELETE-REASON VID 다음 페이로드:VID, 예약됨:0x0, 길이:23
*11월 11일 19:30:34.814:IKEv2:공급업체별 페이로드 구문 분석:(사용자 지정) VID 다음 페이로드:알림, 예약됨:0x0, 길이:21
*11월 11일 19:30:34.814:IKEv2:구문 분석 알림 페이로드:NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) 다음 페이로드:알림, 예약됨:0x0, 길이:28
보안 프로토콜 ID:IKE, spi 크기:0, 유형:NAT_DETECTION_SOURCE_IP
*11월 11일 19:30:34.814:IKEv2:구문 분석 알림 페이로드:NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) 다음 페이로드:없음, 예약됨:0x0, 길이:28
보안 프로토콜 ID:IKE, spi 크기:0, 유형:NAT_DETECTION_DESTINATION_IP
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:유휴 이벤트:**EV_RECV_INIT**

Responder는 IKE_INIT 메시지를 확인하고 처리합니다.(1) 개시자가 제

*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_INIT 이벤트:**EV_VERIFY_MSG**
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_INIT 이벤트:**EV_INSERT_SA**
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_INIT 이벤트:**EV_GET_IKE_POLICY**
*11월 11일 19:30:34.814:IKEv2:툴킷 정책에 제안 기본값 추가
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_INIT 이벤트:**EV_PROC_MSG**
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_INIT 이벤트:EV_DETECT_NAT
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):프로세스 NAT 검색 알림
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):처리 nat detect src notify
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):일치하는 원격 주소
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):처리 nat detect dst notify
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):일치하는 로컬 주소
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):NAT를 찾을 수 없음
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_INIT 이벤트:EV_CHK_CONFIG_MODE
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_BLD_INIT 이벤트:EV_SET_POLICY
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):**구성된 정책 설정**
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_BLD_INIT 이벤트:EV_CHK_AUTH4PKI
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:R_BLD_INIT 이벤트:EV_PKI_SESH_OPEN
*11월 11일 19:30:34.814:IKEv2:(SA ID = 1):PKI 세션 열기

공하는 암호화 도구 모음에서 (2) 자체 DH 비밀 키를 계산하고 (3) 이 IKE_SA에 대해 모든 키를 파생시킬 수 있는 키 ID 값을 계산합니다.뒤에 오는 모든 메시지의 헤더를 제외한 모든 헤더가 암호화 및 인증됩니다.암호화 및 무결성 보호에 사용되는 키는 SKEYID에서 파생되며 다음과 같습니다.SK_e(암호화), SK_a(인증), SK_d는 CHILD_SA에 대한 추가 키 자료를 파생하는 데 파생되고 각 방향에 대해 별도의 SK_e 및 SK_a가 계산됩니다.

관련 구성:

```
crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2 crypto ikev2 keyring KEYING peer2
address 10.0.0.1 255.255.255.0
hostname host2 pre-shared-key local cisco pre-shared-key remote cisco
```

*11월 11일 19:30:34.815:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트:**EV_GEN_DH_KEY**
*11월 11일 19:30:34.815:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트:EV_NO_이벤트
*11월 11일 19:30:34.815:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트
:**EV_OK_RECD_DH_PUBKEY_RESP**
*11월 11일 19:30:34.815:IKEv2:(SA ID = 1):작업:작업_Null
*11월 11일 19:30:34.815:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트:**EV_GEN_DH_SECRET**
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트:EV_NO_이벤트
*11월 11일 19:30:34.822:IKEv2:% **주소별 사전 공유 키**
10.0.0.1
*11월 11일 19:30:34.822:IKEv2:툴킷 정책에 제안 기본값 추
가
*11월 11일 19:30:34.822:IKEv2:(2):IKE 프로필 IKEV2-
SETUP 선택
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트
:EV_OK_RECD_DH_SECRET_RESP
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):작업:작업_Null
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트:**EV_GEN_SKEYID**
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):**skeyid 생성**
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트:EV_GET_CONFIG_MODE
*11월 11일 19:30:34.822:IKEv2:IKEv2 responder -
IKE_SA_INIT exch에서 전송할 구성 데이터가 없습니다.
*11월 11일 19:30:34.822:IKEv2: 툴킷에 전송할 구성 데이터
가 없습니다.
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_BLD_INIT 이벤트:EV_BLD_MSG
*11월 11일 19:30:34.822:IKEv2:공급업체별 페이로드 구성
:삭제 사유

*11월 11일 19:30:34.822:IKEv2:공급업체별 페이로드 구성 :(사용자 지정)
*11월 11일 19:30:34.822:IKEv2:구성 알림 페이로드 :NAT_DETECTION_SOURCE_IP
*11월 11일 19:30:34.822:IKEv2:구성 알림 페이로드 :NAT_DETECTION_DESTINATION_IP
*11월 11일 19:30:34.822:IKEv2:구성 알림 페이로드 :HTTP_CERT_LOOKUP_SUPPORTED
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):다음 페이로드 :SA, 버전:2.0 Exchange 유형: **IKE_SA_INIT,** 플래그: **RESPONDER MSG-RESPONSE** 메시지 ID:0, 길이:449
페이로드 내용:
SA 다음 페이로드:KE, 예약됨:0x0, 길이:48
마지막 제안:0x0, 예약됨:0x0, 길이:44
제안:1, 프로토콜 ID:IKE, SPI 크기:0, #trans:마지막 변환 :0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
KE 다음 페이로드:N, 예약됨:0x0, 길이:136
DH 그룹:2, 예약됨:0x0
N 다음 페이로드:VID, 예약됨:0x0, 길이:24
VID 다음 페이로드:VID, 예약됨:0x0, 길이:23
VID 다음 페이로드:알림, 예약됨:0x0, 길이:21
NOTIFY(NAT_DETECTION_SOURCE_IP) 다음 페이로드 :알림, 예약됨:0x0, 길이:28
보안 프로토콜 ID:IKE, spi 크기:0, 유형 :NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP) 다음 페이로드:CERTREQ, 예약됨:0x0, 길이:28
보안 프로토콜 ID:IKE, spi 크기:0, 유형 :NAT_DETECTION_DESTINATION_IP
CERTREQ 다음 페이로드:알림, 예약됨:0x0, 길이:105
PKIX의 인증서 인코딩 해시 및 URL
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) 다음 페이로드:없음, 예약됨:0x0, 길이:8
보안 프로토콜 ID:IKE, spi 크기:0, 유형 :HTTP_CERT_LOOKUP_SUPPORTED
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:INIT_DONE 이벤트:EV_완료
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):Cisco DeleteReason Notify가 활성화됨
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000 CurState:INIT_DONE 이벤트:EV_CHK4_ROLE
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace->

라우터 2는 ASA1에서 수신하는 IKE_SA_INIT 교환에 대한 responder 메시지를 작성합니다. 이 패킷에는 다음이 포함됩니다 .ISAKMP Header(SPI/version /flags), SAr1(IKE 응답자가 선택한 암호화 알고리즘), KEr(responder의 DH 공개 키 값) 및 Responder Nonce입니다.

Router2는 라우터 1에 responder 메시지를 전송합니다.

SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:INIT_DONE 이벤트:**EV_START_TMR**
*11월 11일 19:30:34.822:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000000
CurState:R_WAIT_AUTH 이벤트:EV_NO_이벤트
*11월 11일 19:30:34.822:IKEv2:**새 ikev2 sa 요청이 허용됨**
*11월 11일 19:30:34.822:IKEv2:**발신 협상 sa 수를 1씩 증가**
*11월 11일
19:30:34.823:IKEv2:디스패처
에서 패킷 가져오기

라우터 1은 라우터 2에서 IKE_SA_INIT 응답 패킷을 수신합니다.

*11월 11일
19:30:34.823:IKEv2:디스패처
에서 패킷 가져오기

I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C
4(R) MsgID = 000000000000
CurState:INIT_DONE 이벤트
:**EV_START_TMR**

Responder가 인증 프로세스에 대한 타이머를 시작합니다.

*11월 11일
19:30:34.823:IKEv2:pak 큐에
서 항목 처리
*11월 11일 19:30:34.823:IKEv2:(SA ID = 1):다음 페이로드
:SA, 버전:2.0 Exchange 유형:IKE_SA_INIT, 플래그:
RESPONDER MSG-RESPONSE 메시지 ID:0, 길이:449
페이로드 내용:
SA 다음 페이로드:KE, 예약됨:0x0, 길이:48
마지막 제안:0x0, 예약됨:0x0, 길이:44
제안:1, 프로토콜 ID:IKE, SPI 크기:0, #trans:마지막 변환
:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
KE 다음 페이로드:N, 예약됨:0x0, 길이:136
DH 그룹:2, 예약됨:0x0
N 다음 페이로드:VID, 예약됨:0x0, 길이:24

Router1은 응답을 확인하고 처리합니다.(1) 개시자 DH 비밀 키가 계산되고 (2) 개시자 키 ID도 생성됩니다.

*11월 11일 19:30:34.823:IKEv2:공급업체별 페이로드 구문
분석:CISCO-DELETE-REASON VID 다음 페이로드:VID, 예
약됨:0x0, 길이:23

*11월 11일 19:30:34.823:IKEv2:공급업체별 페이로드 구문
분석:(사용자 지정) VID 다음 페이로드:알림, 예약됨:0x0, 길
이:21

*11월 11일 19:30:34.823:IKEv2:구문 분석 알림 페이로드
:NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_SOURCE_IP) 다음 페이로드
:알림, 예약됨:0x0, 길이:28
보안 프로토콜 ID:IKE, spi 크기:0, 유형
:NAT_DETECTION_SOURCE_IP

*11월 11일 19:30:34.824:IKEv2:구문 분석 알림 페이로드
:NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP) 다음 페이
로드:CERTREQ, 예약됨:0x0, 길이:28
   보안 프로토콜 ID:IKE, spi 크기:0, 유형
:NAT_DETECTION_DESTINATION_IP
 CERTREQ 다음 페이로드:알림, 예약됨:0x0, 길이:105
   PKIX의 인증서 인코딩 해시 및 URL

*11월 11일 19:30:34.824:IKEv2:구문 분석 알림 페이로드
:HTTP_CERT_LOOKUP_SUPPORTED
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) 다음 페이
로드:없음, 예약됨:0x0, 길이:8
   보안 프로토콜 ID:IKE, spi 크기:0, 유형
:HTTP_CERT_LOOKUP_SUPPORTED
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_WAIT_INIT 이벤트:EV_RECV_INIT
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):IKE_SA_INIT
메시지 처리 중
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_PROC_INIT 이벤트:EV_CHK4_NOTIFY
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_PROC_INIT 이벤트:EV_VERIFY_MSG
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_PROC_INIT 이벤트:EV_PROC_MSG
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_PROC_INIT 이벤트:EV_DETECT_NAT
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):프로세스 NAT
검색 알림
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):처리 nat detect
src notify
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):일치하는 원격
주소
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):처리 nat detect
dst notify
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):일치하는 로컬
주소
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):NAT를 찾을 수
없음
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000

CurState:I_PROC_INIT 이벤트:EV_CHK_NAT_T
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_PROC_INIT 이벤트:EV_CHK_CONFIG_MODE
*11월 11일 19:30:34.824:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:INIT_DONE 이벤트:**EV_GEN_DH_SECRET**
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:INIT_DONE 이벤트:EV_NO_이벤트
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:INIT_DONE 이벤트
:EV_OK_RECD_DH_SECRET_RESP
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):작업:작업_Null
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:INIT_DONE 이벤트:**EV_GEN_SKEYID**
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):**skeyid 생성**
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:INIT_DONE 이벤트:EV_완료
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):Cisco
DeleteReason Notify가 활성화됨
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:INIT_DONE 이벤트:EV_CHK4_ROLE
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_BLD_AUTH 이벤트:EV_GET_CONFIG_MODE
*11월 11일 19:30:34.831:IKEv2:구성 데이터를 툴킷에 전송
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_BLD_AUTH 이벤트:EV_CHK_EAP
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_BLD_AUTH 이벤트:**EV_GEN_AUTH**
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_BLD_AUTH 이벤트:EV_CHK_AUTH_TYPE
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B

개시자는 IKE_AUTH 교환을 시작하고 인증 페이로드를 생성합니다 .IKE_AUTH 패킷에는 다음이 포함됩니다.ISAKMP 헤더 (SPI/ 버전/플래그), IDi(개시자의 ID), AUTH 페이로드,

R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_BLD_AUTH 이벤트:EV_OK_AUTH_GEN
*11월 11일 19:30:34.831:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000000
CurState:I_BLD_AUTH 이벤트:EV_SEND_AUTH
*11월 11일 19:30:34.831:IKEv2:공급업체별 페이로드 구성
:CISCO-그래닛
*11월 11일 19:30:34.831:IKEv2:구성 알림 페이로드:초기
_연락처

SAi2(IKEv1에서 2단계 변환 세트 교환과 유사한 SA 시작) 및 TSi 및 TSr(개시자 및 응답자 트래픽 선택기):암호화된 트래픽을 전달/수신하기 위해 각각 initiator와 responder의 소스 및 목적지 주소를 포함합니다.주소 범위는 해당 범위에서 들어오고 나가는 모든 트래픽이 터널링되도록 지정합니다.제안서가 응답자에게 수락될 경우 동일한 TS 페이로드를 다시 전송합니다.첫 번째 CHILD_SA는 트리거 패킷과 일치하는 proxy_ID 쌍에 대해 생성됩니다.

관련 구성:
```
crypto ipsec transform-set TS esp-3des esp-sha-hmac
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
```

*11월 11일 19:30:34.831:IKEv2:구성 알림 페이로드
:SET_WINDOW_SIZE
*11월 11일 19:30:34.831:IKEv2:구성 알림 페이로드
:ESP_TFC_NO_SUPPORT
*11월 11일 19:30:34.831:IKEv2:구성 알림 페이로드
:NON_FIRST_FRAGS
페이로드 내용:
VID 다음 페이로드:IDi, 예약됨:0x0, 길이:20
IDi 다음 페이로드:AUTH, 예약됨:0x0, 길이:12
ID 유형:IPv4 주소, 예약됨:0x0 0x0
AUTH 다음 페이로드:CFG, 예약됨:0x0, 길이:28
인증 방법 PSK, 예약됨:0x0, 예약됨 0x0
CFG 다음 페이로드:SA, 예약됨:0x0, 길이:309
cfg 유형:CFG_REQUEST, 예약됨:0x0, 예약됨:0x0
*11월 11일 19:30:34.831: SA Next 페이로드: **TSi**, 예약됨
:0x0, 길이:40
마지막 제안:0x0, 예약됨:0x0, 길이:36
제안:1, 프로토콜 ID:ESP, SPI 크기:4, #trans:마지막 변환
:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:3DES
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:5, 예약됨:0x0, id:ESN 사용 안 함
TSi 다음 페이로드:TSr, 예약됨:0x0, 길이:24
TS 수:1, 예약됨 0x0, 예약됨 0x0
TS 유형:TS_IPV4_ADDR_RANGE, proto id:0, 길이:16
시작 포트:0, 끝 포트:65535
시작 주소:0.0.0.0, 끝 주소:255.255.255.255
TSr 다음 페이로드:알림, 예약됨:0x0, 길이:24
TS 수:1, 예약됨 0x0, 예약됨 0x0
TS 유형:TS_IPV4_ADDR_RANGE, proto id:0, 길이:16
시작 포트:0, 끝 포트:65535
시작 주소:0.0.0.0, 끝 주소:255.255.255.255
NOTIFY(INITIAL_CONTACT) 다음 페이로드:알림, 예약됨
:0x0, 길이:8
보안 프로토콜 ID:IKE, spi 크기:0, 유형:초기_연락처
NOTIFY(SET_WINDOW_SIZE) 다음 페이로드:알림, 예약됨
:0x0, 길이:12
보안 프로토콜 ID:IKE, spi 크기:0, 유형
:SET_WINDOW_SIZE
알림(ESP_TFC_NO_SUPPORT) 다음 페이로드:알림, 예약
됨:0x0, 길이:8

보안 프로토콜 ID:IKE, spi 크기:0, 유형
:ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) 다음 페이로드:없음, 예약됨
:0x0, 길이:8
보안 프로토콜 ID:IKE, spi 크기:0, 유형
:NON_FIRST_FRAGS

*11월 11일 19:30:34.832:IKEv2:(SA ID = 1):다음 페이로드
:ENCR, 버전:2.0 Exchange 유형: **IKE_AUTH**, 플래그:
INITIATOR Message id:1, 길이:556
페이로드 내용:
ENCR 다음 페이로드:VID, 예약됨:0x0, 길이:528

*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID =
0000000001**Cur상태:I_WAIT_AUTH** 이벤트:EV_NO_이벤트
*11월 11일 19:30:34.832:IKEv2:디스패처에서 패킷 가져오
기
*11월 11일 19:30:34.832:IKEv2:pak 큐에서 항목 처리
*11월 11일 19:30:34.832:IKEv2:(SA ID = 1):요청에
mess_id 1이 있습니다.1부터 1까지
*11월 11일 19:30:34.832: **IKEv2:(SA ID = 1)**:다음 페이로드
:ENCR, 버전:2.0 Exchange 유형: **IKE_AUTH**, 플래그:
INITIATOR 메시지 ID:1, 길이:556
페이로드 내용:
*11월 11일 19:30:34.832:IKEv2:공급업체별 페이로드 구문
분석:(사용자 지정) VID 다음 페이로드:IDi, 예약됨:0x0, 길이
:20
IDi 다음 페이로드:AUTH, 예약됨:0x0, 길이:12
ID 유형:IPv4 주소, 예약됨:0x0 0x0
AUTH 다음 페이로드:CFG, 예약됨:0x0, 길이:28
인증 방법 PSK, 예약됨:0x0, 예약됨 0x0
CFG 다음 페이로드:SA, 예약됨:0x0, 길이:309
cfg 유형:CFG_REQUEST, 예약됨:0x0, 예약됨:0x0
*11월 11일 19:30:34.832: atrib 유형:내부 IP4 DNS, 길이
:0
*11월 11일 19:30:34.832: atrib 유형:내부 IP4 DNS, 길이
:0
*11월 11일 19:30:34.832: atrib 유형:내부 IP4 NBNS, 길이
:0
*11월 11일 19:30:34.832: atrib 유형:내부 IP4 NBNS, 길이
:0
*11월 11일 19:30:34.832: atrib 유형:내부 IP4 서브넷, 길
이:0
*11월 11일 19:30:34.832: atrib 유형:애플리케이션 버전,
길이:257
atrib 유형:알 수 없음 - 28675, 길이:0
*11월 11일 19:30:34.832: atrib 유형:알 수 없음 - 28672,
길이:0
*11월 11일 19:30:34.832: atrib 유형:알 수 없음 - 28692,
길이:0
*11월 11일 19:30:34.832: atrib 유형:알 수 없음 - 28681,

라우터 2는 라우터 1에서 수신된 인증 데이터를 수신하고 확인합니다.
관련 구성: `crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-1 md5`

길이:0
*11월 11일 19:30:34.832: atrib 유형:알 수 없음 - 28674, 길이:0
*11월 11일 19:30:34.832: **SA** 다음 페이로드:TSi, 예약됨:0x0, 길이:40
  마지막 제안:0x0, 예약됨:0x0, 길이:36
  제안:1, 프로토콜 ID:ESP, SPI 크기:4, #trans:마지막 변환:0x3, 예약됨:0x0:길이:8
    유형:1, 예약됨:0x0, id:3DES
    마지막 변환:0x3, 예약됨:0x0:길이:8
    유형:3, 예약됨:0x0, id:SHA96
    마지막 변환:0x0, 예약됨:0x0:길이:8
    유형:5, 예약됨:0x0, id:ESN 사용 안 함
 TSi 다음 페이로드:TSr, 예약됨:0x0, 길이:24
    TS 수:1, 예약됨 0x0, 예약됨 0x0
    TS 유형:TS_IPV4_ADDR_RANGE, proto id:0, 길이:16
    시작 포트:0, 끝 포트:65535
    시작 주소:0.0.0.0, 끝 주소:255.255.255.255
 TSr 다음 페이로드:알림, 예약됨:0x0, 길이:24
    TS 수:1, 예약됨 0x0, 예약됨 0x0
    TS 유형:TS_IPV4_ADDR_RANGE, proto id:0, 길이:16
    시작 포트:0, 끝 포트:65535
    시작 주소:0.0.0.0, 끝 주소:255.255.255.255
 *11월 11일 19:30:34.832:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트: EV_RECV_AUTH
*11월 11일 19:30:34.832:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트:EV_CHK_NAT_T
*11월 11일 19:30:34.832:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트:EV_PROC_ID
*11월 11일 19:30:34.832:IKEv2:(SA ID = 1):프로세스 ID에서 유효한 매개 변수를 받았습니다.
*11월 11일 19:30:34.832:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트 :EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_인출됨_FOR_PROF_SEL
*11월 11일 19:30:34.832:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트 :EV_GET_POLICY_BY_PEERID
*11월 11일 19:30:34.833:IKEv2:(1):IKE 프로필 IKEV2-SETUP 선택
*11월 11일 19:30:34.833:IKEv2:% 주소별 사전 공유 키 가져오기 10.0.0.1
*11월 11일 19:30:34.833:IKEv2:% 주소별 사전 공유 키 가

라우터 2는 라우터 1에서 받은 IKE_AUTH 패킷에 대한 응답을 작성합니다. 이 응답 패킷에는 다음이 포함됩니다.ISAKMP Header(SPI/version/flags), IDr(responder ID), AUTH 페이로드, SAr2(IKEv1에서 2단계 변환 세트 교환과 유사한 SA 시작) 및 TSi 및 TSr(Initiator 및 Responder Traffic Selectors) 암호화된 트래픽을 전달/수신하기 위해 각각 initiator와 responder의 소스 및 목적지 주소를 포함합니다.주소 범위는 해당 범위에서 들어오고 나가는 모든 트래픽이 터널링되도록 지정합니다.이러한 매개변수는 ASA1에서 수신한

져오기 10.0.0.1
*11월 11일 19:30:34.833:IKEv2:툴킷 정책에 제안 기본값 추가
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):IKEv2 프로파일 'IKEV2-SETUP' 사용
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트:EV_SET_POLICY
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):구성된 정책 설정
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트 :EV_VERIFY_POLICY_BY_PEERID
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트:EV_CHK_AUTH4EAP
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_WAIT_AUTH 이벤트:EV_CHK_POLREQEAP
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트:EV_CHK_AUTH_TYPE

매개변수와 동일합니다.

*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트 :EV_GET_PRESHR_KEY
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트:EV_VERIFY_AUTH
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트:EV_CHK4_IC
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트:EV_CHK_리디렉션
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1): 리디렉션 확인이 필요하지 않으므로 건너뜁니다.
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트 :EV_NOTIFY_AUTH_DONE
*11월 11일 19:30:34.833:IKEv2:AAA 그룹 권한 부여가 구성

되지 않음
*11월 11일 19:30:34.833:IKEv2:AAA 사용자 권한 부여가 구성되지 않음
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트 :EV_CHK_CONFIG_MODE
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트 :EV_SET_RECD_CONFIG_MODE
*11월 11일 19:30:34.833:IKEv2: 툴킷에서 구성 데이터를 받았습니다.
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트:EV_PROC_SA_TS
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_VERIFY_AUTH 이벤트 :EV_GET_CONFIG_MODE
*11월 11일 19:30:34.833:IKEv2:컨피그레이션 응답을 구성하는 동안 오류가 발생했습니다.
*11월 11일 19:30:34.833:IKEv2: 툴킷에 전송할 구성 데이터가 없습니다.
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_BLD_AUTH 이벤트:EV_MY_AUTH_METHOD
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_BLD_AUTH 이벤트:EV_GET_PRESHR_KEY
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_BLD_AUTH 이벤트:EV_GEN_AUTH
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_BLD_AUTH 이벤트:EV_CHK4_SIGN
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_BLD_AUTH 이벤트:EV_OK_AUTH_GEN
*11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:R_BLD_AUTH 이벤트:EV_SEND_AUTH
*11월 11일 19:30:34.833:IKEv2:공급업체별 페이로드 구성

	:CISCO-그래닛 *11월 11일 19:30:34.833:IKEv2:구성 알림 페이로드 :SET_WINDOW_SIZE *11월 11일 19:30:34.833:IKEv2:구성 알림 페이로드 :ESP_TFC_NO_SUPPORT *11월 11일 19:30:34.833:IKEv2:구성 알림 페이로드:NON_FIRST_FRAGS *11월 11일 19:30:34.833:IKEv2:(SA ID = 1):다음 페이로드 :ENCR, 버전:2.0 Exchange 유형: **IKE_AUTH**, 플래그: **RESPONDER MSG-RESPONSE** 메시지 ID:1, 길이:252 페이로드 내용: **ENCR** 다음 페이로드:VID, 예약됨:0x0, 길이:224 *11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:EV_확인 *11월 11일 19:30:34.833:IKEv2:(SA ID = 1):작업:작업_Null *11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:EV_PKI_SESH_CLOSE *11월 11일 19:30:34.833:IKEv2:(SA ID = 1):PKI 세션 닫기 *11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:EV_UPDATE_CAC_STATS *11월 11일 19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:**EV_INSERT_IKE** *11월 11일 19:30:34.834:IKEv2:Store mib index ikev2 1, platform 60 *11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:EV_GEN_LOAD_IPSEC *11월 11일 19:30:34.834:IKEv2:(SA ID = 1):비동기 요청이 대기되었습니다. *11월 11일 19:30:34.834:IKEv2:(SA ID = 1): *11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000001 Cur State: AUTH_DONE 이벤트:EV_NO_이벤트	응답자는 IKE_AUTH에 대한 응답을 보냅니다.
Initiator가 Responder로부터 응답을 받습니다.	*11월 11일 19:30:34.834:IKEv2:디스패처에서 패킷 가져오기 *11월 11일 19:30:34.834:IKEv2:pak 큐에서 항목 처리	*11월 11일 19:30:34.840:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트 :EV_OK_RECD_LOAD_IPSE	응답자는 SAD에 항목을 삽입합니다.

C
*11월 11일 19:30:34.840:IKEv2:(SA ID = 1):작업:작업_Null
*11월 11일 19:30:34.840:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:EV_START_ACCT
*11월 11일 19:30:34.840:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:EV_CHECK_DUPLES
*11월 11일 19:30:34.840:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:EV_CHK4_ROLE

*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):다음 페이로드:ENCR, 버전:2.0 Exchange 유형: **IKE_AUTH**, 플래그: **RESPONDER MSG-RESPONSE** 메시지 ID:1, 길이:252
페이로드 내용:

*11월 11일 19:30:34.834:IKEv2:공급업체별 페이로드 구문 분석:(사용자 지정) VID 다음 페이로드:IDr, 예약됨:0x0, 길이:20

라우터 1은 이 패킷의 인증 데이터를 확인하고 처리합니다.그러면 라우터 1이 SAD에 이 SA를 삽입합니다.

IDr 다음 페이로드:AUTH, 예약됨:0x0, 길이:12
ID 유형:IPv4 주소, 예약됨:0x0 0x0
AUTH 다음 페이로드:SA, 예약됨:0x0, 길이:28
인증 방법 PSK, 예약됨:0x0, 예약됨 0x0
SA 다음 페이로드:TSi, 예약됨:0x0, 길이:40
마지막 제안:0x0, 예약됨:0x0, 길이:36
제안:1, 프로토콜 ID:ESP, SPI 크기:4, #trans:마지막 변환:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:3DES
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:5, 예약됨:0x0, id:ESN 사용 안 함
TSi 다음 페이로드:TSr, 예약됨:0x0, 길이:24

TS 수:1, 예약됨 0x0, 예약됨 0x0
TS 유형:TS_IPV4_ADDR_RANGE, proto id:0, 길이:16
시작 포트:0, 끝 포트:65535
시작 주소:0.0.0.0, 끝 주소:255.255.255.255
TSr 다음 페이로드:알림, 예약됨:0x0, 길이:24
TS 수:1, 예약됨 0x0, 예약됨 0x0
TS 유형:TS_IPV4_ADDR_RANGE, proto id:0, 길이:16
시작 포트:0, 끝 포트:65535
시작 주소:0.0.0.0, 끝 주소:255.255.255.255

*11월 11일 19:30:34.834:IKEv2:구문 분석 알림 페이로드
:SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) 다음
페이로드:알림, 예약됨:0x0, 길이:12
보안 프로토콜 ID:IKE, spi 크기:0, 유형
:SET_WINDOW_SIZE

*11월 11일 19:30:34.834:IKEv2:구문 분석 알림 페이로드
:ESP_TFC_NO_SUPPORT
NOTIFY(ESP_TFC_NO_SUPPORT) 다음 페이로드:알림,
예약됨:0x0, 길이:8
보안 프로토콜 ID:IKE, spi 크기:0, 유형
:ESP_TFC_NO_SUPPORT

*11월 11일 19:30:34.834:IKEv2:구문 분석 알림 페이로드
:NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) 다음
페이로드:없음, 예약됨:0x0, 길이:8
보안 프로토콜 ID:IKE, spi 크기:0, 유형
:NON_FIRST_FRAGS

*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:I_WAIT_AUTH 이벤트:**EV_RECV_AUTH**
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):작업:작업_Null
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:I_PROC_AUTH 이벤트:EV_CHK4_NOTIFY
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:I_PROC_AUTH 이벤트:**EV_PROC_MSG**
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:I_PROC_AUTH 이벤트
:EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_인출됨
_FOR_PROF_SEL
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:I_PROC_AUTH 이벤트
:EV_GET_POLICY_BY_PEERID

*11월 11일 19:30:34.834:IKEv2:툴킷 정책에 제안 단계 1-prop 추가
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):IKEv2 프로파일 'IKEV2-SETUP' 사용
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트 :EV_VERIFY_POLICY_BY_PEERID
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트:EV_CHK_AUTH_TYPE
*11월 11일 19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트:EV_GET_PRESHR_KEY
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트:**EV_VERIFY_AUTH**
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트:EV_CHK_EAP
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트 :**EV_NOTIFY_AUTH_DONE**
*11월 11일 19:30:34.835:IKEv2:AAA 그룹 권한 부여가 구성되지 않음
*11월 11일 19:30:34.835:IKEv2:AAA 사용자 권한 부여가 구성되지 않음
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트 :EV_CHK_CONFIG_MODE
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트:EV_CHK4_IC
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트:EV_CHK_IKE_ONLY
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:I_PROC_AUTH 이벤트:EV_PROC_SA_TS
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B

R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:AUTH_DONE 이벤트:EV_확인
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):작업:작업_Null
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:AUTH_DONE 이벤트:EV_PKI_SESH_CLOSE
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):PKI 세션 닫기
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:AUTH_DONE 이벤트:EV_UPDATE_CAC_STATS
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:AUTH_DONE 이벤트:EV_INSERT_IKE
*11월 11일 19:30:34.835:IKEv2:Store mib index ikev2 1,
platform 60
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:AUTH_DONE 이벤트:EV_GEN_LOAD_IPSEC
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):비동기 요청이
대기되었습니다.

*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):
*11월 11일 19:30:34.835:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:AUTH_DONE 이벤트:EV_NO_이벤트
*11월 11일 19:30:34.835:IKEv2:KMI 메시지 8이 사용되었
습니다.수행한 작업이 없습니다.
*11월 11일 19:30:34.835:IKEv2:KMI 메시지 12가 사용되었
습니다.수행한 작업이 없습니다.
*11월 11일 19:30:34.835:IKEv2:모드 컨피그레이션 세트에
서 전송할 데이터가 없습니다.
*11월 11일 19:30:34.841:IKEv2:세션 8에 대해 SPI
0x9506D414와 연결된 ID 핸들 0x8000002 추가

*11월 11일 19:30:34.841:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:AUTH_DONE 이벤트
:EV_OK_RECD_LOAD_IPSEC
*11월 11일 19:30:34.841:IKEv2:(SA ID = 1):작업:작업_Null
*11월 11일 19:30:34.841:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001
CurState:AUTH_DONE 이벤트:EV_START_ACCT
*11월 11일 19:30:34.841:IKEv2:(SA ID = 1):어카운팅이 필
요하지 않음
*11월 11일 19:30:34.841:IKEv2:(SA ID = 1):SM Trace->
SA:I_SPI=F074D8BBD5A59F0B

	R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:AUTH_DONE 이벤트:EV_CHECK_DUPLES *11월 11일 19:30:34.841:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 000000000001 Cur State: AUTH_DONE 이벤트:EV_CHK4_ROLE		
Tunnel이 Initiator에서 작동되고 상태가 READY로 *표시됩니다*.	*11월 11일 19:30:34.841:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 00000000001 CurState: READYEvent:EV_CHK_IKE_ONLY *11월 11일 19:30:34.841:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I) MsgID = 0000000001 CurState:READY 이벤트:EV_I_확인	*11월 11일 19시 30분 34초 840:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 000000000001 Cur 상태: **READY** 이벤트:EV_R_확인 *11월 11일 19:30:34.840:IKEv2:(SA ID = 1):SM Trace-> SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R) MsgID = 0000000001 CurState:READY 이벤트:EV_NO_이벤트	Responder에 터널이 있습니다.일반적으로 Responder 터널은 Initiator보다 먼저 나타납니다.

CHILD_SA 디버그

이 교환은 단일 요청/응답 쌍으로 구성되며 IKEv1에서 2단계 교환이라고 합니다. 초기 교환이 완료된 후 IKE_SA의 양쪽 끝에 의해 시작될 수 있습니다.

라우터 1 CHILD_SA 메시지 설명	**디버깅**	**라우터 2 CHILD_SA 메시지 설명**
라우터 1이 CHILD_SA 교환을 시작합니다 .CREATE_CHILD_SA 요청입니다 .CHILD_SA 패킷에는 일반적으로 다음이 포함됩니다. • SA HDR(version.flags/exchange type) • Nonce Ni(선택 사항):CHILD_SA가 초기 교환의 일부로 생성된 경	*11월 11일 19:31:35.873:IKEv2:디스패처에서 패킷 가져오기 *11월 11일 19:31:35.873:IKEv2:pak 큐에서 항목 처리 *11월 11일 19:31:35.873:IKEv2:(SA ID = 2):요청에 mess_id 3;3~7까지 *11월 11일 19:31:35.873:IKEv2:(SA ID = 2):다음 페이로드:ENCR, 버전:2.0 **Exchange 유형:CREATE_CHILD_SA**, 플래그: **개시자** 메시지 ID:3, 길이:396 페이로드 내용: **SA** 다음 페이로드:N, 예약됨:0x0, 길이:152 마지막 제안:0x0, 예약됨:0x0, 길이:148 제안:1, 프로토콜 ID:IKE, SPI 크기:8, #trans:마지막 변환 15개:0x3, 예약됨:0x0:길이:12 유형:1, 예약됨:0x0, id:AES-CBC 마지막 변환:0x3, 예약됨:0x0:길이:12	

우 두 번째 KE 페이로드 및 nonce를 전송하지 않아야 함)

- SA 페이로드
- KEi(키 선택 사항):CREATE_CHILD_SA 요청에는 CHILD_SA에 대한 전달 비밀의 강력한 보장을 활성화하기 위해 추가 DH 교환을 위한 KE 페이로드가 선택적으로 포함될 수 있습니다.SA에서 제공하는 DH 그룹이 서로 다른 경우, KEi는 응답자가 수락할 것으로 기대하는 그룹의 요소여야 합니다.잘못 추정한 경우 CREATE_CHILD_SA 교환이 실패하고 다른 KEi로 다시 시도해야 합니다.
- N(Notify payload-optional). Notify Payload는 오류 조건 및 상태 전환과 같은 정보 데이터를 IKE 피어로 전송하는 데 사용됩니다.알림 페이로드는 응답 메시지(일반적

유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA512
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA384
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA256
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:MD5
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA512
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA384
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA256
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:MD596
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1536_MODP/그룹 5
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
N 다음 페이로드:KE, 예약됨:0x0, 길이:24
KE 다음 페이로드:알림, 예약됨:0x0, 길이:136
DH 그룹:2, 예약됨:0x0

*11월 11일 19:31:35.874:IKEv2:구문 분석 알림 페이로드 :SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) 다음 페이로드:없음, 예약됨:0x0, 길이:12
보안 프로토콜 ID:IKE, spi 크기:0, 유형 :SET_WINDOW_SIZE

*11월 11일 19:31:35.874:IKEv2:(**SA ID = 2**):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:준비 이벤트: **EV_RECV_CREATE_CHILD**
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):작업:작업_Null
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:CHILD_R_INIT 이벤트 :EV_RECV_CREATE_CHILD
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):작업:작업_Null
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:CHILD_R_INIT 이벤트:EV_VERIFY_MSG
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->

으로 요청이 거부된 이유를 지정), INFORMATIONAL Exchange(IKE 요청에 없는 오류를 보고하기 위해) 또는 기타 메시지에 나타날 수 있습니다.이 CREATE_CHILD_SA 교환이 IKE_SA 이외의 기존 SA를 재입력 중인 경우 REKEY_SA 유형의 선행 N 페이로드는 키 재지정된 SA를 식별해야 합니다.이 CREATE_CHILD_SA 교환에서 기존 SA를 재지정하지 않으면 N 페이로드를 생략해야 합니다.

SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_INIT 이벤트:EV_CHK_CC_TYPE
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_IKE 이벤트: **EV_REKEY_IKESA**
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_IKE 이벤트:EV_GET_IKE_POLICY
*11월 11일 19:31:35.874:IKEv2:% **주소별 사전 공유 키 10.0.0.2**
*11월 11일 19:31:35.874:IKEv2:% 주소별 사전 공유 키 가져오기 10.0.0.2
*11월 11일 19:31:35.874:IKEv2:툴킷 정책에 제안 단계 1-prop 추가
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):IKEv2 프로파일 'IKEV2-SETUP' 사용
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_IKE 이벤트:EV_PROC_MSG
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_IKE 이벤트:EV_SET_POLICY
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):**구성된 정책 설정**
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_BLD_MSG 이벤트:EV_GEN_DH_KEY
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_BLD_MSG 이벤트:EV_NO_이벤트
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_BLD_MSG 이벤트
:EV_OK_RECD_DH_PUBKEY_RESP
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):작업:작업_Null
*11월 11일 19:31:35.874:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_BLD_MSG 이벤트
:**EV_GEN_DH_SECRET**
*11월 11일 19:31:35.881:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_BLD_MSG 이벤트:EV_NO_이벤트
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace->

SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_BLD_MSG 이벤트
:EV_OK_RECD_DH_SECRET_RESP
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):작업:작업_Null
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003
CurState:CHILD_R_BLD_MSG 이벤트:EV_BLD_MSG
*11월 11일 19:31:35.882: **IKEv2:구성 알림 페이로드**
:SET_WINDOW_SIZE
페이로드 내용:
SA 다음 페이로드:N, 예약됨:0x0, 길이:56
마지막 제안:0x0, 예약됨:0x0, 길이:52
제안:1, 프로토콜 ID:IKE, SPI 크기:8, #trans:마지막 변환
:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
N 다음 페이로드:KE, 예약됨:0x0, 길이:24
KE 다음 페이로드:알림, 예약됨:0x0, 길이:136
DH 그룹:2, 예약됨:0x0
NOTIFY(SET_WINDOW_SIZE) 다음 페이로드:없음, 예약
됨:0x0, 길이:12
보안 프로토콜 ID:IKE, spi 크기:0, 유형
:SET_WINDOW_SIZE
*11월 11일 19:31:35.869:IKEv2:(**SA ID = 2**):다음 페이로드
:ENCR, 버전:2.0 Exchange 유형: **CREATE_CHILD_SA**, 플
래그: **INITIATOR** 메시지 ID:2, 길이:460
페이로드 내용:
ENCR 다음 페이로드:SA, 예약됨:0x0, 길이:432
*11월 11일 19:31:35.873:IKEv2:구성 알림 페이로드
:SET_WINDOW_SIZE
페이로드 내용:
SA 다음 페이로드:N, 예약됨:0x0, 길이:152
마지막 제안:0x0, 예약됨:0x0, 길이:148
제안:1, 프로토콜 ID:IKE, SPI 크기:8, #trans:마지막 변환
15개:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA512
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA384
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA256

이 패킷은 라우터 2에서 수신됩니다.

마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:MD5
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA512
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA384
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA256
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:MD596
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1536_MODP/그룹 5
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
N 다음 페이로드:KE, 예약됨:0x0, 길이:24
KE 다음 페이로드:알림, 예약됨:0x0, 길이:136
DH 그룹:2, 예약됨:0x0
NOTIFY(SET_WINDOW_SIZE) 다음 페이로드:없음, 예약됨:0x0, 길이:12
보안 프로토콜 ID:IKE, spi 크기:0, 유형:SET_WINDOW_SIZE

*11월 11일 19:31:35.882:IKEv2:(**SA ID = 2**):다음 페이로드:ENCR, 버전:2.0 Exchange 유형: **CREATE_CHILD_SA,** 플래그: **RESPONDER MSG-RESPONSE** 메시지 ID:3, 길이:300
페이로드 내용:
SA 다음 페이로드:N, 예약됨:0x0, 길이:56
마지막 제안:0x0, 예약됨:0x0, 길이:52
제안:1, 프로토콜 ID:IKE, SPI 크기:8, #trans:마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
N 다음 페이로드:KE, 예약됨:0x0, 길이:24
KE 다음 페이로드:알림, 예약됨:0x0, 길이:136
DH 그룹:2, 예약됨:0x0

*11월 11일 19:31:35.882:IKEv2:구문 분석 알림 페이로드:SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) 다음 페이로드:없음, 예약됨:0x0, 길이:12
보안 프로토콜 ID:IKE, spi 크기:0, 유형:SET_WINDOW_SIZE

*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6

이제 라우터 2가 CHILD_SA 교환에 대한 응답을 작성합니다
.CREATE_CHILD_SA 응답입니다
.CHILD_SA 패킷에는 일반적으로 다음이 포함됩니다.

- SA HDR(version.flags/exchange type)
- Nonce Ni(선택 사항):CHILD_SA가 초기 교환의 일부로 생성된 경우 두 번째 KE 페이로드와 nonce를 전송하지 않아야 합니다.
- SA 페이로드
- KEi(키 선택 사항

R_SPI=F14E2BBA78024DE3(I) MsgID = 000000000003
CurState: **CHILD_I_WAIT** 이벤트:
RECV_RECV_RECV_EV 생성_하위
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):작업:작업_Null
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 00000000003
CurState: **CHILD_I_PROC** 이벤트:EV_CHK4_NOTIFY
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_PROC 이벤트: **EV_VERIFY_MSG**
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_PROC 이벤트:EV_PROC_MSG
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_PROC 이벤트:EV_CHK4_PFS
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_PROC 이벤트:EV_GEN_DH_비밀
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_PROC 이벤트:EV_NO_이벤트
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_PROC 이벤트
:EV_OK_RECD_DH_SECRET_RESP
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):작업:작업_Null
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_PROC 이벤트:EV_CHK_IKE_REKEY
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_PROC 이벤트:EV_GEN_SKEYID
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):skeyid 생성
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000000003
CurState: **CHILD_I_DONE** 이벤트:
EV_NEW_ACTIVATE_NEW_ACTIVATE_NEW_NEW SA(_A)
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace->
SA:I_SPI=0C33DB40DBAADE6
R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003
CurState:CHILD_I_DONE 이벤트

):CREATE_CHILD_SA 요청에는 CHILD_SA에 대한 전달 비밀의 강력한 보장을 활성화하기 위해 추가 DH 교환을 위한 KE 페이로드가 선택적으로 포함될 수 있습니다.SA에서 제공하는 DH 그룹이 서로 다른 경우, KEi는 응답자가 수락할 것으로 기대하는 그룹의 요소여야 합니다.잘못 추정한 경우 CREATE_CHILD_SA 교환이 실패하고 다른 KEi로 다시 시도해야 합니다.

- N(페이로드 알림 - 선택 사항):Notify Payload는 오류 조건 및 상태 전환과 같은 정보 데이터를 IKE 피어로 전송하는 데 사용됩니다.알림 페이로드는 응답 메시지(일반적으로 요청이 거부된 이유를 지정), 정보 교환(IKE 요청에 없는 오류를 보고하기 위해) 또는 발신자 기능을 나타내거나 요청의 의미를

:EV_UPDATE_CAC_STATS
*11월 11일 19:31:35.890:IKEv2:새 ikev2 sa 요청이 활성화됨
*11월 11일 19:31:35.890:IKEv2:발신 협상에 대한 개수를 줄이지 못했습니다.
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003 CurState:CHILD_I_DONE 이벤트:EV_CHECK_DUPLES
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003 CurState:CHILD_I_DONE 이벤트:EV_확인
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003 CurState:종료 이벤트:EV_CHK_보류 중
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):메시지 ID가 3인 처리된 응답, 요청 범위는 4~8입니다.
*11월 11일 19:31:35.890:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I) MsgID = 000000003 **CurState:종료** 이벤트:EV_NO_이벤트

수정하기 위해 다른 메시지에 나타날 수 있습니다.이 CREATE_CHILD_SA 교환이 IKE_SA 이외의 기존 SA를 재입력하는 경우 REKEY_SA 유형의 선행 N 페이로드가 키 재지정되는 SA를 식별해야 합니다.이 CREATE_CHILD_SA 교환에서 기존 SA를 재지정하지 않으면 N 페이로드를 생략해야 합니다.

라우터 2가 응답을 보내고 새 CHILD SA 활성화를 완료합니다.

*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):다음 페이로드:ENCR, 버전:2.0 Exchange 유형: **CREATE_CHILD_SA**, 플래그: **RESPONDER MSG-RESPONSE** 메시지 ID:3, 길이:300
페이로드 내용:
ENCR 다음 페이로드:SA, 예약됨:0x0, 길이:272

*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:CHILD_R_BLD_MSG 이벤트:**EV_CHK_IKE_REKEY**
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:CHILD_R_BLD_MSG 이벤트:EV_GEN_SKEYID
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):**skeyid 생성**
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:CHILD_R_DONE 이벤트:**EV_ACTIVATE_NEW_SA**
*11월 11일 19:31:35.882:IKEv2:Store mib index ikev2 3, platform 62

라우터 1은 라우터 2에서 응답 패킷을 수신하고 CHILD_SA 활성화를 완료합니다.

*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:CHILD_R_DONE 이벤트 :EV_UPDATE_CAC_STATS
*11월 11일 19:31:35.882:IKEv2:새 ikev2 sa 요청이 활성화됨
*11월 11일 19:31:35.882:IKEv2: 수신 협상에 대한 수를 감소시키지 못했습니다.
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 00000000003 CurState: **CHILD_R_DONE** 이벤트:EV_CHECK_DUPLES
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:CHILD_R_DONE 이벤트:EV_확인
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:CHILD_R_DONE 이벤트 :EV_START_DEL_NEG_TMR
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):작업:작업_Null
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 CurState:종료 이벤트:EV_CHK_보류 중
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):메시지 ID가 3인 보낸 응답, 요청이 4에서 8까지 수락될 수 있음
*11월 11일 19:31:35.882:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R) MsgID = 000000003 **CurState:종료** 이벤트:EV_NO_이벤트

터널 확인

ISAKMP

명령

show crypto ikev2 sa detailed

라우터 1 출력

```
Router1#show crypto ikev2 sa  detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.0.1/500 10.0.0.2/500 none/none READY
Encr: AES-CBC, keysize: 128,
```

```
Hash: SHA96, DH Grp:2,
Auth sign: PSK, Auth verify: PSK
Life/Active Time: 120/10 sec
CE id: 1006, Session-id: 4
Status Description: Negotiation done
Local spi: E58F925107F8B73F Remote spi: AFD098F4147869DA
Local id: 10.0.0.1
Remote id: 10.0.0.2
Local req msg id: 2 Remote req msg id: 0
Local next msg id: 2 Remote next msg id: 0
Local req queued: 2 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

라우터 2 출력

```
Router2#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 10.0.0.2/500 10.0.0.1/500 none/none READY
Encr: AES-CBC, keysize: 128, Hash: SHA96,
DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 120/37 sec
CE id: 1006, Session-id: 4
Status Description: Negotiation done
Local spi: AFD098F4147869DA Remote spi: E58F925107F8B73F
Local id: 10.0.0.2
Remote id: 10.0.0.1
Local req msg id: 0 Remote req msg id: 2
Local next msg id: 0 Remote next msg id: 2
Local req queued: 0 Remote req queued: 2
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

IPsec

명령

show crypto ipsec sa

참고:이 출력에서는 IKEv1과 달리 PFS DH 그룹 값이 "PFS (Y/N):N, DH 그룹:첫 번째 터널 협상 중에 none"이 표시되지만 rekey가 발생하면 오른쪽 값이 나타납니다.Cisco 버그 ID CSCug67056에 동작에 대해 설명하더라도 이는 버그가 아닙니다.

IKEv1과 IKEv2의 차이점은 후자의 하위 SA는 AUTH 교환 자체의 일부로 생성된다는 것입니다.암호화 맵에 구성된 DH 그룹은 키 재설정 중에만 사용됩니다.따라서 'PFS(Y/N):N, DH 그룹:none'은 첫 번째 키 재설정 전까지 적용됩니다.

IKEv1에서는 하위 SA가 빠른 모드 중에 생성되고 CREATE_CHILD_SA 메시지에는 새 공유 암호를 파생하기 위해 DH 매개변수를 지정하는 키 교환 페이로드를 전달하는 프로비저닝이 있기 때문에 다른 동작이 표시됩니다.

라우터 1 출력

```
Router1#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0,
local addr 10.0.0.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt:
10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt:
10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.0.1,
remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xF6083ADD(4127734493)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x6B74CB79(1802816377)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 18, flow_id: SW:18,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec):
(4276853/3592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF6083ADD(4127734493)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 17, flow_id: SW:17,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key
lifetime (k/sec): (4276853/3592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:
```

```
outbound pcp sas:
```

라우터 2 출력

```
Router2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.0.2,
remote crypto endpt.: 10.0.0.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x6B74CB79(1802816377)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xF6083ADD(4127734493)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 17, flow_id: SW:17,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime
(k/sec): (4347479/3584)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x6B74CB79(1802816377)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 18, flow_id: SW:18,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key
lifetime (k/sec): (4347479/3584)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

두 라우터 모두에서 **show crypto session** 명령의 출력을 확인할 수도 있습니다.이 출력은 터널 세션 상태를 UP-ACTIVE로 표시합니다.

```
Router1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map

Router2#show cry session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map
```

관련 정보

- IKEv2 패킷 교환 및 프로토콜 레벨 디버깅
- 기술 지원 및 문서 – Cisco Systems