ASA IPsec 및 IKE Debugs(IKEv1 Aggressive Mode) 문제 해결 기술 참고

목차

소개

이 문서에서는 적극적인 모드와 PSK(pre-shared key)가 모두 사용되는 경우 Cisco ASA(Adaptive Security Appliance)의 디버그에 대해 설명합니다.특정 디버그 행을 컨피그레이션으로 변환하는 방법도 설명합니다.Cisco에서는 IPsec 및 IKE(Internet Key Exchange)에 대한 기본적인 지식을 보유하고 있는 것이 좋습니다.

이 문서에서는 터널이 설정된 후 트래픽 전달에 대해 설명하지 않습니다.

핵심 문제

IKE 및 IPsec 디버그는 종종 암호이지만 IPsec VPN 터널 설정 문제를 파악하기 위해 사용할 수 있습니다.

시나리오

적극적인 모드는 일반적으로 소프트웨어(Cisco VPN Client) 및 하드웨어 클라이언트(Cisco ASA 5505 Adaptive Security Appliance 또는 Cisco IOS가 있는 Easy VPN(EzVPN)의 경우 사용됩니다 ·소프트웨어 라우터). 그러나 사전 공유 키가 사용되는 경우에만 해당됩니다.주 모드와 달리 적극적인 모드는 세 개의 메시지로 구성됩니다.

디버그는 소프트웨어 버전 8.3.2을 실행하고 EzVPN 서버 역할을 하는 ASA에서 가져온 것입니다 .EzVPN 클라이언트는 소프트웨어 클라이언트입니다.

사용된 디버그 명령

다음은 이 문서에서 사용되는 디버그 명령입니다.

```
debug crypto isakmp 127
debug crypto ipsec 127
```

ASA 컨피그레이션

이 예의 ASA 컨피그레이션은 엄격하게 기본이 되어야 합니다.외부 서버가 사용되지 않습니다.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
lifetime 86400

username cisco password  cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 pre-shared-key *****

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
 default-domain value jyoungta-labdomain.cisco.com
```

디버깅

참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

<table>
<tr><th>서버 메시지 설명</th><th colspan="2">디버깅</th></tr>
<tr><td></td><td colspan="2">49711:28:30.28908/24/12Sev=정보/6IKE/0x6300003B
64.102.156.88과 연결을 설정하려고 합니다.
49811:28:30.29708/24/12Sev=디버그/7IKE/0x63000076
NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000Cu
AM_초기화 이벤트:EV_개시자
49911:28:30.29708/24/12Sev=정보/4IKE/0x63000001
IKE 1단계 협상 시작
50011:28:30.29708/24/12Sev=디버그/7IKE/0x6300076
NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000Cu
AM_SND_MSG1이벤트:EV_GEN_DHKEY
50111:28:30.30408/24/12Sev=디버그/7IKE/0x63000076
NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000Cu
AM_SND_MSG1이벤트:EV_BLD_MSG
50211:28:30.30408/24/12Sev=디버그/7IKE/0x63000076
NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000Cu
AM_SND_MSG1이벤트:EV_START_RETRY_TMR
50311:28:30.30408/24/12Sev=디버그/7IKE/0x63000076
NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000Cu
AM_SND_MSG1이벤트:EV_SND_MSG</td></tr>
<tr><td></td><td colspan="2">50411:28:30.30408/24/12Sev=정보/4IKE/0x63000013
SENDING >>> ISAKMP OAK AG(SA, KE, NON, ID, VID(Xauth), VID(dpd), VID
VID(Unity)를 64.102.156.88으로</td></tr>
<tr><td></td><td colspan="2"><========== 적극적인 메시지 1(AM1) =======</td></tr>
<tr><td>클라이언트에서 AM1을 받습니다.</td><td>8월 24일 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message(msgid=0) with payloads:HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) 총 길이:849</td><td>50611:28:30.33308/24/12Sev=디버그/7IKE/0x6300076
NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=000000000000000CurState: AM_WAIT_MSG2이벤트:EV_NO_이벤트</td></tr>
<tr><td>프로세스 AM1. 수신된 제안 및 변형을 이미 구성된 제안과 비교합니다.
관련 구성:
ISAKMP는 인터페이스에서 활성화되며 클라이언트가 전송한 것과 일치하는 정책이 하나 이상 정의됩니다.</td><td colspan="2">8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, SA 페이로드 처리
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, 처리 키 페이로드
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, 처리 ISA_KE 페이로드
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, 처리 nonce 페이로드
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, 처리 ID 페이로드
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID 페이로드 처리
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received xauth V6 VID
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID 페이로드 처리
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received DPD VID
8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID 페이로드 처리</td></tr>
</table>

crypto isakmp enable outside crypto isakmp policy 10 authentication pre-share encryption aes hash sha group 2 lifetime 86400 ID 이름과 일치하는 터널 그룹: tunnel-group EZ type remote-access tunnel-group EZ general-attributes default-group-policy EZ tunnel-group EZ ipsec-attributes pre-shared-key cisco	8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received Fragmentatio 8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, IKE Peer에 포함된 IKE 모드:TrueAggressive 모드:False 8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID 페이로드 처리 8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received NAT-Traversa 8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID 페이로드 처리 8월 24일 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received Cisco Unity c 8월 24일 11:31:03 [IKEv1]IP = 64.102.156.87, 연결이 tunnel_group ipsec에 연 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, IKE SA 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1]1단계 실패:클래스 그룹 설명:Rcv'd의 특성 유형이 일 룹 5 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, IKE SA acceptableMatches global IKE entry # 1과 일치
AM2를 구성합니다. 이 프로세스에는 다음이 포함됩니다. - 선택한 정책 - DH(Diffie-Hellman) - 응답자 ID - 인증 - NAT(Network Address Translation) 탐지 페이로드	8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, ISAKMF 8월 24일 11:31:03 [IKEv1 DEBUG]그룹 = ipsec, IP = 64.102.156.87, 키 페이로 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, nonce 페 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Respon 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, ID 페이 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, 해시 페 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, ISAKMF 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Cisco U 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, xauth V 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, dpd VID

	8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, NAT-Tra 성 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, NAT-Dis 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, computi 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, NAT-Dis 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, computi 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, fragmen 드 구성 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, VID 페이 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Send AI ASA GW VID
AM2를 보냅니다.	8월 24일 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Messa payloads:HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDO VENDOR (13) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13)
	========== 적극적인 메시지 2(AM2) ========
	50711:28:30.40208/24/12Sev=정보/5IKE/0x6300002F 수신된 ISAKMP 패킷:피어 = 64.102.156.8 50811:28:30.40308/24/12Sev=정보/4IKE/0x63000014 64.102.156.88에서 <<< ISAKMP OAK AG(SA, KE, NON, ID, HASH, VID(Unity) VID(Nat-T), NAT-D, VID(Frag), VID(?) 수신 51011:28:30.41208/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710E AM_WAIT_MSG2이벤트:EV_RCVD_MSG
	51111:28:30.41208/24/12Sev=정보/5IKE/0x63000001 피어는 Cisco-Unity 호환 피어입니다. 51211:28:30.41208/24/12Sev=정보/5IKE/0x63000001 피어가 XAUTH를 지원합니다. 51311:28:30.41208/24/12Sev=정보/5IKE/0x63000001 피어가 DPD 지원 51411:28:30.41208/24/12Sev=정보/5IKE/0x63000001 피어가 NAT-T 지원 51511:28:30.41208/24/12Sev=정보/5IKE/0x63000001 피어가 IKE 조각화 페이로드를 지원합니다. 51611:28:30.41208/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710E AM_WAIT_MSG2이벤트:EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710E AM_WAIT_MSG2이벤트:EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710E AM_WAIT_MSG2이벤트:EV_ADJUST_PORT 51911:28:30.42208/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710E AM_WAIT_MSG2이벤트:EV_CRYPTO_ACTIVE
	52011:28:30.42208/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710E AM_SND_MSG3이벤트:EV_BLD_MSG] 52111:28:30.42208/24/12Sev=디버그/8IKE/0x63000001 IOS 공급업체 ID 구성이 시작되었습니다. 52211:28:30.42208/24/12Sev=정보/6IKE/0x63000001 IOS 공급업체 ID 구성 성공

	52311:28:30.42308/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710ED AM_SND_MSG3이벤트:EV_SND_MSG 52411:28:30.42308/24/12Sev=정보/4IKE/0x63000013 SENDING >> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTAC VID(Unity) to 64.102.156.88
	<========== 적극적인 메시지 3(AM3) ========
클라이언트에서 AM3을 받습니다.	8월 24일 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Mess payloads:HDR + HASH (8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + VE NONE (0) 총 길이:168
AM 3 처리. NAT-T(NAT traversal) 사용 확인이제 양쪽은 트래픽 암호화를 시작할 준비가 되었습니다.	8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, 처리 해 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, ISAKMP 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, 처리 중 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, 처리 NA 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, computi 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, 처리 NA 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, computi 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, 처리 VID 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Process payload(버전:1.0.0, 기능:00000408) 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, 처리 VID 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Receive 8월 24일 11:31:03 [IKEv1]그룹 = ipsec, IP = 64.102.156.87, 자동 NAT 탐지 상태: 원격 endISNAT 장치 뒤에 있음NAT 장치 뒤에 없음
1.5단계(XAUTH)를 시작하고 사용자 자격 증명을 요청합니다.	8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, 빈 해시 8월 24일 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, qm 해시 8월 24일 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Messa payloads:HDR + HASH (8) + ATTR (14) + NONE (0) 총 길이:72
	========== XAuth - 자격 증명 요청 ==========>
	53511:28:30.43008/24/12Sev=정보/4IKE/0x63000014 64.102.156.88에서 <<< ISAKMP OAK TRANS *(HASH, ATTR) 수신 53611:28:30.43108/24/12Sev=디코드/11IKE/0x63000001 ISAKMP 헤더 개시자 쿠키:D56197780D7BE3E5 응답자 쿠키:1B301D2DE710EDA0 다음 페이로드:해시 버전(16진수):10 Exchange 유형:트랜잭션 플래그:(암호화) MessageID(16진수):FB709D4D 길이:76 페이로드 해시 다음 페이로드:속성 예약됨:00 페이로드 길이:24 데이터(16진수):C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 페이로드 특성 다음 페이로드:없음 예약됨:00 페이로드 길이:20 유형:ISAKMP_CFG_REQUEST 예약됨:00

	식별자:0000 XAUTH 유형:일반 XAUTH 사용자 이름:(비어 있음) XAUTH 사용자 암호:(비어 있음) 53711:28:30.43108/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_초기화 이벤트:EV_RCVD_M
	53811:28:30.43108/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_PCS_XAUTH_REQEvent:EV 53911:28:30.43108/24/12 Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_PCS_XAUTH_REQEvent:EV 54011:28:30.43208/24/12Sev=디버그/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_WAIT_4USEREvent:EV_NO 541 11:28:36.41508/24/12Sev=디버그/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_WAIT_4USEREvent:EV_RC
	54211:28:36.41508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_WAIT_4USEREvent:EV_SN 54311:28:36.41508/24/12Sev=정보/4IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR)를 64.102.156.88으로 54411:28:36.41508/24/12Sev=디코드/11IKE/0x63000001 ISAKMP 헤더 개시자 쿠키:D56197780D7BE3E5 응답자 쿠키:1B301D2DE710EDA0 다음 페이로드:해시 버전(16진수):10 Exchange 유형:트랜잭션 플래그:(암호화) MessageID(16진수):FB709D4D 길이:85 페이로드 해시 다음 페이로드:속성 예약됨:00 페이로드 길이:24 데이터(16진수):1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 페이로드 특성 다음 페이로드:없음 예약됨:00 페이로드 길이:33 유형:ISAKMP_CFG_REPLY 예약됨:00 식별자:0000 XAUTH 유형:일반 XAUTH 사용자 이름:(데이터가 표시되지 않음) XAUTH 사용자 암호:(데이터가 표시되지 않음)
	<========== Xauth - 사용자 자격 증명 ======
사용자 자격 증명을 받습니다.	8월 24일 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Mess payloads:HDR + 해시(8) + 속성(14) + 없음(0) 총 길이:85 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, process
사용자 자격 증명을 처리합니다.자격 증명을 확인하고 모드 구성 페이로드	8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Process 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64. IKEGetUserAttributes:기본 DNS = 192.168.1.99

를 생성합니다. 관련 구성: username cisco password cisco	8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:보조 DNS = 지워짐 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:기본 WINS = 지워짐 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:보조 WINS = 지워짐 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:스플릿 터널링 목록 = 분할 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:기본 도메인 = jyota-labdomain.cisco.com 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:IP 압축 = 비활성화됨 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:스플릿 터널링 정책 = 사용 안 함 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:브라우저 프록시 설정 = 수정 안 함 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 IKEGetUserAttributes:브라우저 프록시 Bypass Local = disable 8월 24일 11:31:09 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.8
결과를 보냅니다.	8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 생성 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 구성 8월 24일 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Messa payloads:HDR + HASH (8) + ATTR (14) + NONE (0) 총 길이:64
	========== XAuth - 권한 부여 결과 =======
	54511:28:36.41608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_XAUTHREQ_DUSUMvent:E 54611:28:36.41608/24/12Sev=디버그/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_XAUTHREQ_DUSUMvent:E 54711:28:36.42408/24/12Sev=정보/5IKE/0x6300002F 수신된 ISAKMP 패킷:피어 = 64.102.156.88 54811:28:36.42408/24/12Sev=정보/4IKE/0x63000014 64.102.156.88에서 <<< ISAKMP OAK TRANS *(HASH, ATTR) 수신 54911:28:36.42508/24/12Sev=디코드/11IKE/0x63000001 ISAKMP 헤더 개시자 쿠키:D56197780D7BE3E5 응답자 쿠키:1B301D2DE710EDA0 다음 페이로드:해시 버전(16진수):10 Exchange 유형:트랜잭션 플래그:(암호화) MessageID(16진수):5B6910FF 길이:76 페이로드 해시 다음 페이로드:속성 예약됨:00 페이로드 길이:24 데이터(16진수):7DCF47827164198731639BFB7595F694C9DFE85 페이로드 특성 다음 페이로드:없음 예약됨:00 페이로드 길이:12

	유형:ISAKMP_CFG_SET 예약됨:00 식별자:0000 XAUTH 상태:통과 55011:28:36.42508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState:TM_초기화 이벤트:EV_RCVD_MS 55111:28:36.42508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState:TM_PCS_XAUTH_SETEvent:EV_ 55211:28:36.42508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState:TM_PCS_XAUTH_SETEvent:EV_
	55311:28:36.42508/24/12Sev=정보/4IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR)를 64.102.156.88으로
	<========== Xauth - 승인 ==========
ACK 수신 및 처리서버에서 응답이 없습니다.	8월 24일 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED 메시 :HDR + HASH (8) + ATTR (14) + NONE (0) 총 길이:60 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 하라! 8월 24일 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 ACK 특성
	55511:28:36.42608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState:TM_XAUTH_DUSUMvent: EV_XAUTH_DONE_SUC 55611:28:36.42608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState:TM_XAUTH_DUSUMvent:EV_NO 55711:28:36.42608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_XAUTHREQ_DUSUMvent:E 55811:28:36.42608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_FREEEvent:제거(_R) 55911:28:36.42608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:TM_FREEEvent:EV_NO_이벤트 56011:28:36.42608/24/12Sev=디버그/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710ED CMN_XAUTH_PROGEvent:EV_XAUTH_DONE_SUC 56111:28:38.40608/24/12Sev=디버그/8IKE/0x6300004C IKE SA용 DPD 타이머 시작(I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0) sa->state = 1, sa->dpd.worry_freq(mSec) = 56211:28:38.40608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710ED CMN_MODECFG_PROGEvent:EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710ED CMN_MODECFG_PROGEvent:EV_NO_이벤트 56411:28:38.40608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState:TM_초기화 이벤트:EV_INIT_MOD 56511:28:38.40808/24/12Sev=정보/5IKE/0x6300005E Concentrator에 방화벽 요청을 보내는 클라이언트 56611:28:38.40908/24/12Sev=디버그/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState:TM_SND_MODEFGREQEvent: EV_START_RETRY_TMR
	56711:28:38.40908/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState:TM_SND_MODEFGREQEvent:EV 56811:28:38.40908/24/12Sev=정보/4IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR)를 64.102.156.88으로

	56911:28:38.62708/24/12Sev=디코드/11IKE/0x63000001 ISAKMP 헤더 개시자 쿠키:D56197780D7BE3E5 응답자 쿠키:1B301D2DE710EDA0 다음 페이로드:해시 버전(16진수):10 Exchange 유형:트랜잭션 플래그:(암호화) MessageID(16진수):84B4B653 길이:183 페이로드 해시 다음 페이로드:속성 예약됨:00 페이로드 길이:24 데이터(16진수):81BFBF6721A744A815D69A315EF4AAA571D6B687 페이로드 특성 다음 페이로드:없음 예약됨:00 페이로드 길이:131 유형:ISAKMP_CFG_REQUEST 예약됨:00 식별자:0000 IPv4 주소:(비어 있음) IPv4 넷마스크:(비어 있음) IPv4 DNS:(비어 있음) IPv4 NBNS(WINS):(비어 있음) 주소 만료:(비어 있음) Cisco 확장:배너:(비어 있음) Cisco 확장:PWD 저장:(비어 있음) Cisco 확장:기본 도메인 이름:(비어 있음) Cisco 확장:분할 포함:(비어 있음) Cisco 확장:스플릿 DNS 이름:(비어 있음) Cisco 확장:PFS 수행:(비어 있음) 알 수 없음:(비어 있음) Cisco 확장:백업 서버:(비어 있음) Cisco 확장:스마트 카드 분리 연결 해제:(비어 있음) 응용 프로그램 버전:Cisco Systems VPN Client 5.0.07.0290:WinNT Cisco 확장:방화벽 유형:(비어 있음) Cisco 확장:동적 DNS 호스트 이름:ATBASU-LABBOX	
	<========== Mode-config 요청 ==========	
수신 모드-구성 요청.	8월 24일 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED 메시지 (msgid=84b4b653) (페이로드 포함):HDR + HASH (8) + ATTR (14) + NONE (0) 총 길이 :183	57011:28:38.62808/24/12Sev= 디버그/7IKE/0x6300076 NAV Trace- >TM:MsgID=84B4B653CurState:TM_WAIT_MODEFGREF

	8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr():진입하라!	
Process mode-config 요청. 이러한 값 중 다수는 일반적으로 그룹 정책에서 구성됩니다.그러나 이 예제의 서버는 매우 기본적인 컨피그레이션을 가지므로 여기에 표시되지 않습니다.	8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 Request attributes 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 주소에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 넷마스크에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 서버 주소에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 서버 주소에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.8 transaction mode attribute:5 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 저장 설정에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 도메인 이름에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 릿 터널 목록에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 릿 DNS에 대한 요청을 받았습니다. 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 설정에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 이언트 브라우저 프록시 설정에 대한 요청을 받았습니다! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 ip-sec 피어 목록에 대한 요청을 받았습니다. 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 이언트 스마트 카드 제거 연결 끊기 설정에 대한 요청을 받았습니다. 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 프로그램 버전에 대한 요청을 받았습니다. 8월 24일 11:31:11 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.8 :WinNTClient 응용 프로그램 버전:5.0.07.0290 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 MODE_CFG:FWTYPE에 대한 요청을 받았습니다. 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 MODE_CFG:DDNS에 대한 DHCP 호스트 이름 요청 수신:ATBASU-랩박스!
구성된 모든 값으로 mode-config 응답을 구성합니다. 관련 구성: 이 경우 사용자에게 항상 동일한 IP가 할당됩니다.	8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 (192.168.1.100) before initiating Mode Cfg (XAuth enabled) 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 mask (255.255.255.0) to remote client 8월 24일 11:31:11 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.8 설 IP 주소 192.168.1.100 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1

username cisco attributes **vpn-framed-ip-address 192.168.1.100 255.255.255.0** group-policy EZ internal group-policy EZ attributes password-storage enabledns-server value 192.168.1.129 vpn-tunnel-protocol ikev1 split-tunnel-policy tunnelall split-tunnel-network-list value split default-domain value jyoungta-labdomain.cisco.com	생성 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 construct_cfg_set:기본 도메인 = jyota-labdomain.cisco.com 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 Browser Proxy Attributes! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 to No-Modify.브라우저 프록시 데이터는 mode-cfg 응답에 포함되지 않습니다. 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 Smartcard Removal Disconnect enable! 8월 24일 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 구성
Send mode-config response(보내기 모드-컨피그레이션 응답).	8월 24일 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Messa payloads:HDR + HASH (8) + ATTR (14) + NONE (0) 총 길이:215
	========== Mode-config 응답 ==========
	57111:28:38.63808/24/12Sev=정보/5IKE/0x6300002F 수신된 ISAKMP 패킷:피어 = 64.102.156.88 57211:28:38.63808/24/12Sev=정보/4IKE/0x63000014 64.102.156.88에서 <<< ISAKMP OAK TRANS *(HASH, ATTR) 수신 57311:28:38.63908/24/12Sev=디코드/11IKE/0x63000001 ISAKMP 헤더 개시자 쿠키:D56197780D7BE3E5 응답자 쿠키:1B301D2DE710EDA0 다음 페이로드:해시 버전(16진수):10 Exchange 유형:트랜잭션 플래그:(암호화) MessageID(16진수):84B4B653 길이:220 페이로드 해시 다음 페이로드:속성 예약됨:00 페이로드 길이:24 데이터(16진수):6DE2E70ACF6B1858846BC62E590C00A66745D14D 페이로드 특성 다음 페이로드:없음 예약됨:00 페이로드 길이:163 유형:ISAKMP_CFG_REPLY 예약됨:00 식별자:0000 IPv4 주소:192.168.1.100 IPv4 넷마스크:255.255.255.0 IPv4 DNS:192.168.1.99 Cisco 확장:PWD 저장:아니요 Cisco 확장:기본 도메인 이름:

<table>
<tr><td></td><td colspan="2">jyoungta-labdomain.cisco.com
Cisco 확장:PFS 수행:아니요
응용 프로그램 버전:Cisco Systems, Inc ASA5505 버전 8.4(4)1, 6월 14일~12일
Cisco 확장:스마트 카드 분리 연결 해제:예</td></tr>
<tr><td>서버에서 1단계가 완료되었습니다.QM(빠른 모드) 프로세스를 시작합니다.</td><td>8월 24일 11:31:13 [IKEv1 DECODE]IP = 64.102.156.87, IKE Responder starting QM:msg id = 0e83792e
8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Delay Quick Mode processing, Cert/Trans Exch/RM DSID 진행 중
8월 24일 11:31:13 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.87, 무상 ARP가 192.168.1.100에 전송됨
8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Resume Quick Mode processing, Cert/Trans Exch/RM DSID가 완료되었습니다.
8월 24일 11:31:13 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.87, 단계 1 완료</td><td>57411:28:38.63908/24/12Sev= 디버그/7IKE/0x6300076
NAV Trace->TM:MsgID=84B4B653CurState:
TM_WAIT_MODEFGREPLYEvent:EV_RCVD_MSG
57511:28:38.63908/24/12Sev= 정보/5IKE/0x63000010
MODE_CFG_REPLY:특성 = INTERNAL_IPV4_ADDRESS
값 = 192.168.1.100
57611:28:38.63908/24/12Sev=정보/5IKE/0x63000010
MODE_CFG_REPLY:특성 = INTERNAL_IPV4_NETMASK
값 = 255.255.255.0
57711:28:38.63908/24/12Sev= 정보/5IKE/0x63000010
MODE_CFG_REPLY:특성 = INTERNAL_IPV4_DNS(1):,
값 = 192.168.1.99
57811:28:38.63908/24/12Sev=정보/5IKE/0x630000D
MODE_CFG_REPLY:특성 =
MODEFG_UNITY_SAVEPWD:, 값 = 0x00000000
57911:28:38.63908/24/12Sev=정보/5IKE/0x630000E
MODE_CFG_REPLY:특성 =
MODEFG_UNITY_DEFDOMAIN:, 값 = jyounta-labdomain.cisco.com
58011:28:38.63908/24/12Sev= 정보/5IKE/0x630000D
MODE_CFG_REPLY:속성 = MODEFG_UNITY_PFS:, 값 =
58111:28:38.63908/24/12Sev=정보/5IKE/0x630000E
MODE_CFG_REPLY:속성 = APPLICATION_VERSION,
value = Cisco Systems, Inc ASA5505 버전 8.4(4)1
건설사 목 14-6월 12일 11:20
58211:28:38.63908/24/12Sev= 정보/5IKE/0x630000D
MODE_CFG_REPLY:특성 =
MODEFG_UNITY_SMARTCARD_REMOVAL_DISCONNE
58311:28:38.63908/24/12Sev= 정보/5IKE/0x630000D
MODE_CFG_REPLY:특성 = 수신 및 NAT-T 사용
포트 번호, 값 = 0x0001194
58411:28:39.36708/24/12Sev= 디버그/9IKE/0x6300093
ini 매개 변수 EnableDNSRedirection의 값은 1입니다.
58511:28:39.36708/24/12Sev= 디버그/7IKE/0x6300076
NAV Trace->TM:MsgID=84B4B653CurState:
TM_MODEFG_FUSUMvent:EV_MODEFG_DONE_SUC</td></tr>
<tr><td>클라이언트용 DPD를 구성하고 보냅니다.</td><td colspan="2">8월 24일 11:31:13 [IKEv1]IP = 64.102.156.87, 이 연결의 Keep-alive 유형:DPD
8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1
머 시작:82080초
8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1
8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1
생성</td></tr>
</table>

	8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 구성 8월 24일 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Messa payloads:HDR + 해시(8) + 알림(11) + 없음(0) 총 길이:92
	================ DPD(Dead Peer Detection) ======
	58811:28:39.79508/24/12Sev=디버그/7IKE/0x63000015 intf_data:lcl=0x0501A8C0, 마스크=0x00FFFFFF, bcast=0xFF01A8C0, b 58911:28:39.79508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710ED CMN_MODECFG_PROGEvent:EV_INIT_P2 59011:28:39.79508/24/12Sev=정보/4IKE/0x6300056 드라이버로부터 키 요청을 받았습니다.로컬 IP = 192.168.1.100, GW IP = 64.10 59111:28:39.79508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710ED CMN_ACTIVEvent:EV_NO_이벤트 59211:28:39.79508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState:QM_초기화 이벤트:EV_개시자 59311:28:39.79508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState:QM_BLD_MSG1이벤트:EV_CHK_ 59411:28:39.79608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState:QM_BLD_MSG1이벤트:EV_BLD_ 59511:28:39.79608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState:QM_SND_MSG1이벤트:EV_STA
	59611:28:39.79608/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState:QM_SND_MSG1이벤트:EV_SND 59711:28:39.79608/24/12Sev=정보/4IKE/0x63000013 >>>ISAKMP OAK QM *(HASH, SA, NON, ID, ID)를 64.102.156.88으로 전송
	<================ 빠른 모드 메시지 1(QM1) ======
QM1을 받습니다.	8월 24일 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Mess payloads:HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0
QM1을 처리합니다. 관련 구성: `crypto dynamic-map DYN 10 set transform-set TRA`	8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 드 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 8월 24일 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64 ID 수신 192.168.1.100 8월 24일 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.8 격 프록시 호스트 데이터(주소 192.168.1.100, 프로토콜 0, 포트 0) 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 8월 24일 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64 ID_IPV4_ADDR_SUBNET ID received—0.0.0.0—0.0.0.0 8월 24일 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.8 IP 프록시 서브넷 데이터:주소 0.0.0.0, 마스크 0.0.0.0, 프로토콜 0, 포트 0 8월 24일 11:31:13 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.8 found by addr 8월 24일 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.8 checking map = out-map, seq = 10... 8월 24일 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.8 by-passed:암호화 맵 항목이 완전하지 않습니다. 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1

	의해 정의된 UDP-Encapsulated-Tunnel 및 UDP-Encapsulated-Transport 모드 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 의해 정의된 UDP-Encapsulated-Tunnel 및 UDP-Encapsulated-Transport 모드 8월 24일 11:31:13 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.8 IKE 원격 피어:out-dyn-map 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 처리
QM2를 구성합니다. 관련 구성: tunnel-group EZ type **remote-access** *!* *(tunnel type ra = tunnel type remote-access)* crypto ipsec transform-set TRA **esp-aes esp-sha-hmac** crypto ipsec security-association **lifetime seconds 28800** crypto ipsec security-association lifetime kilobytes 4608000 **crypto dynamic-map DYN 10 set transform-set TRA** crypto map MAP 65000 ipsec-isakmp dynamic DYN crypto map MAP interface outside	8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 # 12, Transform # 1 acceptableMatches global IPSec SA entry # 10 8월 24일 11:31:13 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.8 IPSEC:0xcfdffc90에서 생성된 새로운 원시 SA, SCB:0xCFDFFB58, 방향:인바운드 SPI:0x9E18ACB2 세션 ID:0x00138000 VPIF 번호:0x00000004 터널 유형:라 프로토콜:esp 수명:240초 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 SPI를 받았습니다.SPI = 0x9e18acb2 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 드 구축 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 생성 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 구성 8월 24일 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.8 재지정 기간(2147483초 ~ 86400초) 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 로드 구성 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 8월 24일 11:31:13 [IKEv1 DEBUG]그룹 = ipsec, 사용자 이름 = user1, IP = 64.1 원격 호스트:192.168.1.100프로토콜 0포트 0 로컬 서브넷:0.0.0.0mask 0.0.0.0 프로토콜 0포트 0 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 RESPONDER LIFETIME notification to Initiator 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 구성
QM2를 보냅니다.	8월 24일 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64 보내는 IKE Responder:msg id = 0e83792e 8월 24일 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Messa payloads:HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY
	========== 빠른 모드 메시지 2(QM2) =======
	60811:28:39.96208/24/12Sev=정보/4IKE/0x63000014 수신 <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, ID, NOTIFY:STATUS_RESP_LIFETIME)의 64.102.156.88
	60911:28:39.96408/24/12Sev=디코드/11IKE/0x63000001 ISAKMP 헤더 개시자 쿠키:D56197780D7BE3E5 응답자 쿠키:1B301D2DE710EDA0 다음 페이로드:해시 버전(16진수):10 Exchange 유형:빠른 모드

	플래그:(암호화) MessageID(16진수):E83792E 길이:188 페이로드 해시 다음 페이로드:보안 연계 예약됨:00 페이로드 길이:24 데이터(16진수):CABF38A62C9B88D1691E81F3857D6189534B2EC0 페이로드 보안 연결 다음 페이로드:노네 예약됨:00 페이로드 길이:52 도이:IPsec 상황:(SIT_IDENTITY_ONLY) 페이로드 제안 다음 페이로드:없음 예약됨:00 페이로드 길이:40 제안 #:1 프로토콜 ID:PROTO_IPSEC_ESP SPI 크기:4 변환 수:1 SPI:9E18ACB2 페이로드 변환 다음 페이로드:없음 예약됨:00 페이로드 길이:28 변환 번호:1 변환 ID:ESP_3DES 예약2:0000 수명 유형:초 수명 기간(16진수):0020C49B 캡슐화 모드:UDP 터널 인증 알고리즘:SHA1 페이로드 Nonce 다음 페이로드:식별 예약됨:00 페이로드 길이:24 데이터(16진수):3A079B75DA512473706F235EA3FCA61F1D15D4CD 페이로드 식별 다음 페이로드:식별 예약됨:00 페이로드 길이:12 ID 유형:IPv4 주소 프로토콜 ID(UDP/TCP 등):0 포트:0 ID 데이터(&F);192.168.1.100 페이로드 식별 다음 페이로드:알림 예약됨:00 페이로드 길이:16

	ID 유형:IPv4 서브넷 프로토콜 ID(UDP/TCP 등):0 포트:0 ID 데이터(&F);0.0.0.0/0.0.0.0 페이로드 알림 다음 페이로드:없음 예약됨:00 페이로드 길이:28 도이:IPsec 프로토콜 ID:PROTO_IPSEC_ESP SPI 크기:4 알림 유형:STATUS_RESP_LIFETIME SPI:9E18ACB2 데이터 콜론(&F); 수명 유형:초 수명 기간(16진수):00015180
	61011:28:39.96508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState:QM_WAIT_MSG2이벤트:EV_RCV 61111:28:39.96508/24/12Sev=정보/5IKE/0x63000045 RESPONDER-LIFETIME 알림의 값은 86400초입니다. 61211:28:39.96508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState:QM_WAIT_MSG2이벤트:EV_CHK 61311:28:39.96508/24/12Sev=디버그/7IKE/0x63000076
	NAV Trace->QM:MsgID=0E83792ECurState:QM_BLD_MSG3이벤트:EV_BLD_ 61411:28:39.96508/24/12Sev=디버그/7IKE/0x63000076 ISAKMP 헤더 개시자 쿠키:D56197780D7BE3E5 응답자 쿠키:1B301D2DE710EDA0 다음 페이로드:해시 버전(16진수):10 Exchange 유형:빠른 모드 플래그:(암호화) MessageID(16진수):E83792E 길이:52 페이로드 해시 다음 페이로드:없음 예약됨:00 페이로드 길이:24 데이터(16진수):CDDC20D91EB4B568C826D6A5770A5CF020141236
	61511:28:39.96508/24/12Sev=디버그/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState:QM_SND_MSG3이벤트:EV_SND 61611:28:39.96508/24/12Sev=정보/4IKE/0x63000013 >>>ISAKMP OAK QM *(HASH)를 64.102.156.88으로 전송
	<========== 빠른 모드 메시지 3(QM3) ======
QM3를 받습니다.	8월 24일 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Mess payloads:HDR + HASH (8) + NONE (0) 총 길이:52
QM3 처리. 인바운드 및 아웃바운드 SPI(보안 매개 변수 인덱스)를 만듭니다. 호스트에 대한 고정	8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 드 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1

경로를 추가합니다. 관련 구성: crypto ipsec transform-set TRA esp-aes esp-sha-hmac crypto ipsec security-association lifetime seconds 28800 crypto ipsec security-association lifetime kilobytes 4608000 crypto dynamic-map DYN 10 set transform-set TRA crypto dynamic-map DYN 10 **set reverse-route**	Mode Key! 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 회에서 암호화 맵 out-dyn-map 10 일치하는 ACL을 찾습니다. 알 수 없음:반환됨 cs_id=cc107410;규칙=00000000 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 Mode Key! IPSEC:0xccc9ed60에서 생성된 새 원시 SA, SCB:0xCF7F59E0, 방향:아웃바운드 SPI:0xC055290A 세션 ID:0x00138000 VPIF 번호:0x00000004 터널 유형:라 프로토콜:esp 수명:240초 IPSEC:완료된 호스트 OBSA 업데이트, SPI 0xC055290A IPSEC:아웃바운드 VPN 컨텍스트 생성, SPI 0xC055290A 플래그:0x00000025 SA:0xccc9ed60 SPI:0xC055290A MTU:1500바이트 VCID:0x00000000 피어:0x00000000 SCB:0xA5922B6B 채널:0xc82afb60 IPSEC:완료된 아웃바운드 VPN 컨텍스트, SPI 0xC055290A VPN 핸들:0x0015909c IPSEC:새 아웃바운드 암호화 규칙, SPI 0xC055290A 소스 주소:0.0.0.0 소스 마스크:0.0.0.0 dst 주소:192.168.1.100 Dst 마스크:255.255.255.255 소스 포트 상한:0 낮음:0 운영:무시 Dst 포트 상한:0 낮음:0 운영:무시 프로토콜:0 프로토콜 사용:거짓 SPI:0x00000000 SPI 사용:거짓 IPSEC:완료된 아웃바운드 암호화 규칙, SPI 0xC055290A 규칙 ID:0xcb47a710 IPSEC:새 아웃바운드 허용 규칙, SPI 0xC055290A 소스 주소:64.102.156.88 소스 마스크:255.255.255.255 dst 주소:64.102.156.87 Dst 마스크:255.255.255.255 소스 포트 상한:4500

	낮음:4500 운영:같음 Dst 포트 상한:58506 낮음:58506 운영:같음 프로토콜:17 프로토콜 사용:참 SPI:0x00000000 SPI 사용:거짓 IPSEC:아웃바운드 허용 규칙, SPI 0xC055290A 완료 규칙 ID:0xcdf3cfa0 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 회에서 암호화 맵 out-dyn-map 10 일치하는 ACL을 찾습니다. 알 수 없음:반환됨 cs_id=cc107410;규칙=00000000 8월 24일 11:31:13 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.8 운드 SPI = 0x9e18acb2, 아웃바운드 보안 협상 완료 SPI = 0xc055290a 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 SA에 대한 KEY_ADD 메시지가 있습니다.SPI = 0xc055290a IPSEC:완료된 호스트 IBSA 업데이트, SPI 0x9E18ACB2 IPSEC:인바운드 VPN 컨텍스트 생성, SPI 0x9E18ACB2 플래그:0x00000026 SA:0xcfdffc90 SPI:0x9E18ACB2 MTU:0바이트 VCID:0x00000000 피어:0x0015909C SCB:0xA5672481 채널:0xc82afb60 IPSEC:완료된 인바운드 VPN 컨텍스트, SPI 0x9E18ACB2 VPN 핸들:0x0016219c IPSEC:아웃바운드 VPN 컨텍스트 0x0015909C, SPI 0xC055290A 업데이트 플래그:0x00000025 SA:0xccc9ed60 SPI:0xC055290A MTU:1500바이트 VCID:0x00000000 피어:0x0016219C SCB:0xA5922B6B 채널:0xc82afb60 IPSEC:완료된 아웃바운드 VPN 컨텍스트, SPI 0xC055290A VPN 핸들:0x0015909c IPSEC:완료된 아웃바운드 내부 규칙, SPI 0xC055290A 규칙 ID:0xcb47a710 IPSEC:완료된 아웃바운드 외부 SPD 규칙, SPI 0xC055290A 규칙 ID:0xcdf3cfa0 IPSEC:새 인바운드 터널 흐름 규칙, SPI 0x9E18ACB2 소스 주소:192.168.1.100 소스 마스크:255.255.255.255 dst 주소:0.0.0.0 Dst 마스크:0.0.0.0 소스 포트

	상한:0 낮음:0 운영:무시 Dst 포트 상한:0 낮음:0 운영:무시 프로토콜:0 프로토콜 사용:거짓 SPI:0x00000000 SPI 사용:거짓 IPSEC:완료된 인바운드 터널 흐름 규칙, SPI 0x9E18ACB2 규칙 ID:0xcdf15270 IPSEC:새 인바운드 암호 해독 규칙, SPI 0x9E18ACB2 소스 주소:64.102.156.87 소스 마스크:255.255.255.255 dst 주소:64.102.156.88 Dst 마스크:255.255.255.255 소스 포트 상한:58506 낮음:58506 운영:같음 Dst 포트 상한:4500 낮음:4500 운영:같음 프로토콜:17 프로토콜 사용:참 SPI:0x00000000 SPI 사용:거짓 IPSEC:인바운드 암호 해독 규칙, SPI 0x9E18ACB2 완료 규칙 ID:0xce03c2f8 IPSEC:새 인바운드 허용 규칙, SPI 0x9E18ACB2 소스 주소:64.102.156.87 소스 마스크:255.255.255.255 dst 주소:64.102.156.88 Dst 마스크:255.255.255.255 소스 포트 상한:58506 낮음:58506 운영:같음 Dst 포트 상한:4500 낮음:4500 운영:같음 프로토콜:17 프로토콜 사용:참 SPI:0x00000000 SPI 사용:거짓 IPSEC:완료된 인바운드 허용 규칙, SPI 0x9E18ACB2 규칙 ID:0xcf6f58c0 8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 KEY_UPDATE, spi 0x9e18acb2

	8월 24일 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.1 머 시작:82080초 8월 24일 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.8 정 경로 추가:192.168.1.100
2단계가 완료되었습니다.양쪽 모두 지금 암호화하고 해독하고 있습니다.	8월 24일 11:31:13 [IKEv1]그룹 = ipsec, 사용자 이름 = user1, IP = 64.102.156.8 (msgid=0e83792e)
하드웨어 클라이언트의 경우 클라이언트가 자신에 대한 정보를 보내는 메시지를 하나 더 받습니다.자세히 살펴보면 EzVPN 클라이언트의 호스트 이름, 클라이언트에서 실행되는 소프트웨어, 소프트웨어의 위치 및 이름을 찾을 수 있습니다	8월 24일 11:31:13 [IKEv1]:IP = 10.48.66.23, IKE_DECODE RECEIVED Messa payloads:HDR + 해시(8) + 알림(11) + 없음(0) 총 길이:184 8월 24일 11:31:13 [IKEv1 DEBUG]:그룹 = EZ, 사용자 이름 = cisco, IP = 10.48. 8월 24일 11:31:13 [IKEv1 DEBUG]:그룹 = EZ, 사용자 이름 = cisco, IP = 10.48. 8월 24일 11:31:13 [IKEv1 DECODE]:사용되지 않는 설명자 - 인덱스 1 8월 24일 11:31:13 [IKEv1 DECODE]:0000:0000000 7534000B 62736E73 2D383731 ....u4..**bsns-871** 0010:2D332E75 3200943 697366F 20383731 **-3**.u2..**Cisco 871** 0020:7535000B 46484B30 393431 32513675 u5..FHK094412Q6u 0030:3600932 32383538 393638 7539009 6.228589568u9. 0040:31343532 31363331 32753300 2B666C61 145216312u3.+**fla** 0050:73683A63 3837302D 61647669 70736572 **sh:c870-관리자** 0060:76696365 736B392D 6D7A2E31 32342D32 **vicesk9-mz.124-2** 0070:302E5435 2E62696E **0.T5.bin** 8월 24일 11:31:13 [IKEv1 DEBUG]:그룹 = EZ, 사용자 이름 = cisco, IP = 10.48. 8월 24일 11:31:13 [IKEv1]:그룹 = EZ, 사용자 이름 = cisco, IP = 192.168.1.100, 8월 24일 11:31:13 [IKEv1 DEBUG]:그룹 = EZ, 사용자 이름 = cisco, IP = 10.48.

터널 확인

ISAKMP

sh cry isa sa **det** 명령의 출력은 다음과 같습니다.

```
 Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.48.66.23
 Type : user Role : responder
 Rekey : no State : AM_ACTIVE
 Encrypt : aes Hash : SHA
 Auth : preshared Lifetime: 86400
 Lifetime Remaining: 86387
 AM_ACTIVE - aggressive mode is active.
```

IPsec

터널을 트리거하는 데 ICMP(Internet Control Message Protocol)가 사용되므로 IPsec SA는 하나만 작동합니다.프로토콜 1은 ICMP입니다.SPI 값은 디버그에서 협상된 값과 다릅니다.이는 2단계 키 재설정 이후 동일한 터널입니다.

sh crypto ipsec sa 명령의 출력:

```
interface: outside
 Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14

 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0)
 current_peer: 10.48.66.23, username: cisco
 dynamic allocated peer ip: 192.168.1.100

 #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: 5, #pkts comp failed: 0, #pkts decomp failed: 0
 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
 #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
 path mtu 1500, ipsec overhead 74, media mtu 1500
 current outbound spi: C4B9A77C
 current inbound spi : EA2B6B15

 inbound esp sas:
 spi: 0xEA2B6B15 (3928714005)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x0000003F
 outbound esp sas:
 spi: 0xC4B9A77C (3300501372)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x00000001
```

관련 정보

- IPsec에 대한 위키백과 문서
- IPsec 문제 해결:디버그 명령 이해 및 사용
- 기술 지원 및 문서 – Cisco Systems