PSK를 사용하여 사이트 간 VPN에 대한 IOS IKEv2 디버깅 문제 해결

목차

소개

이 문서에서는 PSK(Unshared Key)가 사용될 때 Cisco IOS®에서 IKEv2(Internet Key Exchange version 2)를 디버깅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 IKEv2의 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

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

배경 정보

이 문서에서는 컨피그레이션의 특정 디버그 라인을 변환하는 방법에 대한 정보를 제공합니다.

핵심 문제

IKEv2의 패킷 교환은 IKEv1의 패킷 교환과 근본적으로 다릅니다. IKEv1에는 6개의 Phase1 교환과 3개의 Phase2 교환으로 구성된 이후 Phase1 교환이 명확하게 구분되어 있었습니다. IKEv2 교환은 가변적입니다. 차이점 및 패킷 교환에 대한 자세한 내용은 IKEv2 패킷 교환 및 프로토콜 레벨 디버깅을 다시 참조하십시오.

라우터 컨피그레이션

이 섹션에서는 이 문서에 사용된 컨피그레이션을 소개합니다.

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 다음 debug 명령을 사용합니다.

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

라우터 1(개시자) 메시지 설명	디버그	라우 2(Respo 메시지
라우터 1은 피어 ASA 10.0.0.2의 암호화 acl과 일치하는 패킷을 수신합니다. SA 생성 시작	*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:% 주소 10.0.0.2로 사전 공유 키 가져오기 *11월 11일 19:30:34.811: IKEv2:툴킷 정책에 제안 PHASE1-prop 추가 *11월 11일 19:30:34.811: IKEv2:(1): IKE 프로필 선택 IKEV2-SETUP *11월 11일 19:30:34.811: IKEv2:New ikev2 sa request admitted *11월 11일 19:30:34.811: IKEv2:발신 협상 sa 수 1씩 증가	
첫 번째 메시지 쌍은 IKE_SA_INIT 교환입니다. 이러한 메시지는 암호화 알고리즘을 협상하고 논스를 교환하며 Diffie-Hellman 교환을 수행합니다. 관련 구성: `crypto ikev2 제안 PHASE1-prop encryption 3des aes-cbc-128 integrity sha1 group 2crypto ikev2 keyring peer1 address 10.0.0.2 255.255.255.0 hostname host1`	*11월 11일 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: IDLE 이벤트: EV_INIT_SA *11월 11일 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: 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=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: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=0000000000000000 (I) MsgID = 00000000 CurState: 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=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event:EV_GEN_DH_KEY *11월 11일 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT 이벤트: EV_NO_EVENT *11월 11일 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT 이벤트:	

pre-shared-key local cisco pre-shared-key remote cisco	EV_OK_RECD_DH_PUBKEY_RESP *11월 11일 19:30:34.811: IKEv2:(SA ID = 1):작업: Action_Null *11월 11일 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT 이벤트: EV_GET_CONFIG_MODE *11월 11일 19:30:34.811: IKEv2:IKEv2 개시자 - IKE_SA_INIT exch에서 전송할 구성 데이터가 없습니다. *11월 11일 19:30:34.811: IKEv2:툴킷으로 전송할 컨피그레이션 데이터 없음: *11월 11일 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT 이벤트: EV_BLD_MSG *11월 11일 19:30:34.811: IKEv2:Construct Vendor Specific Payload: DELETE-REASON *11월 11일 19:30:34.811: IKEv2:Construct Vendor Specific Payload: (CUSTOM) *11월 11일 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *11월 11일 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP	
개시자가 IKE_INIT_SA 패킷을 구축합니다. 여기에는 ISAKMP 헤더 (SPI/version/flags), SAi1(IKE 개시자가 지원하는 암호화 알고리즘), KEi(개시자의 DH 공개 키 값) 및 N(개시자 Nonce)이 포함됩니다.	*11월 11일 19:30:34.811: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, flags:INITIATOR Message id: 0, length: 344 페이로드 내용: SA 다음 페이로드: KE, 예약: 0x0, 길이: 56 마지막 제안: 0x0, 예약됨: 0x0, 길이: 52 제안: 1, 프로토콜 ID: IKE, SPI 크기: 0, #trans: 5 마지막 변환: 0x3, 예약: 0x0: 길이: 8 유형: 1, 예약됨: 0x0, id: 3DES 마지막 변환: 0x3, 예약됨: 0x0: 길이: 12 유형: 1, 예약: 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/Group 2 KE 다음 페이로드: N, 예약: 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: NOTIFY, 예약됨: 0x0, 길이: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28 보안 프로토콜 ID: IKE, spi 크기: 0, 유형: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) 다음 페이로드: 없음, 예	

	약됨: 0x0, 길이: 28 보안 프로토콜 ID: IKE, spi 크기: 0, 유형: NAT_DETECTION_DESTINATION_IP	
----------Initiator가 IKE_INIT_SA를 ---------->		
	*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:New ikev2 sa request admitted *11월 11일 19:30:34.814: IKEv2:수신 협상 sa 수 1씩 증가	응답자가 IKE_INIT 수신합니
	*Nov 11 19:30:34.814: IKEv2:Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 344 페이로드 내용: SA Next 페이로드: KE, 예약: 0x0, 길이: 56 마지막 제안: 0x0, 예약됨: 0x0, 길이: 52 제안: 1, 프로토콜 ID: IKE, SPI 크기: 0, #trans: 5 마지막 변환: 0x3, 예약: 0x0: 길이: 8 유형: 1, 예약됨: 0x0, id: 3DES 마지막 변환: 0x3, 예약됨: 0x0: 길이: 12 유형: 1, 예약: 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/Group 2 KE 다음 페이로드: N, 예약됨: 0x0, 길이: 136 DH 그룹: 2, 예약됨: 0x0 N 다음 페이로드: VID, 예약됨: 0x0, 길이: 24 *11월 11일 19:30:34.814: IKEv2:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID Next 페이로드: VID, 예약: 0x0, 길이: 23 *11월 11일 19:30:34.814: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: NOTIFY, reserved: 0x0, length: 21 *Nov 11 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28 보안 프로토콜 ID: IKE, spi 크기: 0, 유형: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.814: IKEv2:Parse Notify 페이로드: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload: NONE, reserved: 0x0, length: 28 보안 프로토콜 ID: IKE, spi 크기: 0, 유형:	Respond 해당 피어 한 SA 생 시작합니

	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 = 00000000 CurState: IDLE Event:EV_RECV_INIT *11월 11일 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 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 = 00000000 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 = 00000000 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 = 00000000 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 = 00000000 CurState: R_INIT 이벤트: EV_DETECT_NAT *11월 11일 19:30:34.814: IKEv2:(SA ID = 1):Process NAT discovery notify *11월 11일 19:30:34.814: IKEv2:(SA ID = 1):NAT 처리 시 src 알림 탐지 *11월 11일 19:30:34.814: IKEv2:(SA ID = 1):원격 주소 일치 *11월 11일 19:30:34.814: IKEv2:(SA ID = 1):NAT 처리, dst notify 탐지 *11월 11일 19:30:34.814: IKEv2:(SA ID = 1):로컬 주소 일치 *11월 11일 19:30:34.814: IKEv2:(SA ID = 1):NAT를 찾을 수 없음 *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 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 = 00000000 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 = 00000000 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 = 00000000 CurState: R_BLD_INIT 이벤트: EV_PKI_SESH_OPEN *11월 11일 19:30:34.814: IKEv2:(SA ID = 1):PKI 세션 열기 *11월 11일 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:EV_GEN_DH_KEY *11월 11일 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA:	Respond IKE_INIT 지를 확인 처리합니 개시자가 한 암호화 을 선택하 (2) 자체 D 밀 키를 계 고, (3) 이 IKE_SA에 모든 키를 할 수 있는 ID 값을 계 니다. 뒤에 는 모든 메 의 헤더를 한 모든 하 암호화 및 됩니다. 암 및 무결성 에 사용되 는 SKEYI 서 파생되 SK_e(암호 SK_a(인증 SK_d가 파 어 CHILD_SA 대한 추가 자료 도출 용되며, 각 향에 대하 의 SK_e SK_a가 계 니다. 관련 구성 : crypto ik 제안 PHASE encryptio aes-cbc-1 integrity

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT 이벤트: EV_NO_EVENT *11월 11일 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:EV_OK_RECD_PUBKEY_RESP *11월 11일 19:30:34.815: IKEv2:(SA ID = 1):작업: Action_Null *11월 11일 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: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 = 00000000 CurState: R_BLD_INIT 이벤트: EV_NO_EVENT *11월 11일 19:30:34.822: IKEv2:% 주소 10.0.0.1로 사전 공유 키 가져오기 *11월 11일 19:30:34.822: IKEv2:툴킷 정책에 제안 기본값 추가 *11월 11일 19:30:34.822: IKEv2:(2): IKE 프로필 선택 IKEV2-SETUP *11월 11일 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT 이벤트: EV_OK_RECD_DH_SECRET_RESP *11월 11일 19:30:34.822: IKEv2:(SA ID = 1):작업: Action_Null *11월 11일 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:EV_GEN_SKEYID *11월 11일 19:30:34.822: IKEv2:(SA ID = 1):Generate skeyid *11월 11일 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT 이벤트: EV_GET_CONFIG_MODE *11월 11일 19:30:34.822: IKEv2:IKEv2 responder - IKE_SA_INIT exch에서 전송할 컨피그레이션 데이터 없음 *11월 11일 19:30:34.822: IKEv2:툴킷으로 전송할 컨피그레이션 데이터 없음: *11월 11일 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT 이벤트: EV_BLD_MSG *11월 11일 19:30:34.822: IKEv2:공급업체별 페이로드 구성: DELETE-REASON *11월 11일 19:30:34.822: IKEv2:Construct Vendor Specific Payload: (CUSTOM) *11월 11일 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *11월 11일 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP *11월 11일 19:30:34.822: IKEv2:Construct 알림 페이로드: HTTP_CERT_LOOKUP_SUPPORTED	group 2 c ikev2 key KEYRNG pe address 10.0.0.1 255.255.2 hostname pre-share local cis pre-share remote ci

	*11월 11일 19:30:34.822: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, flags: RESPONDER MSG-RESPONSE Message id: 0, length: 449 페이로드 내용: SA 다음 페이로드: KE, 예약: 0x0, 길이: 48 마지막 제안: 0x0, 예약됨: 0x0, 길이: 44 제안: 1, 프로토콜 ID: IKE, SPI 크기: 0, #trans: 4 마지막 변환: 0x3, 예약: 0x0: 길이: 12 유형: 1, 예약: 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/Group 2 KE 다음 페이로드: N, 예약: 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: NOTIFY, 예약됨: 0x0, 길이: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 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: NOTIFY, 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	라우터 2 ASA1에서 신하는 IKE_SA_ 교환을 우 responde 지를 작성 다. 이 패 는 ISAKM 더(SPI/ 버 래그), SAr1(IKE 자가 선택 암호화 알 즘), KEr(자의 DH 키 값) 및 Respond Nonce가 되어 있습
	*11월 11일 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE 이벤트: EV_DONE *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 = 00000000 CurState: INIT_DONE 이벤트: EV_CHK4_ROLE *11월 11일 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =	Router2는 responde 지를 Rou 1로 전송 다.

	00000000 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 = 00000000 CurState: R_WAIT_AUTH 이벤트: EV_NO_EVENT *11월 11일 19:30:34.822: IKEv2:New ikev2 sa request admitted *11월 11일 19:30:34.822: IKEv2:발신 협상 작업 수 1씩 증가		
<----------Responder가 IKE_INIT_SA 메시지를 ----------			
라우터 1은 라우터 2로부터 IKE_SA_INIT 응답 패킷을 수신합니다.	*11월 11일 19:30:34.823: IKEv2:디스패처에서 패킷 가져오기 *11월 11일 19:30:34.823: IKEv2:디스패처에서 패킷 가져오기 *11월 11일 19:30:34.823: IKEv2:pak 큐에서 항목 처리	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE 이벤트 :EV_START_TMR	응답자가 프로세스 한 타이머 작합니다
Router1은 (1) 개시자 DH 비밀 키가 계산되고 (2) 개시자 skeyid도 생성됨을 확인하고 응답을 처리합니다.	*11월 11일 19:30:34.823: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, flags: RESPONDER MSG-RESPONSE Message id: 0, length: 449 페이로드 내용: SA 다음 페이로드: KE, 예약: 0x0, 길이: 48 마지막 제안: 0x0, 예약됨: 0x0, 길이: 44 제안: 1, 프로토콜 ID: IKE, SPI 크기: 0, #trans: 4 마지막 변환: 0x3, 예약: 0x0: 길이: 12 유형: 1, 예약: 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/Group 2 KE 다음 페이로드: N, 예약: 0x0, 길이: 136 DH 그룹: 2, 예약됨: 0x0 N 다음 페이로드: VID, 예약됨: 0x0, 길이: 24 *11월 11일 19:30:34.823: IKEv2:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID Next 페이로드: VID, 예약: 0x0, 길이: 23 *11월 11일 19:30:34.823: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: NOTIFY, reserved: 0x0, length: 21 *Nov 11 19:30:34.823: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP		

NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28
   보안 프로토콜 ID: IKE, spi 크기: 0, 유형: NAT_DETECTION_SOURCE_IP

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

*11월 11일 19:30:34.824: IKEv2:Parse Notify 페이로드: HTTP_CERT_LOOKUP_SUPPORTED
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Next payload: NONE, reserved: 0x0, length: 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 = 00000000 CurState: I_WAIT_INIT 이벤트: EV_RECV_INIT
*11월 11일 19:30:34.824: IKEv2:(SA ID = 1):IKE_SA_INIT 메시지 처리
*11월 11일 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 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 = 00000000 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 = 00000000 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 = 00000000 CurState: I_PROC_INIT 이벤트: EV_DETECT_NAT
*11월 11일 19:30:34.824: IKEv2:(SA ID = 1):Process NAT discovery notify
*11월 11일 19:30:34.824: IKEv2:(SA ID = 1):NAT 처리 시 src 알림 탐지
*11월 11일 19:30:34.824: IKEv2:(SA ID = 1):원격 주소 일치
*11월 11일 19:30:34.824: IKEv2:(SA ID = 1):NAT 처리, dst notify 탐지
*11월 11일 19:30:34.824: IKEv2:(SA ID = 1):로컬 주소 일치
*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 = 00000000 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 = 00000000 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 = 00000000 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 = 00000000 CurState: INIT_DONE 이벤트: EV_NO_EVENT *11월 11일 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE 이벤트: EV_OK_RECD_SECRET_RESP *11월 11일 19:30:34.831: IKEv2:(SA ID = 1):작업: Action_Null *11월 11일 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE 이벤트:EV_GEN_SKEYID *11월 11일 19:30:34.831: IKEv2:(SA ID = 1):Generate skeyid *11월 11일 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE 이벤트: EV_DONE *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 = 00000000 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 = 00000000 CurState: I_BLD_AUTH 이벤트: EV_GET_CONFIG_MODE *11월 11일 19:30:34.831: IKEv2:툴킷에 컨피그레이션 데이터 전송 *11월 11일 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH 이벤트: EV_CHK_EAP	
Initiator는 IKE_AUTH 교환을 시작하고 인증 페이로드를 생성합니다. IKE_AUTH 패킷에는 ISAKMP 헤더(SPI/버전/플래그), IDi(이니시에이터 ID), AUTH 페이로드, SAi2(IKEv1에서 2단계 변형 집합 교	*11월 11일 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event:EV_GEN_AUTH *11월 11일 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 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 R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 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 = 00000000 CurState: I_BLD_AUTH 이벤트: EV_SEND_AUTH	

환과 유사한 SA를 시작), TSi 및 TSr(이니시에이터 및 응답자 트래픽 선택기)이 포함됩니다. 여기에는 암호화된 트래픽을 전달/수신하기 위한 initiator 및 responder의 소스 및 목적지 주소가 각각 포함됩니다. 주소 범위는 해당 범위를 오가는 모든 트래픽이 터널링되도록 지정합니다. 제안서가 응답자에게 허용 가능한 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 phase2-prof set transform-set TS set ikev2-profile IKEV2-SETUP`	*11월 11일 19:30:34.831: IKEv2:Construct Vendor Specific Payload: CISCO-GRANITE *11월 11일 19:30:34.831: IKEv2:Construct Notify Payload: INITIAL_CONTACT *11월 11일 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *11월 11일 19:30:34.831: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *11월 11일 19:30:34.831: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS 페이로드 내용: VID 다음 페이로드: IDi, 예약: 0x0, 길이: 20 IDi 다음 페이로드: AUTH, reserved: 0x0, length: 12 ID 유형: IPv4 주소, 예약됨: 0x0 0x0 인증 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 payload: TSi, reserved: 0x0, length: 40 마지막 제안: 0x0, 예약됨: 0x0, 길이: 36 제안: 1, 프로토콜 id: ESP, SPI 크기: 4, #trans: 3 마지막 변환: 0x3, 예약: 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, reserved 0x0, reserved 0x0 TS 유형: TS_IPV4_ADDR_RANGE, 프로토콜 ID: 0, 길이: 16 시작 포트: 0, 종료 포트: 65535 시작 주소: 0.0.0.0, 끝 주소: 255.255.255.255 TSr 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 24 TS 수: 1, reserved 0x0, reserved 0x0 TS 유형: TS_IPV4_ADDR_RANGE, 프로토콜 ID: 0, 길이: 16 시작 포트: 0, 종료 포트: 65535 시작 주소: 0.0.0.0, 끝 주소: 255.255.255.255 NOTIFY(INITIAL_CONTACT) 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 8 보안 프로토콜 ID: IKE, spi 크기: 0, 유형: INITIAL_CONTACT NOTIFY(SET_WINDOW_SIZE) 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 12 보안 프로토콜 ID: IKE, spi 크기: 0, 유형: SET_WINDOW_SIZE NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved:	

0x0, length: 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):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: INITIATOR Message id: 1, length: 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 = 000000001 CurState: I_WAIT_AUTH 이벤트: EV_NO_EVENT

----------Initiator sent IKE_AUTH ---------->

*11월 11일 19:30:34.832: IKEv2:디스패처에서 패킷 가져오기
*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. 1~1이 필요합니다.
*11월 11일 19:30:34.832: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: INITIATOR Message id: 1, length: 556
페이로드 내용:
*11월 11일 19:30:34.832: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDi, reserved: 0x0, length: 20
IDi 다음 페이로드: AUTH, reserved: 0x0, length: 12
ID 유형: IPv4 주소, 예약됨: 0x0 0x0
AUTH Next payload: 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: 특성 유형: 내부 IP4 DNS, 길이: 0
*11월 11일 19:30:34.832: 특성 유형: 내부 IP4 DNS, 길이: 0
*11월 11일 19:30:34.832: 속성 유형: 내부 IP4 NBNS, 길이: 0
*11월 11일 19:30:34.832: 속성 유형: 내부 IP4 NBNS, 길이: 0
*11월 11일 19:30:34.832: 특성 유형: 내부 IP4 서브넷, 길이: 0
*11월 11일 19:30:34.832: 속성 유형: 애플리케이션 버전, 길이: 257
특성 유형: 알 수 없음 - 28675, 길이: 0
*11월 11일 19:30:34.832: 속성 유형: 알 수 없음 - 28672, 길이: 0
*11월 11일 19:30:34.832: 속성 유형: 알 수 없음 - 28692, 길이: 0
*11월 11일 19:30:34.832: 속성 유형: 알 수 없음 - 28681, 길이: 0
*11월 11일 19:30:34.832: 속성 유형: 알 수 없음 - 28674, 길이: 0
*11월 11일 19:30:34.832: SA Next payload: TSi, reserved: 0x0, length: 40
마지막 제안: 0x0, 예약됨: 0x0, 길이: 36

라우터 2
우터 1로
수신한 인
이터를 수
고 확인합

관련 구성

```
crypto ip
ikev2 ips
proposal
protocol
encryptio
256 proto
esp integ
sha-1 md5
```

	제안: 1, 프로토콜 id: ESP, SPI 크기: 4, #trans: 3 마지막 변환: 0x3, 예약: 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, reserved 0x0, reserved 0x0 TS 유형: TS_IPV4_ADDR_RANGE, 프로토콜 ID: 0, 길이: 16 시작 포트: 0, 종료 포트: 65535 시작 주소: 0.0.0.0, 끝 주소: 255.255.255.255 TSr 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 24 TS 수: 1, reserved 0x0, reserved 0x0 TS 유형: TS_IPV4_ADDR_RANGE, 프로토콜 ID: 0, 길이: 16 시작 포트: 0, 종료 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 = 00000001 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 = 00000001 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 = 00000001 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 = 00000001 CurState: R_WAIT_AUTH 이벤트: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETTED_FOR_PROF_SEL *11월 11일 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH 이벤트: EV_GET_POLICY_BY_PEERID *11월 11일 19:30:34.833: IKEv2:(1): IKE 프로필 선택 IKEV2-SETUP *11월 11일 19:30:34.833: IKEv2:% 주소 10.0.0.1로 사전 공유 키 가져오기 *11월 11일 19:30:34.833: IKEv2:% 주소 10.0.0.1로 사전 공유 키 가져오기 *11월 11일 19:30:34.833: IKEv2:툴킷 정책에 제안 기본값 추가 *11월 11일 19:30:34.833: IKEv2:(SA ID = 1):IKEv2 프로필 'IKEV2-SETUP' 사용 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =	라우터 2 우터 1에 신한 IKE_AUT 킷에 대한 을 빌드합 이 응답 패 는 ISAKM 더(SPI/ 버 래그), IDr.(respo identity), 페이로드 SAr2(IKE 서 2단계 집합 교환 사한 SA를 작합니다 및 TSr(In 및 Respo Traffic selector) 함됩니다 에는 암호 트래픽을 /수신하기 initiator 및 responde

	00000001 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 = 00000001 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 = 00000001 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 = 00000001 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 = 00000001 CurState: R_VERIFY_AUTH 이벤트: EV_CHK_AUTH_TYPE *11월 11일 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 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 = 00000001 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 = 00000001 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 = 00000001 CurState: R_VERIFY_AUTH 이벤트: EV_CHK_REDIRECT *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 = 00000001 CurState: R_VERIFY_AUTH 이벤트: EV_NOTIFY_AUTH_DONE *11월 11일 19:30:34.833: IKEv2:AAA 그룹 권한 부여가 구성되지 않음 *11월 11일 19:30:34.833: IKEv2:AAA 사용자 권한 부여가 구성되지 않음 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH 이벤트: EV_CHK_CONFIG_MODE *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH 이벤트: EV_SET_RECD_CONFIG_MODE *11월 11일 19:30:34.833: IKEv2:툴킷에서 컨피그레이션 데이터 수신: *11월 11일 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =	스 및 목적 주소가 각 함됩니다 범위는 해 위를 오기 든 트래픽 널링되도 정합니다 한 매개변 ASA1에서 신한 매개 와 동일합

	00000001 CurState: R_VERIFY_AUTH 이벤트: EV_PROC_SA_TS *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH 이벤트: EV_GET_CONFIG_MODE *11월 11일 19:30:34.833: IKEv2: 컨피그레이션 응답 구성 오류 *11월 11일 19:30:34.833: IKEv2:툴킷으로 전송할 컨피그레이션 데이터 없음: *11월 11일 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 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 = 00000001 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 = 00000001 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 = 00000001 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 = 00000001 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 = 00000001 CurState: R_BLD_AUTH 이벤트: EV_SEND_AUTH *11월 11일 19:30:34.833: IKEv2:Construct Vendor Specific Payload: CISCO-GRANITE *11월 11일 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *11월 11일 19:30:34.833: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *11월 11일 19:30:34.833: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS	
	*11월 11일 19:30:34.833: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 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 = 00000001 CurState: AUTH_DONE 이벤트: EV_OK *11월 11일 19:30:34.833: IKEv2:(SA ID = 1):작업: Action_Null *11월 11일 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =	Respond IKE_AUT 대한 응답 냅니다.

	00000001 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 = 00000001 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 = 00000001 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 = 00000001 CurState: AUTH_DONE 이벤트: EV_GEN_LOAD_IPSEC *11월 11일 19:30:34.834: IKEv2:(SA ID = 1):비동기 요청 대기 *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 = 00000001 CurState: AUTH_DONE 이벤트: EV_NO_EVENT	
<----------응답자가 IKE_AUTH를 전송했습니다----------			
Initiator가 Responder로부터 응답을 수신합니다.	*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 = 00000001 CurState: AUTH_DONE 이벤트: EV_OK_RECD_LOAD_IPSEC *11월 11일 19:30:34.840: IKEv2:(SA ID = 1):작업: Action_Null *11월 11일 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 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 = 00000001 CurState: AUTH_DONE 이벤트: EV_CHECK_DUPE *11월 11일 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B	Respond SAD에 항 삽입합니

		R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE 이벤트: EV_CHK4_ROLE	
라우터 1은 이 패킷의 인증 데이터를 확인하고 처리합니다. 그런 다음 라우터 1은 이 SA를 SAD에 삽입합니다.	*11월 11일 19:30:34.834: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 252 페이로드 내용: *11월 11일 19:30:34.834: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDr., reserved: 0x0, length: 20 IDr. 다음 페이로드: AUTH, reserved: 0x0, length: 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: 3 마지막 변환: 0x3, 예약: 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, reserved 0x0, reserved 0x0 TS 유형: TS_IPV4_ADDR_RANGE, 프로토콜 ID: 0, 길이: 16 시작 포트: 0, 종료 포트: 65535 시작 주소: 0.0.0.0, 끝 주소: 255.255.255.255 TSr 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 24 TS 수: 1, reserved 0x0, reserved 0x0 TS 유형: TS_IPV4_ADDR_RANGE, 프로토콜 ID: 0, 길이: 16 시작 포트: 0, 종료 포트: 65535 시작 주소: 0.0.0.0, 끝 주소: 255.255.255.255 *11월 11일 19:30:34.834: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12 보안 프로토콜 ID: IKE, spi 크기: 0, 유형: SET_WINDOW_SIZE *Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8 보안 프로토콜 ID: IKE, spi 크기: 0, 유형: ESP_TFC_NO_SUPPORT	

*11월 11일 19:30:34.834: IKEv2:Parse Notify Payload:
NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) Next payload:
NONE, reserved: 0x0, length: 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 =
00000001 CurState: I_WAIT_AUTH Event:EV_RECV_AUTH
*11월 11일 19:30:34.834: IKEv2:(SA ID = 1):작업: Action_Null
*11월 11일 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000001 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 =
00000001 CurState: I_PROC_AUTH Event:EV_PROC_MSG
*11월 11일 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000001 CurState: I_PROC_AUTH 이벤트:
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
*11월 11일 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000001 CurState: I_PROC_AUTH 이벤트:
EV_GET_POLICY_BY_PEERID
*11월 11일 19:30:34.834: IKEv2: 툴킷 정책에 제안 PHASE1-prop 추가
*11월 11일 19:30:34.834: IKEv2:(SA ID = 1):IKEv2 프로필 'IKEV2-SETUP'
사용
*11월 11일 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000001 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 =
00000001 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 =
00000001 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 =
00000001 CurState: I_PROC_AUTH Event:EV_VERIFY_AUTH
*11월 11일 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000001 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 =

00000001 CurState: I_PROC_AUTH Event: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 =
00000001 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 =
00000001 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 =
00000001 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 =
00000001 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 =
00000001 CurState: AUTH_DONE 이벤트: EV_OK
*11월 11일 19:30:34.835: IKEv2:(SA ID = 1):작업: Action_Null
*11월 11일 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000001 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 =
00000001 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 =
00000001 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 =
00000001 CurState: AUTH_DONE 이벤트: EV_GEN_LOAD_IPSEC
*11월 11일 19:30:34.835: IKEv2:(SA ID = 1):비동기 요청 대기

*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 =
00000001 CurState: AUTH_DONE 이벤트: EV_NO_EVENT
*11월 11일 19:30:34.835: IKEv2:KMI 메시지 8이 사용되었습니다. 수행된
작업이 없습니다.
*11월 11일 19:30:34.835: IKEv2:KMI 메시지 12가 사용되었습니다. 수행된
작업이 없습니다.
*11월 11일 19:30:34.835: IKEv2:No data to send in mode config set.
*11월 11일 19:30:34.841: 세션 8에 대한 SPI 0x9506D414와 연결된

	IKEv2:IDENT 핸들 0x80000002 추가 *11월 11일 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE 이벤트: EV_OK_RECD_LOAD_IPSEC *11월 11일 19:30:34.841: IKEv2:(SA ID = 1):작업: Action_Null *11월 11일 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE 이벤트: EV_START_ACCT *11월 11일 19:30:34.841: IKEv2:(SA ID = 1):계정 관리가 필요하지 않음 *11월 11일 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE 이벤트: EV_CHECK_DUPE *11월 11일 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE 이벤트: EV_CHK4_ROLE		
터널이 Initiator에서 가동 중이고 상태는 READY로 표시됩니다.	*11월 11일 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 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 = 00000001 CurState: READY 이벤트: EV_I_OK	*11월 11일 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: READY 이벤트: EV_R_OK *11월 11일 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: READY 이벤트: EV_NO_EVENT	터널이 Respond 서 작동 중 다. Respo 터널은 일 으로 Initia 다 먼저 입 .

자식_SA 디버그

이 교환은 단일 요청/응답 쌍으로 구성되며 IKEv1에서 2단계 교환이라고 했습니다. 초기 교환이 완료된 후 IKE_SA의 어느 한 쪽 끝에 시작할 수 있습니다.

라우터 1 CHILD_SA 메시지 설명	디버그	라우터 2 CHILD_SA 메시지 설
라우터 1은 CHILD_SA 교환을 시작합니다. CREATE_CHILD_SA 요청입니다. CHILD_SA 패킷에는 일반적으로 다음이 포함됩니다. • SA HDR(version.flags/exchange 유형)	*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	

• Nonce Ni(선택 사항): CHILD_SA가 초기 교환의 일부로 생성되는 경우 두 번째 KE 페이로드와 nonce를 보내지 않아야 합니다. • SA 페이로드 • KEi(키-선택 사항): CREATE_CHILD_SA 요청에는 추가 DH 교환에 대한 KE 페이로드가 선택적으로 포함될 수 있어 CHILD_SA에 대한 전달 비밀성을 보다 강력하게 보장할 수 있습니다. SA에 다른 DH 그룹이 포함된 경우 KEi는 초기자가 응답자가 수락할 것으로 예상하는 그룹의 요소여야 합니다. 잘못 추측하면 CREATE_CHILD_SA 교환이 실패하고 다른 KEi로 다시 시도할 수 있습니다 • N(Notify payload-optional). Notify Payload는 오류 조건 및 상태 전환과 같은 정보 데이터를 IKE 피어로 전송하는 데 사용됩니다. Notify Payload는 응답 메시지(일반적으로 요청이 거부된 이유를 지정함), 정보 교환(IKE 요청에 없는 오류를 보고함) 또는 발신자 기능을 나타내거나 요청의 의미를 수정하기 위한 기타 메시지에 나타날 수 있습니다.이 CREATE_CHILD_SA 교환이 IKE_SA 이외의 기존 SA를 재입력하는 경우 REKEY_SA 유형의 선행 N 페이로드는 재입력 중인 SA를 식별해야 합니다. 이 CREATE_CHILD_SA 교환이 기존 SA를 재입력 중이 아니면 N 페이로드를 생략해야 합니다.	ID = 2):요청에 mess_id 3이 있습니다. 3~7이 필요합니다. *11월 11일 19:31:35.873: IKEv2:(SA ID = 2):Next payload: ENCR, version: 2.0 Exchange type: CREATE_CHILD_SA, flags: INITIATOR Message id: 3, length: 396 페이로드 내용: SA 다음 페이로드: N, 예약: 0x0, 길이: 152 마지막 제안: 0x0, 예약됨: 0x0, 길이: 148 제안: 1, 프로토콜 ID: IKE, SPI 크기: 8, #trans: 15 마지막 변환: 0x3, 예약: 0x0: 길이: 12 유형: 1, 예약: 0x0, ID: AES-CBC 마지막 변환: 0x3, 예약됨: 0x0: 길이: 12 유형: 1, 예약: 0x0, ID: AES-CBC 마지막 변환: 0x3, 예약됨: 0x0: 길이: 12 유형: 1, 예약: 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/Group 5 마지막 변환: 0x0, 예약됨: 0x0: 길이: 8 유형: 4, 예약됨: 0x0, id: DH_GROUP_1024_MODP/Group 2 N 다음 페이로드: KE, 예약: 0x0, 길이: 24 KE 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 136 DH 그룹: 2, 예약됨: 0x0 *11월 11일 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Next payload: NONE, reserved: 0x0, length: 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 = 00000003 CurState: READY 이벤트: EV_RECV_CREATE_CHILD *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):작업: Action_Null *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R)	

	MsgID = 00000003 CurState: CHILD_R_INIT 이벤트: EV_RECV_CREATE_CHILD *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):작업: Action_Null *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT 이벤트: EV_VERIFY_MSG *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 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 = 00000003 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 = 00000003 CurState: CHILD_R_IKE 이벤트: EV_GET_IKE_POLICY *11월 11일 19:31:35.874: IKEv2:% 주소 10.0.0.2로 사전 공유 키 가져오기 *11월 11일 19:31:35.874: IKEv2:% 주소 10.0.0.2로 사전 공유 키 가져오기 *11월 11일 19:31:35.874: IKEv2: 툴킷 정책에 제안 PHASE1-prop 추가 *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):IKEv2 프로필 'IKEV2-SETUP' 사용 *11월 11일 19:31:35.874: IKEv2:(SA	

	ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 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 = 00000003 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 = 00000003 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 = 00000003 CurState: CHILD_R_BLD_MSG 이벤트: EV_NO_EVENT *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG 이벤트: EV_OK_RECD_PUBKEY_RESP *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):작업: Action_Null *11월 11일 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 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 = 00000003 CurState: CHILD_R_BLD_MSG 이벤트: EV_NO_EVENT *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG 이벤트: EV_OK_RECD_DH_SECRET_RESP *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):작업: Action_Null *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG 이벤트: EV_BLD_MSG *11월 11일 19:31:35.882: IKEv2:ConstructNotify 페이로드: SET_WINDOW_SIZE 페이로드 내용: SA 다음 페이로드: N, 예약: 0x0, 길이: 56 마지막 제안: 0x0, 예약됨: 0x0, 길이: 52 제안: 1, 프로토콜 ID: IKE, SPI 크기: 8, #trans: 4 마지막 변환: 0x3, 예약: 0x0: 길이: 12 유형: 1, 예약: 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/Group 2	

	N 다음 페이로드: KE, 예약: 0x0, 길이: 24 KE 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 136 DH 그룹: 2, 예약됨: 0x0 알림(SET_WINDOW_SIZE) 다음 페이로드: 없음, 예약됨: 0x0, 길이: 12 보안 프로토콜 ID: IKE, spi 크기: 0, 유형: SET_WINDOW_SIZE	
	*11월 11일 19:31:35.869: IKEv2:(SA ID = 2):Next payload: ENCR, version: 2.0 Exchange type: CREATE_CHILD_SA, flags: INITIATOR Message id: 2, length: 460 페이로드 내용: ENCR 다음 페이로드: SA, 예약됨: 0x0, 길이: 432 *11월 11일 19:31:35.873: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE 페이로드 내용: SA 다음 페이로드: N, 예약: 0x0, 길이: 152 마지막 제안: 0x0, 예약됨: 0x0, 길이: 148 제안: 1, 프로토콜 ID: IKE, SPI 크기: 8, #trans: 15 마지막 변환: 0x3, 예약: 0x0: 길이: 12 유형: 1, 예약: 0x0, ID: AES-CBC 마지막 변환: 0x3, 예약됨: 0x0: 길이: 12 유형: 1, 예약: 0x0, ID: AES-CBC 마지막 변환: 0x3, 예약됨: 0x0: 길이: 12 유형: 1, 예약: 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:	이 패킷은 라우터 2에서 수신됩니다.

	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/Group 5 마지막 변환: 0x0, 예약됨: 0x0: 길이: 8 유형: 4, 예약됨: 0x0, id: DH_GROUP_1024_MODP/Group 2 N 다음 페이로드: KE, 예약: 0x0, 길이: 24 KE 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 136 DH 그룹: 2, 예약됨: 0x0 알림(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):Next payload: ENCR, version: 2.0 Exchange type: CREATE_CHILD_SA, flags:	이제 라우터 2에서 CHILD_SA 교환에 대한 회신을 작성합니다. CREATE_CHILD_SA 응답입니다 CHILD_SA 패킷에는 일반적으로 다음이 포함됩니다.

	RESPONDER MSG-RESPONSE Message id: 3, length: 300 페이로드 내용: SA 다음 페이로드: N, 예약: 0x0, 길이: 56 마지막 제안: 0x0, 예약됨: 0x0, 길이: 52 제안: 1, 프로토콜 ID: IKE, SPI 크기: 8, #trans: 4 마지막 변환: 0x3, 예약: 0x0: 길이: 12 유형: 1, 예약: 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/Group 2 N 다음 페이로드: KE, 예약: 0x0, 길이: 24 KE 다음 페이로드: NOTIFY, 예약됨: 0x0, 길이: 136 DH 그룹: 2, 예약됨: 0x0 *11월 11일 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Next payload: NONE, reserved: 0x0, length: 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 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_WAIT 이벤트: EV_RECV_CREATE_CHILD *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):작업: Action_Null	• SA HDR(version.flags/exchan 유형) • Nonce Ni(선택 사항): CHILD_SA가 초기 교환의 부로 생성되는 경우 두 번째 KE 페이로드와 nonce를 보 내지 않아야 합니다. • SA 페이로드 • KEi(키-선택 사항): CREATE_CHILD_SA 요청 는 추가 DH 교환에 대한 K 페이로드가 선택적으로 포 될 수 있어 CHILD_SA에 대 한 전달 비밀성을 보다 강력 하게 보장할 수 있습니다. SA에 다른 DH 그룹이 포함 된 경우 KEi는 초기자가 응 자가 수락할 것으로 예상하 는 그룹의 요소여야 합니다. 잘못 추측하면 CREATE_CHILD_SA 교환 실패하며 다른 KEi로 다시 도해야 합니다. • N(Notify payload-optional) Notify Payload는 오류 조건 및 상태 전환과 같은 정보 이터를 IKE 피어로 전송하 데 사용됩니다. Notify Payload는 응답 메시지(일 적으로 요청이 거부된 이유 를 지정함), 정보 교환(IKE 청에 없는 오류를 보고하기 위해) 또는 발신자 기능을 타내거나 요청의 의미를 수 정하기 위해 다른 메시지에 나타날 수 있습니다. 이 CREATE_CHILD_SA 교환 IKE_SA가 아닌 기존 SA를 재입력 중인 경우 REKEY_SA 유형의 선행 N 페이로드는 재입력 중인 SA를 식별해야 합니다. 이 CREATE_CHILD_SA 교환 기존 SA를 재입력 중이 아

	*11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 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 = 00000003 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 = 00000003 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 = 00000003 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 = 00000003 CurState: CHILD_I_PROC 이벤트: EV_GEN_DH_SECRET *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC 이벤트: EV_NO_EVENT *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6	면 N 페이로드를 생략해야 합니다. 라우터 2는 응답을 외부로 보내고 새 하위 SA 활성화를 완료합니다

	R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC 이벤트: EV_OK_RECD_DH_SECRET_RESP *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):작업: Action_Null *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 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 = 00000003 CurState: CHILD_I_PROC 이벤트: EV_GEN_SKEYID *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):Generate skeyid *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE 이벤트: EV_ACTIVATE_NEW_SA *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE 이벤트: EV_UPDATE_CAC_STATS *11월 11일 19:31:35.890: IKEv2:New ikev2 sa request activated *11월 11일 19:31:35.890: IKEv2:발 신 협상의 수를 줄이지 못했습니다. *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I)	

	MsgID = 00000003 CurState: CHILD_I_DONE 이벤트: EV_CHECK_DUPE *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE 이벤트: EV_OK *11월 11일 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: EXIT 이벤트: EV_CHK_PENDING *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 = 0000003 CurState: EXIT Event: EV_NO_EVENT	
라우터 1은 라우터 2로부터 응답 패킷을 수신하고 CHILD_SA 활성화를 완료합니다.	*11월 11일 19:31:35.882: IKEv2:(SA ID = 2):Next payload: ENCR, version: 2.0 Exchange type: CREATE_CHILD_SA, flags: RESPONDER MSG-RESPONSE Message id: 3, length: 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 = 00000003 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 = 00000003 CurState: CHILD_R_BLD_MSG 이벤트: EV_GEN_SKEYID *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):Generate skeyid *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE 이벤트 :EV_ACTIVATE_NEW_SA *11월 11일 19:31:35.882: IKEv2:Store mib index ikev2 3, platform 62 *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE 이벤트: EV_UPDATE_CAC_STATS *11월 11일 19:31:35.882: IKEv2:New ikev2 sa request activated *11월 11일 19:31:35.882: IKEv2:수 신 협상에 대한 수를 줄이지 못했습 니다. *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE 이벤트: EV_CHECK_DUPE *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE 이벤트: EV_OK *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6	

	R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE 이벤트: EV_START_DEL_NEG_TMR. *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):작업: Action_Null *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: EXIT 이벤트: EV_CHK_PENDING *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):메시지 ID 3이 포함된 응답 전 송, 4~8 범위에서 요청 수락 가능 *11월 11일 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: EXIT Event: EV_NO_EVENT	

터널 확인

ISAKMP

명령을 사용합니다

<#root>

show crypto ikev2 sa detailed

라우터 1 출력

<#root>

```
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

<#root>

```
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

명령을 사용합니다

<#root>

```
show crypto ipsec sa
```

참고: 이 출력에서는 IKEv1과 달리 첫 번째 터널 협상 중에 PFS DH 그룹 값이 "PFS (Y/N): N, DH group: none"으로 나타나지만, rekey가 발생한 후에는 올바른 값이 나타납니다. 이 동작은 Cisco 버그 ID CSCug67056에 설명되어 있지만 버그는 아닙니다. (등록된 Cisco 사용자만 내부 Cisco 툴 또는 정보에 액세스할 수 있습니다.)
IKEv1과 IKEv2의 차이점은 후자에서 하위 SA는 AUTH 교환 자체의 일부로 생성된다는 점입니다. 암호화 맵 아래에 구성된 DH 그룹은 키 재설정 중에만 사용됩니다. 따라서 첫 번째 키 재설정 전까지는 'PFS (Y/N): N, DH group: none'이 표시됩니다.
IKEv1에서는 하위 SA 생성이 빠른 모드 중에 수행되며 CREATE_CHILD_SA 메시지에는 새 공유 암호를 파생하기 위해 DH 매개변수를 지정하는 Key Exchange 페이로드를 전달하는 프로비전이 있으므로 다른 동작이 표시됩니다.

라우터 1 출력

<#root>

```
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

<#root>

```
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 라우터에서 show crypto session 명령의 출력을 확인할 수도 있습니다. 이 출력은 터널 세션 상태를 UP-ACTIVE로 표시합니다.

<#root>

```
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
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.