원격 액세스 VPN 문제 해결을 위한 ASA IKEv2 디버깅

목차

소개

이 문서에서는 Cisco AnyConnect Secure Mobility Client와 함께 IKEv2(Internet Key Exchange Version 2)를 사용할 때 Cisco ASA(Adaptive Security Appliance)의 디버그를 이해하는 방법에 대해 설명합니다.이 문서에서는 ASA 컨피그레이션에서 특정 디버그 라인을 변환하는 방법에 대한 정보도 제공합니다.

이 문서에서는 ASA에 VPN 터널이 설정된 후 트래픽을 전달하는 방법에 대해 설명하지 않으며 IPSec 또는 IKE의 기본 개념을 포함하지 않습니다.

사전 요구 사항

요구 사항

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IKEv2(Internet Key Exchange Version 2)
- Cisco ASA(Adaptive Security Appliance) 버전 8.4 이상

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

핵심 문제

Cisco TAC(Technical Assistance Center)에서는 IPSec VPN 터널 설정에 문제가 있는 위치를 파악하기 위해 IKE 및 IPSec 디버그 명령을 자주 사용하지만, 이 명령은 암호화할 수 있습니다.

시나리오

디버그 명령

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
debug aggregate-auth xml 5
```

ASA 컨피그레이션

이 ASA 컨피그레이션은 외부 서버를 사용하지 않고 기본적으로 제공됩니다.

```
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.0

ip local pool webvpn1 10.2.2.1-10.2.2.10

crypto ipsec ikev2 ipsec-proposal 3des
 protocol esp encryption aes-256 aes 3des des
 protocol esp integrity sha-1
crypto dynamic-map dynmap 1000 set ikev2 ipsec-proposal 3des
crypto map crymap 10000 ipsec-isakmp dynamic dynmap
crypto map crymap interface outside

crypto ca trustpoint Anu-ikev2
 enrollment self
 crl configure

crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 2
```

```
 prf sha
 lifetime seconds 86400

crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint Anu-ikev2
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1
ssl trust-point Anu-ikev2 outside

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.0.1047-k9.pkg 1
 anyconnect profiles Anyconnect-ikev2 disk0:/anyconnect-ikev2.xml
 anyconnect enable
 tunnel-group-list enable

group-policy ASA-IKEV2 internal
group-policy ASA-IKEV2 attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ikev2
 default-domain none
 webvpn
 anyconnect modules value dart
 anyconnect profiles value Anyconnect-ikev2 type user

username Anu password lAuoFgF7KmB3D0WI encrypted privilege 15

tunnel-group ASA-IKEV2 type remote-access
tunnel-group ASA-IKEV2 general-attributes
 address-pool webvpn1
 default-group-policy ASA-IKEV2
tunnel-group ASA-IKEV2 webvpn-attributes
 group-alias ASA-IKEV2 enable
```

XML 파일

```
<ServerList>
       <HostEntry>
               <HostName>Anu-IKEV2</HostName>
               <HostAddress>10.0.0.1</HostAddress>
               <UserGroup>ASA-IKEV2</UserGroup>
               <PrimaryProtocol>IPsec</PrimaryProtocol>
       </HostEntry>
</ServerList>
```

참고:XML 클라이언트 프로파일의 UserGroup 이름은 ASA의 터널 그룹 이름과 같아야 합니다 .그렇지 않으면 오류 메시지 'Invalid Host Entry.AnyConnect 클라이언트에서 '를 다시 입력하십시오.

디버그 로그 및 설명

참고:DART(Diagnostics and Reporting Tool)의 로그는 일반적으로 매우 수다합니다. 따라서 이 예에서는 중요하지 않아 특정 DART 로그가 생략되었습니다.

서버 메시지 설명	디버깅
	날짜:04/23/2013

시간:16:24:55
유형:정보
출처:acvpnui

설명:기능:ClientIfcBase::connect
파일:.\ClientIfcBase.cpp
줄:964
사용자가 Anu-IKEV2에 대한 VPN 연결을 요청했습니다.
****
날짜:04/23/2013
시간:16:24:55
유형:정보
출처:acvpnui

설명:사용자에게 전송된 메시지 유형 정보:
Anu-IKEV2에 연결하는 중입니다.
****
날짜:04/23/2013
시간:16:24:55
유형:정보
출처:acvpnui

설명:기능:ApiCert::getCertList
파일:.\ApiCert.cpp
줄:259
찾은 인증서 수:0
****
날짜:04/23/2013
시간:16:25:00
유형:정보
출처:acvpnui

설명:**보안 게이트웨이에 대한 VPN 연결 시작 https://10.0.0.1/ASA-IKEV2**
****
날짜:04/23/2013
시간:16:25:00
유형:정보
출처:acvpnagent

설명:GUI 클라이언트에서 시작된 터널입니다.
****

날짜:04/23/2013
시간:16:25:02
유형:정보
출처:acvpnagent

설명:기능:CIPsecProtocol::connectTransport
파일:.\IPsecProtocol.cpp
줄:1629
192.168.1.1:25170에서 10.0.0.1:500으로 IKE 소켓 열기
****
—IKE_SA_INIT Exchange 시작—

ASA는 클라이언트에서 IKE_SA_INIT 메시지를 수신합니다.
첫 번째 메시지 쌍은 IKE_SA_INIT 교환입니다 .이러한 메시지는 암호화 알고리즘을 협상하고, 비품을 교환하며, DH(Diffie-Hellman) 교환을 수행합니다.
클라이언트에서 받은 IKE_SA_INIT 메시지에는 다음 필드가 포함되어 있습니다.

1. **ISAKMP 헤더** - SPI/version/flags.
2. **SAi1** - IKE 이니시에이터가 지원하는 암호화 알고리즘입니다.
3. **KEi** - 개시자의 DH 공개 키 값입니다.
4. **N** - 개시자 Nonce.

IKEv2-PLAT-4:RECV PKT [IKE_SA_INIT] [192.168.1.1]:25170->[10.0.0.1]:50
InitSPI=0x58aff71141ba436b RespSPI=0x0000000000000000=000 000
IKEv2-PROTO-3:Rx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id:0x
IKEv2-PROTO-3:**HDR**[i:58AFF71141BA436B - r:0000000000000000]
IKEv2-PROTO-4:IKEV2 HDR **ispi:58AFF71141BA436B - rspi:**000000000000
IKEv2-PROTO-4:다음 페이로드:SA, **버전:**2.0
IKEv2-PROTO-4:Exchange 유형:IKE_SA_INIT, **플래그:개시자**
IKEv2-PROTO-4:메시지 ID:0x0, 길이:528

SA 다음 페이로드:KE, 예약됨:0x0, 길이:168
IKEv2-PROTO-4: 마지막 제안:0x0, 예약됨:0x0, 길이:164
제안:1, 프로토콜 ID:IKE, SPI 크기:0, #trans:18
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:3DES
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:DES
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA512
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA384
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA256
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:MD5
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA512
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA384
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA256
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:MD596
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1536_MODP/그룹 5
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_1024_MODP/그룹 2
IKEv2-PROTO-4: 마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_768_MODP/그룹 1

KE 다음 페이로드:N, 예약됨:0x0, 길이:104
DH 그룹:1, 예약됨:0x0

eb 5e 29fe cb2e d1 28 ed 4a 54 b1 13 7c b8 89

f7 62 13 6b df 95 88 28 b5 97 ba 52 ef e4 1d 28
ca 06d1 36 b6 67 32 9a c2 dd 4e d8 c7 80 de 20
36 34 c5 b3 3e 1d 83 1a c7 fb 9d b8 c5 f5 ed 5f
ba ba 4f b6 b2 e2 2d 43 4f a0 b6 90 9a 11 3f 7d
0a 21 c3 4d3 0a d2 1e 33 43 d3 5e cc 4b 38 e0
N 다음 페이로드:VID, 예약됨:0x0, 길이:24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77
ce 7c 0b4
IKEv2-PROTO-5:공급업체별 페이로드 구문 분석:CISCO-DELETE-REASON
이로드:VID, 예약됨:0x0, 길이:23
해독된 패킷:데이터:528바이트
IKEv2-PLAT-3:맞춤형 VID 페이로드 처리
IKEv2-PLAT-3:피어에서 받은 Cisco Copyright VID
IKEv2-PLAT-3:피어에서 AnyConnect EAP VID를 받았습니다.
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:IDLE 이벤
:**EV_RECV_INIT**
IKEv2-PROTO-3:(6):NAT 검색 확인
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:IDLE 이벤
:EV_CHK_리디렉션
IKEv2-PROTO-5:(6):리디렉션 확인이 필요하지 않습니다. 건너뛰는 중입니다.
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:IDLE 이벤
:EV_CHK_CAC
IKEv2-PLAT-5:**새 ikev2 sa 요청이 승인됨**
IKEv2-PLAT-5:수신 협상 SA 수를 1씩 증가
IKEv2-PLAT-5:잘못된 PSH 핸들
IKEv2-PLAT-5:잘못된 PSH 핸들
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:IDLE 이벤
:EV_CHK_쿠키
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:IDLE 이벤
:EV_CHK4_COOKIE_NOTIFY
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_INIT 이
:**EV_VERIFY_MSG**
IKEv2-PROTO-3:(6):**SA 초기화 메시지 확인**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_INIT 이
:EV_INSERT_SA
IKEv2-PROTO-3:(6):SA 삽입
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_INIT 이
:EV_GET_IKE_POLICY
IKEv2-PROTO-3:(6):**구성된 정책을 가져오는 중**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_INIT 이
:**EV_PROC_MSG**
IKEv2-PROTO-2:(6):초기 메시지 처리 중
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B

ASA는
IKE_INIT 메시지입니다
.ASA:

1. 다음 중에서 암호화 제품군을 선택합니다. Initiator가 제공하는 것입니다.
2. 자체 DH 비밀 키를 계산합니다.
3. 다음에서 SKEYID 값을 계산합니다. 어떤 키를 파생시킬 수 있는지 이 IKE_SA입니다.모든 헤더의 헤더 후속 메시지는 암호화 및 인증됩니다 .더 암호화 및 무결성 보호 SKEYID에서 다음과 같이 알려져 있습니다 .

   SK_e - 암호화.**SK_a** - 인증.**SK_d** - 파생되고 사용됨 추가 파생으로 키잉 재료 CHILD_SA별도의 SK_e 및 SK_a는 각 방향에 대해 계산됩니다.

관련 구성:

```
crypto ikev2 policy 10
 encryption aes-192
integrity
sha group 2  prf sha
lifetime
```

```
seconds 86400
crypto ikev2 enable outside
```

R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_INIT 이
:EV_DETECT_NAT
IKEv2-PROTO-3:(6):프로세스 NAT 검색 알림
IKEv2-PROTO-5:(6):처리 nat 탐지 src 알림
IKEv2-PROTO-5:(6):원격 주소가 일치하지 않음
IKEv2-PROTO-5:(6):처리 nat 탐지 dst 알림
IKEv2-PROTO-5:(6):일치하는 로컬 주소
IKEv2-PROTO-5:(6):호스트가 외부에 있는 NAT
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_INIT 이
:EV_CHK_CONFIG_MODE
IKEv2-PROTO-3:(6):유효한 구성 모드 데이터를 받았습니다.
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_INIT 이
:EV_SET_RECD_CONFIG_MODE
IKEv2-PROTO-3:(6):수신된 구성 모드 데이터 설정
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_SET_POLICY
IKEv2-PROTO-3:(6):**구성된 정책 설정**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_CHK_AUTH4PKI
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_PKI_SESH_OPEN
IKEv2-PROTO-3:(6):PKI 세션 열기
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_GEN_DH_KEY
IKEv2-PROTO-3:(6):**DH 공개 키 컴퓨팅**
IKEv2-PROTO-3:(6):
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_NO_이벤트
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5:(6):작업:작업_Null
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_GEN_DH_비밀
IKEv2-PROTO-3:(6):**DH 비밀 키 컴퓨팅**
IKEv2-PROTO-3:(6):
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_NO_이벤트
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5:(6):작업:작업_Null
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN

:EV_GEN_SKEYID
IKEv2-PROTO-3:(6):**skeyid 생성**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
:EV_GET_CONFIG_MODE
ASA는 IKE_SA_INIT 교환 IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
에 대한 응답 메시지를 구성 R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_BLD_IN
합니다. :**EV_BLD_MSG**
이 패킷에는 다음이 포함됩니다. IKEv2-PROTO-2:(6):**초기 메시지 보내기**
IKEv2-PROTO-3: IKE 제안:1, SPI 크기:0(초기 협상),
번호.변형:4
AES-CBC SHA1 SHA96 DH_GROUP_768_MODP/Group 1
IKEv2-PROTO-5:공급업체별 페이로드 구성:DELETE-REASONIKEv2-PROTO
체별 페이로드 구성:(사용자 지정)IKEv2-PROTO-5:공급업체별 페이로드 구성
정)IKEv2-PROTO-5:구성 알림 페이로드:NAT_DETECTION_SOURCE_IPIKE
5:구성 알림 페이로드:NAT_DETECTION_DESTINATION_IPIKEv2-PLAT-2:신
는 발급자 해시를 검색하지 못했거나 사용할 수 있는 항목이 없습니다.
IKEv2-PROTO-5:공급업체별 페이로드 구성:fragmentationikev2-PROTO-3:Tx
10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id:0x0
IKEv2-PROTO-3:**HDR**[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR **ispi:58AFF71141BA436B - rspi:FC696330E6B9**
IKEv2-PROTO-4:다음 페이로드:SA, 버전:2.0
IKEv2-PROTO-4:Exchange 유형:IKE_SA_INIT, **플래그:응답자 메시지-응답**
IKEv2-PROTO-4:메시지 ID:0x0, 길이:386
SA 다음 페이로드:KE, 예약됨:0x0, 길이:48
IKEv2-PROTO-4: 마지막 제안:0x0, 예약됨:0x0, 길이:44
제안:1, 프로토콜 ID:IKE, SPI 크기:0, #trans:4
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:2, 예약됨:0x0, id:SHA1
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
IKEv2-PROTO-4: 마지막 변환:0x0, 예약됨:0x0:길이:8
유형:4, 예약됨:0x0, id:DH_GROUP_768_MODP/그룹 1

KE 다음 페이로드:N, 예약됨:0x0, 길이:104
DH 그룹:1, 예약됨:0x0

c9 30 f9 32 d4 7c1 a7 5b 71 72 09 6e 7e 91 0c
e1 ce b4 a4 3c2 8b 74 4e 20 59 b4 0b1 ff 65
37 88 cc c4 a4 b6 fa 4a 63 03 93 89 e1 7e bd6a
64 9a 38 24 e2 a8 40 f5 a3 d6 ef7 1a df 33 cc
a1 8e fa dc 9c 34 45 79 1a 7c 29 05 87 8a ac 02
98개의 2e 7d cb 41 51d6 fe fc c7 76 83 1d 03 b0 d7
N 다음 페이로드:VID, 예약됨:0x0, 길이:24

c2 28 7f 8c 7d b3 1e 51eb f1 97ec 97 b8 67
d5 e7 c2 f5
VID 다음 페이로드:VID, 예약됨:0x0, 길이:23
ASA는 IKE_SA_INIT 교환 IKEv2-PLAT-4:보낸 PKT [IKE_SA_INIT] **********
에 대한 응답 메시지를 전송 [10.0.0.1]:500->[192.168.1.1]:25170 날짜:04/23/2013
합니다.이제 IKE_SA_INIT InitSPI=0x58aff71141ba436b 시간:16:25:02

1. **ISAKMP 헤더** - SPI/version/flags.
2. **SAr1** - IKE 응답자가 선택하는 암호화 알고리즘입니다.
3. **KEr** - responder의 DH 공개 키 값입니다.
4. **N** - Responder Nonce.

교환이 완료되었습니다
.ASA가 인증 프로세스에 대한 타이머를 시작합니다.

RespSPI=0xfc696330e6b94d7f=0000000 00
IKEv2-PROTO-5:(6):SM 추적->
SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID =
0000000000000 Cur상태:INIT_DONE 이벤트
:EV_완료
IKEv2-PROTO-3:(6):조각화가 활성화되어 있습니다.
IKEv2-PROTO-3:(6):Cisco DeleteReason Notify가 활성화되었습니다.
IKEv2-PROTO-3:(6):SA 초기화 교환 완료
IKEv2-PROTO-5:(6):SM 추적->
SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID =
0000000000000 Cur상태:INIT_DONE 이벤트
:EV_CHK4_ROLE
IKEv2-PROTO-5:(6):SM 추적->
SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID =
0000000000000 Cur상태:INIT_DONE 이벤트
:EV_START_TMR
IKEv2-PROTO-3:(6):인증 메시지 대기 타이머 시작(30초)
IKEv2-PROTO-5:(6):SM 추적->
SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID =
0000000000000 Cur상태:R_WAIT_AUTH 이벤트:EV_NO_이벤트
—IKE_SA_INIT 완료—
— IKE_AUTH 시작—
****
날짜:04/23/2013
시간:16:25:00
유형:정보
출처:acvpnagent

설명:보안 게이트웨이 매개변수:
IP 주소:10.0.0.1
포트:443
URL:"10.0.0.1"
인증 방법:**IKE - EAP-AnyConnect**
IKE ID:
****
날짜:04/23/2013
시간:16:25:00
유형:정보
출처:acvpnagent

설명:**Cisco AnyConnect Secure Mobility Client 연결 시작, 버전 3.0.1047**
****
날짜:04/23/2013
시간:16:25:02
유형:정보
출처:acvpnagent

설명:기능:CIPsecProtocol::initia
파일:.\IPsecProtocol.cpp
줄:345
IPsec 터널이 시작 중입니다.
****

출처:acvpnagent

설명:기능:ikev2_log
파일:.\ikev2_anyconnect_ossl.cpp
줄:2730
IPsec 터널 설정 요청을 받았습니다.로컬 트래픽 선택기 = 주소 범위:0.0.0.0-255.255.255.255 프로토콜:0 포트 범위:0-65535;원격 트래픽 선택기 = 주소 범위:0.0.0.0-255.255.255.255 프로토콜:0 포트 범위:0-65535
****
날짜:04/23/2013
시간:16:25:02
유형:정보
출처:acvpnagent

설명:기능:CIPsecProtocol::connectTransport
파일:.\IPsecProtocol.cpp
줄:1629
192.168.1.1:25171에서 10.0.0.1:4500으로 IKE 소켓 열기
****

EAP로 인증이 수행됩니다.EAP 대화 내에서 단일 EAP 인증 방법만 허용됩니다.ASA는 클라이언트에서 IKE_AUTH 메시지를 수신합니다.

IKEv2-PLAT-4:**RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1]:**4500**
InitSPI=0x58aff71141ba436b RespSPI=0xfc6963330e6b94d7d0=000 00001
IKEv2-PROTO-3:**Rx** [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0

클라이언트가 IDi 페이로드를 포함하는 경우 AUTH 페이로드가 아니라 클라이언트가 ID를 선언했지만 검증되지 않았습니다.디버그에서 AUTH는 페이로드가 IKE_AUTH에 없습니다.

IKEv2-PROTO-3:**HDR**[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 **HDR ispi:58AFF71141BA436B - rspi:FC696330E6B9**
IKEv2-PROTO-4:다음 페이로드:ENCR, **버전:**2.0
IKEv2-PROTO-4:Exchange 유형:IKE_AUTH, **플래그:개시자**
IKEv2-PROTO-4:메시지 ID:0x1, 길이:540
IKEv2-PROTO-5:(6):요청에 mess_id 1;1부터 1까지
REAL 암호 해독된 패킷:데이터:465바이트
IKEv2-PROTO-5:공급업체별 페이로드 구문 분석:(사용자 지정) VID 다음 페이
약됨:0x0, 길이:20

클라이언트에서 보낸 패킷입니다.클라이언트에서 EAP 교환에 성공했습니다.ASA가 확장 가능한 인증 방법, EAP를 메시지 4의 페이로드 및 전송 지연 개시자가 인증이 후속 IKE_AUTH 교환입니다.

IKE_AUTH 개시자 패킷에는 다음이 포함됩니다.

1. **ISAKMP 헤더** - SPI/버전/플래그
2. **IDi** - 클라이언트가

58af f6 11 52 8d b0 2c b8 da 30 46 be 91 56 fa
IDi 다음 페이로드:CERTREQ, 예약됨:0x0, 길이:28
ID 유형:그룹 이름, 예약됨:0x0 0x0

2a 24 41 6e 79 43 6f 6e 6e 65 63 74 43 6c 69 65
6e 74 24 2a
CERTREQ 다음 페이로드:CFG, 예약됨:0x0, 길이:25
인증서 인코딩 X.509 인증서 - 서명
CertReq 데이터&콜론;20바이트
CFG 다음 페이로드:SA, 예약됨:0x0, 길이:196
cfg 유형:**CFG_REQUEST**, 예약됨:0x0, 예약됨:0x0

atrib 유형:내부 IP4 주소, 길이:0

atrib 유형:내부 IP4 넷마스크, 길이:0

atrib 유형:내부 IP4 DNS, 길이:0

IDi를 통해
유형 ID_KEY_ID의 페이로드
의 초기 메시지
IKE_AUTH 교환.이
클라이언트 프로필*이(가)
그룹 이름으로 미리 구성된
또는 이전 성공 후
인증, 클라이언트에
그룹 이름을
기본 설정 파일ASA
터널 그룹 매칭 시도
IKE의 내용이 포함된
이름
IDi 페이로드.첫 번째 이후
성공적인 IPSec VPN은
설정됨, 클라이언트는
그룹 이름(그룹 별칭)이
사용자가 인증되었습니다.이 그룹
이름이 IDi로 전달됩니다.
다음 연결의 페이로드
Cisco의
예상 그룹
사용자.EAP 인증이
클라이언트에서 지정
또는 암시됨
프로필 및 프로필은
<IKEIdentity> 포함
요소를 전송하고 클라이언트가
ID_GROUP 유형 IDi 페이로드
고정 문자열
$AnyConnectClient$.

atrib 유형:내부 IP4 NBNS, 길이:0

atrib 유형:내부 주소 만료, 길이:0

atrib 유형:애플리케이션 버전, 길이:27

41 6e 79 43 6f 6e 65 63 74 20 57 69 6e 64 6f
77 73 20 33 2e 30 2e 31 30 34 37

atrib 유형:내부 IP6 주소, 길이:0

atrib 유형:내부 IP4 서브넷, 길이:0

atrib 유형:알 수 없음 - 28682, 길이:15

77 69 6e 78 70 36 34 74 65 6d 70 6c 61 74 65

atrib 유형:알 수 없음 - 28704, 길이:0

atrib 유형:알 수 없음 - 28705, 길이:0

atrib 유형:알 수 없음 - 28706, 길이:0

atrib 유형:알 수 없음 - 28707, 길이:0

atrib 유형:알 수 없음 - 28708, 길이:0

atrib 유형:알 수 없음 - 28709, 길이:0

atrib 유형:알 수 없음 - 28710, 길이:0

atrib 유형:알 수 없음 - 28672, 길이:0

atrib 유형:알 수 없음 - 28684, 길이:0

atrib 유형:알 수 없음 - 28711, 길이:2

05 7e

atrib 유형:알 수 없음 - 28674, 길이:0

atrib 유형:알 수 없음 - 28712, 길이:0

atrib 유형:알 수 없음 - 28675, 길이:0

atrib 유형:알 수 없음 - 28679, 길이:0

atrib 유형:알 수 없음 - 28683, 길이:0

atrib 유형:알 수 없음 - 28717, 길이:0

3. **CERTREQ** - 클라이언트가
ASA에
기본 인증서.인증서
요청 페이로드 포함

atrib 유형:알 수 없음 - 28718, 길이:0

atrib 유형:알 수 없음 - 28719, 길이:0

atrib 유형:알 수 없음 - 28720, 길이:0

가능
보낸 사람이
의 인증서를
수신기입니다.인증서
요청
페이로드 처리
'인증서 인코딩' 검사
필드
프로세서에
이 유형의 인증서그렇
다면
'인증 기관' 필드는
검사하여
프로세서에 인증서가
있습니다.
최대 100개의
지정된 인증
합니다.이는
인증서.

4. **CFG** -
CFG_REQUEST/
CFG_REPLY는 IKE를
허용합니다.
정보를 요청하는 엔드
포인트
있습니다의 속성이
CFG_REQUEST 구성
페이로드의 길이가
0이 아니라
그것을 제안하기 위해
attribute.CFG_REPLY
구성 페이로드가 반환
될 수 있습니다.
새로운 가치를 제공합
니다아마도
새 특성을 추가할 수
도 있고
필요한 항목을 포함합
니다.
요청자가 반환된 것을
무시합니다.
Cisco가 제공하지 않
는
인식합니다.이 디버그
에서는
클라이언트가 터널을
요청하고 있습니다.

atrib 유형:알 수 없음 - 28721, 길이:0

atrib 유형:알 수 없음 - 28722, 길이:0

atrib 유형:알 수 없음 - 28723, 길이:0

atrib 유형:알 수 없음 - 28724, 길이:0

atrib 유형:알 수 없음 - 28725, 길이:0

atrib 유형:알 수 없음 - 28726, 길이:0

atrib 유형:알 수 없음 - 28727, 길이:0

atrib 유형:알 수 없음 - 28729, 길이:0

SA 다음 페이로드:TSi, 예약됨:0x0, 길이:124
IKEv2-PROTO-4: 마지막 제안:0x0, 예약됨:0x0, 길이:120
제안:1, 프로토콜 ID:ESP, SPI 크기:4, #trans:12
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:12
유형:1, 예약됨:0x0, id:AES-CBC
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:3DES
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:DES
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:1, 예약됨:0x0, id:NULL
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA512
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA384
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA256
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:SHA96
IKEv2-PROTO-4: 마지막 변환:0x3, 예약됨:0x0:길이:8
유형:3, 예약됨:0x0, id:MD596
IKEv2-PROTO-4: 마지막 변환:0x0, 예약됨:0x0:길이:8
유형:5, 예약됨:0x0, id:

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

의 컨피그레이션
CFG_REQUEST.ASA
여기에 응답하고 터널
을 전송합니다.
구성 속성
EAP 교환에 성공했습
니다.

5. **SAi2** - SAi2가 SA를
   시작하고
   2단계와 유사한
   IKEv1에서 변환 세트
   교환
6. **TSi** 및 **TSr** - 개시자
   및
   responder 트래픽 선
   택기
   각각 소스 포함
   및 대상 주소
   initiator 및
   responder를 사용하여
   전달 및 수신 암호화
   트래픽.주소 범위
   모든 트래픽을 수신
   및 발신
   해당 범위가 터널링됩
   니다.이(가)
   제안서는
   응답자는 동일한
   TS를
   다시 로드됩니다.

클라이언트가 제공해야 하는 특성
그룹 인증은
AnyConnect 프로파일 파일
입니다.

***관련 프로필 구성:**

```
<ServerList>
<HostEntry>
 <HostName>Anu-IKEV2
</HostName>
 <HostAddress>10.0.0.1
</HostAddress>
```

```
<PrimaryProtocol>IPsec
</PrimaryProtocol>
```

시작 포트:0, 끝 포트:65535
시작 주소:0.0.0.0, 끝 주소:255.255.255.255

```
</HostEntry>
</ServerList>
```

ASA는 IKE_AUTH 메시지에 대한 응답을 생성하고 클라이언트에 대한 자체 인증을 준비합니다.

해독된 패킷:데이터&콜론;540바이트
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_RECV_AUTH
IKEv2-PROTO-3:(6):인증 메시지를 대기하기 위해 타이머를 중지하는 중
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_CHK_NAT_T
IKEv2-PROTO-3:(6):NAT 검색 확인
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_CHG_NAT_T_PORT
IKEv2-PROTO-2:(6):NAT가 init 포트 25171에 대한 부동 소수점 검색, resp 포
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_PROC_ID
IKEv2-PROTO-2:(6):프로세스 ID에서 유효한 매개 변수를 받았습니다.
IKEv2-PLAT-3:(6) 피어 인증 방법 설정:0
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_인출됨_FOR_PROF_SEL
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3:(6):구성된 정책을 가져오는 중
IKEv2-PLAT-3:ID 페이로드를 기반으로 새 AnyConnect 클라이언트 연결이 탐
IKEv2-PLAT-3:my_auth_method = 1
IKEv2-PLAT-3:(6) 피어 인증 방법 설정:256
IKEv2-PLAT-3:supported_peers_auth_method = 16
IKEv2-PLAT-3:(6) tp_name 설정 대상:아누이케브2
IKEv2-PLAT-3:**신뢰 지점 설정:**아누이케브2
IKEv2-PLAT-3:P1 ID = 0
IKEv2-PLAT-3:IKE_ID_AUTO를 = 9로 변환
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_SET_POLICY
IKEv2-PROTO-3:(6):**구성된 정책 설정**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3:(6):피어의 정책 확인
IKEv2-PROTO-3:(6):**일치하는 인증서를 찾았습니다.**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_CHK_CONFIG_MODE
IKEv2-PROTO-3:(6):유효한 구성 모드 데이터를 받았습니다.
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU :EV_SET_RECD_CONFIG_MODE
IKEv2-PLAT-3:(6) DDNS의 DHCP 호스트 이름은 다음으로 설정됩니다.winxp
IKEv2-PROTO-3:(6):수신된 구성 모드 데이터 설정
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B

R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU
:EV_CHK_AUTH4EAP
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_WAIT_AU
:EV_CHK_EAP
IKEv2-PROTO-3:(6):**EAP 교환 확인**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:**R_BLD_AUT**
:EV_GEN_AUTH
IKEv2-PROTO-3:(6):**내 인증 데이터 생성**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_BLD_AUT
:EV_CHK4_SIGN
IKEv2-PROTO-3:(6):내 인증 방법 가져오기
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_BLD_AUT
:EV_서명
IKEv2-PROTO-3:(6):**서명 인증 데이터**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태:R_BLD_AUT
:EV_OK_AUTH_GEN
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태
:R_BLD_EAP_AUTH_REQ 이벤트:EV_AUTHEN_REQ
IKEv2-PROTO-2:(6):**인증자에게 EAP 요청을 보내는 중**
생성된 요소 이름 **config-auth 값**
요소 config-auth에 특성 이름 클라이언트 값 vpn이 추가되었습니다.
요소 config-auth에 특성 이름 유형 값 hello가 추가되었습니다.
생성된 요소 이름 버전 값 9.0(2)8
요소 config-auth에 요소 이름 버전 값 9.0(2)8을 추가했습니다.
요소 버전에 sg 값을 지정하는 특성 이름이 추가되었습니다.
아래에 생성된 XML 메시지
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="hello**">
<version who="sg">9.0(2)8</version>
</config-auth>

IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태
:R_BLD_EAP_AUTH_REQ 이벤트:EV_RECV_EAP_AUTH
IKEv2-PROTO-5:(6):작업:작업_Null
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태
:R_BLD_EAP_AUTH_REQ 이벤트:EV_CHK_리디렉션
IKEv2-PROTO-3:(6):로드 밸런싱에 대한 플랫폼 확인 리디렉션
IKEv2-PLAT-3:플랫폼에서 확인 리디렉션
IKEv2-PLAT-3:ikev2_ossl_redirect:10.0.0.1에서 세션 수락
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000001 Cur상태
:R_BLD_EAP_AUTH_REQ 이벤트:EV_SEND_EAP_AUTH_REQ
IKEv2-PROTO-2:(6):**EAP 요청을 보내는 중**
IKEv2-PROTO-5:공급업체별 페이로드 구성:CISCO-GRANITEIKEv2-PROTO

ASA는 클라이언트에서 사 **IDr** 다음 페이로드:CERT, 예약됨:0x0, 길이:36

용자 자격 증명을 요청하기 위해 AUTH 페이로드를 전송합니다.ASA는 AUTH 방법을 'RSA'로 전송하므로 클라이언트가 ASA 서버를 인증할 수 있도록 클라이언트에 자체 인증서를 전송합니다.

ASA는 확장 가능한 인증 방법을 사용할 것이므로 메시지 4에 EAP 페이로드를 배치하고 후속 IKE_AUTH 교환에서 개시자 인증이 완료될 때까지 SAr2, TSi 및 TSr을 전송하는 것을 거부합니다.따라서 이러한 세 페이로드가 디버그에 없습니다.

EAP 패킷에는 다음이 포함됩니다.

1. **코드:request** - 인증자가 피어로 이 코드를 전송합니다.
2. **id:1** - id는 EAP 응답과 요청을 일치시키는 데 도움이 됩니다.여기서 값은 1이며, 이는 EAP 교환의 첫 번째 패킷임을 나타냅니다.이 EAP 요청은 EAP 교환을 시작하기 위해 ASA에서 클라이언트로 'hello;'라는 'config-auth' 유형을 가집니다.
3. **길이:150** - EAP 패킷의 길이는 코드, id, 길이 및 EAP 데이터를 포함합니다.
4. **EAP 데이터**.

인증서가 크거나 인증서 체인이 포함된 경우 조각화가 발생할 수 있습니다.개시자 및 responder KE 페이로드에는 모두 큰 키를 포함할 수 있으며, 이는 프래그먼트화에 기여할 수도 있습니다.

```
  ID 유형:DER ASN1 DN, 예약됨:0x0 0x0

   30 1a 31 18 30 16 06 09 2a 86 48 86 f7 0d 01 09
   02 16 09 41 53 41 2d 49 4b 45 56 32
CERT 다음 페이로드:CERT, 예약됨:0x0, 길이:436
  인증서 인코딩 X.509 인증서 - 서명
인증서 데이터 콜론(&F);431바이트
 CERT 다음 페이로드:AUTH, 예약됨:0x0, 길이:436
  인증서 인코딩 X.509 인증서 - 서명
인증서 데이터 콜론(&F);431바이트
AUTH 다음 페이로드:EAP, 예약됨:0x0, 길이:136
  인증 방법 RSA, 예약됨:0x0, 예약됨 0x0
인증 데이터(&P);128바이트
EAP 다음 페이로드:없음, 예약됨:0x0, 길이:154
  코드:요청:id:1, 길이:150
  유형:알 수 없음 - 254
EAP 데이터:145바이트

IKEv2-PROTO-3:Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0
IKEv2-PROTO-3:HDR[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B
IKEv2-PROTO-4:다음 페이로드:ENCR, 버전:2.0
IKEv2-PROTO-4:Exchange 유형:IKE_AUTH, 플래그:응답자 메시지-응답
IKEv2-PROTO-4:메시지 ID:0x1, 길이:1292
 ENCR 다음 페이로드:VID, 예약됨:0x0, 길이:1264
암호화된 데이터(&F);1260바이트

IKEv2-PROTO-5:(6):패킷 조각화, MTU 프래그먼트:544, 프래그먼트 수:3, 조
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
**************************************************

날짜:04/23/2013
시간:16:25:02
유형:정보
```

출처:acvpnagent

설명:기능:ikev2_verify_X509_SIG_certs
파일:.\ikev2_anyconnect_ossl.cpp
줄:2077
사용자로부터 인증서 수락 요청
****
날짜:04/23/2013
시간:16:25:02
유형:오류
출처:acvpnui

설명:기능:CCapiCertificate::verifyChainPolicy
파일:.\Certificates\CapiCertificate.cpp
줄:2032
호출된 함수:인증서 확인 인증서 체인 정책
반환 코드:-2146762487 (0x800B0109)
설명:인증서 체인이 처리되었지만 트러스트 공급자가 신뢰하지 않는 루트 인증
료되었습니다.
****
날짜:04/23/2013
시간:16:25:04
유형:정보
출처:acvpnagent

설명:기능:CEAPMgr::dataRequestCB
파일:.\EAPMgr.cpp
줄:400
EAP 제안 유형:EAP-ANYCONNECT
****

클라이언트가 응답으로 EAP 요청에 응답합니다. EAP 패킷에는 다음이 포함됩니다.

1. **코드:response** - 이 코드는 피어가 EAP 요청에 대한 응답으로 인증자에게 전송됩니다.
2. **id:1 -** id는 EAP 응답과 요청을 일치시키는 데 도움이 됩니다.이 값은 1입니다. 이는 ASA(authenticator)가 이전에 보낸 요청에 대한 응답임을 나타냅니다. 이 EAP 응답에는 'init'의 'config-auth' 유형이 있습니다.클라이언트가 EAP 교환을 초기화하고 있으며

IKEv2-PLAT-4:**RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d MID=0000000 00
IKEv2-PROTO-3:Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0
IKEv2-PROTO-3:HDR[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B9
IKEv2-PROTO-4:다음 페이로드:ENCR, 버전:2.0
IKEv2-PROTO-4:Exchange 유형:IKE_AUTH, 플래그:개시자
IKEv2-PROTO-4:메시지 ID:0x2, 길이:332
IKEv2-PROTO-5:(6):요청에 mess_id 2;2 ~ 2의 예상
REAL 암호 해독된 패킷:데이터:256바이트
EAP 다음 페이로드:없음, 예약됨:0x0, 길이:256
코드:응답:**id:1**, **길이**:252
유형:알 수 없음 - 254
EAP 데이터:247바이트
해독된 패킷:데이터&콜론;332바이트
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000002 Cur상태:R_WAIT_EA
벤트:EV_RECV_AUTH
IKEv2-PROTO-3:(6):인증 메시지를 대기하기 위해 타이머를 중지하는 중
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000002 Cur상태:R_WAIT_EA
벤트:EV_RECV_EAP_RESP
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B

ASA가 인증 요청을 생성하기를 기다리고 있습니다.

3. **길이:252** - EAP 패킷의 길이는 코드, id, 길이 및 EAP 데이터를 포함합니다.
4. **EAP 데이터**.

ASA는 이 응답을 해독하며, 클라이언트는 이전 패킷(인증서 포함)에서 AUTH 페이로드를 수신하고 ASA에서 첫 번째 EAP 요청 패킷을 수신했다고 말합니다.이것이 'init' EAP 응답 패킷에 포함된 것입니다.

ASA가 클라이언트로 보낸 두 번째 요청입니다.
EAP 패킷에는 다음이 포함됩니다.

1. **코드:request** - 인증자가 피어로 이 코드를 전송합니다.
2. **id:2** - id는 EAP 응답과 요청을 일치시키는 데 도움이 됩니다.이 값은 2이며, 이는 교환에서 두 번째 패킷임을 나타냅니다.이 요청에는 'auth-request'의 'config-auth' 유형이 있습니다.ASA는 클라이언트가 사용자 인증 자격 증명을 전송하도록 요청합니다.
3. **길이:457** - EAP 패킷의 길이는 코드, id, 길이 및 EAP 데이터를 포함합니다.
4. **EAP 데이터**.

ENCR 페이로드:
이 페이로드는 암호 해독되고 해당 내용이 추가 페이로드로 구문 분석됩니다.

R_SPI=FC69630E6B94D7F(R) MsgID = 00000000002 Cur상태:R_PROC_EA
이벤트:EV_PROC_MSG
IKEv2-PROTO-2:(6):**EAP 응답 처리**
클라이언트에서 아래 XML 메시지를 받았습니다.
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="init"**>
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<group-select>ASA-IKEV2</group-select>
<group-access>ASA-IKEV2</group-access>
</config-auth>
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000002 Cur상태:R_PROC_EA
이벤트:**EV_RECV_EAP_AUTH**
IKEv2-PROTO-5:(6):작업:작업_Null
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000002 Cur상태:R_BLD_EAP
트:**EV_RECV_EAP_REQ**
IKEv2-PROTO-2:(6):EAP 요청을 보내는 중
아래에 생성된 XML 메시지
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="auth-request"**>
<version who="sg">9.0(2)8</version>
<opaque is-for="sg">
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash>
</opaque>
<csport>443</csport>
<auth id="main">
<양식>
<input type="text" name="username" label="사용자 이름:"></input>
<input type="password" name="password" label="비밀번호:"></input>
</form>
</auth>
</config-auth>
IKEv2-PROTO-3:(6):암호화를 위한 패킷 구축 내용:
EAP 다음 페이로드:없음, 예약됨:0x0, 길이:461
코드:요청:id:2, 길이:457
유형:알 수 없음 - 254
EAP 데이터:452바이트

IKEv2-PROTO-3:Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0x2
IKEv2-PROTO-3:**HDR**[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B94D7F

****
날짜:04/23/2013
시간:16:25:04
유형:정보
출처:acvpnui

설명:기능:SDIMgr::ProcessPromptData
파일:.\SDIMgr.cpp
줄:281
인증 유형이 SDI가 아닙니다.
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnui

설명:기능:ConnectMgr::사용자
파일:.\ConnectMgr.cpp
줄:985
사용자 응답을 처리하는 중입니
****

IKEv2-PROTO-4:다음 페이로드:ENCR, 버전
:2.0
IKEv2-PROTO-4:Exchange 유형:IKE_AUTH,
플래그:**응답자 메시지-응답**
IKEv2-PROTO-4:메시지 ID:0x2, 길이:524
ENCR 다음 페이로드:EAP, 예약됨:0x0, 길이
:496
암호화된 데이터(&F);492바이트

IKEv2-PLAT-4:**보낸 PKT [IKE_AUTH]**
[10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f=0000000
002
IKEv2-PROTO-5:(6):SM 추적->
SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID =
00000000002 Cur상태:R_BLD_EAP_REQ 이
벤트:EV_START_TMR
IKEv2-PROTO-3:(6):**사용자 인증 메시지 대기
타이머 시작**(120초)
IKEv2-PROTO-5:(6):SM 추적->
SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID =
00000000002 Cur상태:R_WAIT_EAP_RESP
이벤트:EV_NO_이벤트

클라이언트는 EAP 페이로드와 함께 다른 IKE_AUTH 개시자 메시지를 보냅니다. EAP 패킷에는 다음이 포함됩니다.

1. **코드:response** - 이 코드는 피어가 EAP 요청에 대한 응답으로 인증자에게 전송됩니다.
2. **id:2** - id는 EAP 응답과 요청을 일치시키는 데 도움이 됩니다.이 값은 2입니다. 이는 ASA(authenticator)가 이전에 보낸 요청에 대한 응답임을 나타냅니다.
3. **길이:420** - EAP 패킷의 길이는 코드, id, 길이 및 EAP 데이터를 포함합니다.
4. **EAP 데이터**.

IKEv2-PLAT-4:RECV PKT [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f=00000000 03
IKEv2-PROTO-3:Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0
IKEv2-PROTO-3:HDR[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B9
IKEv2-PROTO-4:다음 페이로드:ENCR, 버전:2.0
IKEv2-PROTO-4:**Exchange 유형:IKE_AUTH, 플래그:개시자**
IKEv2-PROTO-4:메시지 ID:0x3, 길이:492
IKEv2-PROTO-5:(6):요청에 mess_id 1;3~3에

REAL 암호 해독된 패킷:데이터:424바이트
EAP 다음 페이로드:없음, 예약됨:0x0, 길이:424
코드:응답:id:2, 길이:420
유형:알 수 없음 - 254
EAP 데이터:415바이트

ASA는 이 응답을 처리합니다.클라이언트가 사용자에

해독된 패킷:데이터:492바이트
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B

게 자격 증명 입력을 요청했습니다.이 EAP 응답에는 'auth-reply'의 'config-auth' 유형이 있습니다. 이 패킷은 사용자가 입력한 자격 증명을 포함합니다.

R_SPI=FC69630E6B94D7F(R) MsgID = 00000000003 Cur상태:R_WAIT_EA
벤트:EV_RECV_AUTH
IKEv2-PROTO-3:(6):인증 메시지를 대기하기 위해 타이머를 중지하는 중
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000003 Cur상태:R_WAIT_EA
벤트:EV_RECV_EAP_RESP
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000003 Cur상태:R_PROC_EA
이벤트:EV_PROC_MSG
IKEv2-PROTO-2:(6):**EAP 응답 처리**
클라이언트에서 아래 XML 메시지를 받았습니다.
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="auth-reply"**>
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<session-token></session-token>
<session-id></session-id>
<opaque is-for="sg">
<tunnel-group>**ASA-IKEV2**</tunnel-group>
<config-hash>1367268141499</config-hash></opaque>
<인증>
<password>cisco123</password>
<username>Anu</username></auth>
</config-auth>
IKEv2-PLAT-1:**EAP:사용자 인증 시작**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000003 Cur상태:R_PROC_EA
이벤트:EV_NO_이벤트
IKEv2-PLAT-5:EAP:AAA 콜백에서
검색된 서버 인증서 다이제스트:DACE1C274785F28BA11D64453096BAE29
IKEv2-PLAT-5:**EAP:AAA 콜백에서 성공**
IKEv2-PROTO-3:인증자로부터 응답을 받았습니다.
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000003 Cur상태:R_PROC_EA
이벤트:EV_RECV_EAP_AUTH
IKEv2-PROTO-5:(6):작업:작업_Null

ASA는 교환에서 세 번째 EAP 요청을 작성합니다. EAP 패킷에는 다음이 포함됩니다.

1. **코드:request** - 인증자가 피어로 이 코드를 전송합니다.
2. **id:3** - id는 EAP 응답과 요청을 일치시키는 데 도움이 됩니다.이 값은 3이며, 이는 교환에서 세 번째 패킷임을 나타냅니다.이 패킷은 'config-auth' 유형의 'complete';ASA에서

IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000003 Cur상태:R_BLD_EAP
트:EV_RECV_EAP_REQ
IKEv2-PROTO-2:(6):EAP 요청을 보내는 중
아래에 생성된 XML 메시지
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="complete"**>
<version who="sg">9.0(2)8</version>
<session-id>32768</session-id>
<session-token>18wA0TtGmDxPKQCJywC7fB7EWLCEgz-
ZtjYpAyXx2yJH0H3G3H8t5xpBOx3Ixag</session-token>
<auth id="성공">
<message id="0" param1=" param2="></message
</auth>

IKEv2-PROTO-3:(6):암호화를 위한 패킷 구축내용:
EAP 다음 페이로드:없음, 예약됨:0x0, 길이:4239

응답을 받았으며 EAP 교환이 완료되었습니다.

3. **길이:4235** - EAP 패킷의 길이는 코드, id, 길이 및 EAP 데이터를 포함합니다.
4. **EAP 데이터**.

ENCR 페이로드:
이 페이로드는 암호 해독되고 해당 내용이 추가 페이로드로 구문 분석됩니다.

코드:요청:id:3, 길이:4235
유형:알 수 없음 - 254
EAP 데이터:4230바이트

IKEv2-PROTO-3:Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0x
IKEv2-PROTO-3:HDR[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B9
IKEv2-PROTO-4:다음 페이로드:ENCR, 버전:2.0
IKEv2-PROTO-4:Exchange 유형:IKE_AUTH, 플래그:**응답자 메시지-응답**
IKEv2-PROTO-4:메시지 ID:0x3, 길이:4300
ENCR 다음 페이로드:EAP, 예약됨:0x0, 길이:4272
암호화된 데이터 및 콜론;4268바이트
IKEv2-PROTO-5:(6):패킷 조각화, MTU 프래그먼트:544, **프래그먼트 수:9**, 조직
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000003 Cur상태:R_BLD_EAP
트:EV_START_TMR
IKEv2-PROTO-3:(6):사용자 인증 메시지 대기 타이머 시작(120초)
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000003 Cur상태:R_WAIT_EA
벤트:EV_NO_이벤트
****

날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnagent

설명:**현재 프로필:**Anyconnect-ikev2.xml
수신된 VPN 세션 구성 설정:
설치 유지:활성화됨
프록시 설정:수정 안 함
프록시 서버:없음
프록시 PAC URL:없음
프록시 예외:없음
프록시 잠금:활성화됨
분할 제외:로컬 LAN 액세스 기본 설정을 사용할 수 없습니다.

분할 포함:비활성화됨
스플릿 DNS:비활성화됨
로컬 LAN 와일드카드:로컬 LAN 액세스 기본 설정을 사용할 수 없습니다.
방화벽 규칙:없음
클라이언트 주소:10.2.2.1
클라이언트 마스크:255.0.0.0
클라이언트 IPv6 주소:알 수 없음
클라이언트 IPv6 마스크:알 수 없음
MTU:1406
IKE 연결 유지:20초
IKE DPD:30초
세션 시간 초과:0초
연결 끊기 시간 제한:1800초
유휴 시간 제한:1800초
서버:알 수 없음
MUS 호스트:알 수 없음
DAP 사용자 메시지:없음
쿼런틴 상태:비활성화됨
Always On VPN:비활성화됨
리스 기간:0초
기본 도메인:알 수 없음
홈 페이지:알 수 없음
스마트 카드 분리 연결 해제:활성화됨
라이센스 응답:알 수 없음
****

클라이언트는 EAP 페이로드와 함께 개시자 패킷을 전송합니다.
EAP 패킷에는 다음이 포함됩니다.

1. **코드:response** - 이 코드는 피어가 EAP 요청에 대한 응답으로 인증자에게 전송됩니다.
2. **id:3** - id는 EAP 응답과 요청을 일치시키는 데 도움이 됩니다.이 값은 3입니다. 이는 ASA(authenticator)가 이전에 보낸 요청에 대한 응답임을 나타냅니다. 이제 ASA가 클라이언트에서 응답 패킷을 수신합니다. 이 클라이언트는 'config-auth' 유형이 'ack'입니다.이 응답은 이전에 ASA에서 보낸 EAP 'complete' 메시지를 승인합니다.

IKEv2-PLAT-4:**RECV PKT** [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc6963330e6b94d7f00=0000 004
IKEv2-PROTO-3:Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0
IKEv2-PROTO-3:HDR[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B9
IKEv2-PROTO-4:다음 페이로드:ENCR, 버전:2.0
IKEv2-PROTO-4:**Exchange 유형:IKE_AUTH, 플래그:개시자**
IKEv2-PROTO-4:메시지 ID:0x4, 길이:252
IKEv2-PROTO-5:(6):요청에 mess_id 4;4~4의 예상

REAL 암호 해독된 패킷:데이터:177바이트
EAP 다음 페이로드:없음, 예약됨:0x0, 길이:177
코드:응답:id:3, 길이:173
유형:알 수 없음 - 254
EAP 데이터:168바이트

3. **길이:173** - EAP 패킷의 길이는 코드, id, 길이 및 EAP 데이터를 포함합니다.
4. **EAP 데이터**.

ASA는 이 패킷을 처리합니다.더
EAP 교환에 성공했습니다.ASA
터널 그룹 전송 준비
다음 패킷의 컨피그레이션, 의 클라이언트에서 이전에 요청함
IDi 페이로드.ASA는
클라이언트의 응답 패킷 - 에는 'ack'의 'config-auth' 유형이 있습니다. 이
응답에서 EAP를 승인함
'complete' 메시지가 전송됨
ASA가 이전에 제공되었습니다.

관련 구성:

```
tunnel-group ASA-IKEV2
type remote-access
tunnel-group ASA-IKEV2
general-attributes
 address-pool webvpn1
 authorization-server-group
 LOCAL default-group-policy
ASA-IKEV2
tunnel-group ASA-IKEV2
webvpn-attributes
 group-alias ASA-IKEV2
enable
```

이제 EAP 교환에 성공했습니다.
EAP 패킷에는 다음이 포함됩니다.

1. **코드**:**성공** - 이 코드는 인증자가 전송한 EAP가 완료된 후 피어
인증 방법.이 피어에
성공적으로 인증됨
인증자입니다.
2. **id:3** - ID가 요청에 대한 EAP 응답
이 값은 3입니다.
이는 Cisco의
에서 이전에 보낸 요

해독된 패킷:데이터:252바이트
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_WAIT_E
이벤트:EV_RECV_AUTH
IKEv2-PROTO-3:(6):인증 메시지를 대기하기 위해 타이머를 중지하는 중
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_WAIT_E
이벤트:EV_RECV_EAP_RESP
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_PROC_
이벤트:EV_PROC_MSG
IKEv2-PROTO-2:(6):**EAP 응답 처리**
클라이언트에서 아래 XML 메시지를 받았습니다.
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="ack"**>
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
</config-auth>

IKEv2-PLAT-3:(6) aggrAuthHdl이 0x2000으로 설정됨
IKEv2-PLAT-3:(6) **tg_name을 다음으로 설정:ASA-IKEV2**
IKEv2-PLAT-3:(6) **그룹 유형 설정:RA**
IKEv2-PLAT-1:**EAP:인증 성공**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_PROC_
이벤트:EV_RECV_EAP_SUCCESS
IKEv2-PROTO-2:(6):EAP 상태 메시지를 보내는 중
IKEv2-PROTO-3:(6):암호화를 위한 패킷 구축내용:
EAP 다음 페이로드:없음, 예약됨:0x0, 길이:8
코드:성공:id:3, 길이:4

IKEv2-PROTO-3:Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0x
IKEv2-PROTO-3:HDR[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B9
IKEv2-PROTO-4:다음 페이로드:ENCR, 버전:2.0
IKEv2-PROTO-4:Exchange 유형:IKE_AUTH, 플래그:응답자 메시지-응답
IKEv2-PROTO-4:메시지 ID:0x4, 길이:76
ENCR 다음 페이로드:EAP, 예약됨:0x0, 길이:48
암호화된 데이터&콜론;44바이트

IKEv2-PLAT-4:**보낸 PKT [IKE_AUTH]** [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f=0000000 004
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태:R_PROC_
이벤트:EV_START_TMR
IKEv2-PROTO-3:(6):인증 메시지 대기 타이머 시작(30초)
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B

청
ASA(인증자). 세 번째 세트
Exchange의 패킷 수는
성공 및 EAP 교환 성공.

3. **길이:4** - EAP의 길이 패킷에는 코드, id, 길이 및 EAP 데이터.
4. **EAP 데이터**.

R_SPI=FC69630E6B94D7F(R) MsgID = 0000000000000 Cur상태 :**R_WAIT_EAP_AUTH_VERIFY** 이벤트:EV_NO_이벤트

EAP 교환이 성공하므로 클라이언트는 AUTH 페이로드와 함께 IKE_AUTH 개시자 패킷을 전송합니다.공유 비밀 키에서 AUTH 페이로드가 생성됩니다.

IKEv2-PLAT-4:RECV PKT [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f=00000000 05
IKEv2-PROTO-3:Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0
IKEv2-PROTO-3:HDR[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B9
IKEv2-PROTO-4:다음 페이로드:ENCR, 버전:2.0
IKEv2-PROTO-4:Exchange 유형:IKE_AUTH, **플래그:개시자**
IKEv2-PROTO-4:메시지 ID:0x5, 길이:92
IKEv2-PROTO-5:(6):요청에 mess_id 5;5~5까지

EAP 인증이 지정된 경우 또는
클라이언트 프로파일 및 프로파일에 포함되지 않음 <IKEIdentity> 요소, 클라이언트가
ID_GROUP 유형 IDi 페이로드
고정 문자열 *$AnyConnectClient$*.
ASA에서 이 메시지를 처리합니다.

REAL Decrypted packet:Data:28바이트
AUTH 다음 페이로드:없음, 예약됨:0x0, 길이:28
인증 방법 PSK, 예약됨:0x0, 예약됨 0x0
인증 데이터:20바이트
해독된 패킷:데이터:92바이트
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태 :R_WAIT_EAP_AUTH_VERIFY 이벤트:EV_RECV_AUTH
IKEv2-PROTO-3:(6):인증 메시지를 대기하기 위해 타이머를 중지하는 중
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_GET_EAP_KEY
IKEv2-PROTO-2:(6):EAP 교환 후 피어를 확인하기 위해 AUTH 전송
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_VERIFY_AUTH
IKEv2-PROTO-3:(6):**인증 데이터 확인**
IKEv2-PROTO-3:(6):**ID *$AnyConnectClient$*, key len 20에 대해 사전 공유 키**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_GET_CONFIG_MODE
IKEv2-PLAT-3:컨피그레이션 모드 응답이 대기되었습니다.
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_NO_이벤트
IKEv2-PLAT-3:PSH:client=AnyConnect client-version=3.0.1047 client-os=Win client-os-version=
IKEv2-PLAT-3:구성 모드 회신 완료
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A

관련 구성:

```
crypto dynamic-map dynmap
1000
set ikev2 ipsec-proposal
3des
crypto map crymap 10000
ipsec-isakmp dynamic dynmap
crypto map crymap interface
outside
```

트:EV_OK_GET_CONFIG
IKEv2-PROTO-3:(6):전송할 컨피그레이션 모드 데이터 있음
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_CHK4_IC
IKEv2-PROTO-3:(6):초기 연락처 처리 중
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_CHK_리디렉션
IKEv2-PROTO-5:(6):이 세션에 대해 리디렉션 검사가 이미 완료되었습니다. 건
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_PROC_SA_TS
IKEv2-PROTO-2:(6):**인증 메시지 처리 중**
IKEv2-PLAT-1:**암호화 맵:맵 동적 맵 시퀀스 1000할당된 IP를 사용하여 조정된**
IKEv2-PLAT-3:**암호화 맵:동적 맵 동적 맵 맵 시퀀스 1000에서 일치**
IKEv2-PLAT-3:RA 연결에 대해 PFS가 비활성화됨
IKEv2-PROTO-3:(6):
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_NO_이벤트
IKEv2-PLAT-2:SPI 0x30B848A4에 대한 PFKEY SPI 콜백을 받았습니다. 오류
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_VERIFY_A
트:EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2:(6):**인증 메시지 처리 중**

ASA는 SA, TSi 및 TSr 페이로드를 사용하여 IKE_AUTH 응답 메시지를 작성합니다.
IKE_AUTH responder 패킷에는 다음이 포함됩니다.

1. **ISAKMP 헤더** - SPI/version/flags.
2. **AUTH 페이로드** - 선택한 인증 방법을 사용합니다.
3. **CFG** - CFG_REQUEST/CFG_REPLY를 사용하면 IKE 엔드포인트가 피어에서 정보를 요청할 수 있습니다 .CFG_REQUEST 구성 페이로드의 속성이 0이 아닌 경우 해당 속성에 대한 제안으로 사용됩니다 .CFG_REPLY 구성 페이로드는 해당 값 또는 새 값을 반환할 수

IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:**R_BLD_AUT**
:EV_MY_AUTH_METHOD
IKEv2-PROTO-3:(6):**내 인증 방법 가져오기**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_BLD_AUT
:EV_GET_PRESHR_KEY
IKEv2-PROTO-3:(6):***$AnyConnectClient$*에 대한 피어의 사전 공유 키 가져**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_BLD_AUT
:EV_GEN_AUTH
IKEv2-PROTO-3:(6):**내 인증 데이터 생성**
IKEv2-PROTO-3:(6):**id hostname=ASA-IKEV2, key len 20에 사전 공유 키 사용**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_BLD_AUT
:EV_CHK4_SIGN
IKEv2-PROTO-3:(6):내 인증 방법 가져오기
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:R_BLD_AUT
:EV_OK_AUTH_GEN
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태
:R_BLD_EAP_AUTH_VERIFY 이벤트:EV_GEN_AUTH
IKEv2-PROTO-3:(6):내 인증 데이터 생성
IKEv2-PROTO-3:(6):id hostname=ASA-IKEV2, key len 20에 사전 공유 키 사용
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태

있습니다.또한 새 특성을 추가할 수 있으며 요청된 특성을 일부 포함하지 않을 수도 있습니다.요청자는 인식하지 못하는 반환된 특성을 무시합니다.ASA는 CFG_REPLY 패킷의 터널 구성 특성을 사용하여 클라이언트에 응답합니다.

4. **SAr2** - SAr2가 SA를 시작합니다. 이는 IKEv1의 2단계 변환 세트 교환과 유사합니다.
5. **TSi** 및 **TSr** - 암호화된 트래픽을 포워딩하고 수신하기 위해 개시자 및 responder 트래픽 선택기에는 각각 initiator 및 responder의 소스 및 목적지 주소가 포함됩니다.주소 범위는 해당 범위에서 들어오고 나가는 모든 트래픽이 터널링되도록 지정합니다.제안서가 응답자에게 수락될 경우 동일한 TS 페이로드를 다시 전송합니다.

ENCR 페이로드:
이 페이로드는 암호 해독되고 해당 내용이 추가 페이로드로 구문 분석됩니다.

:R_BLD_EAP_AUTH_VERIFY 이벤트:EV_SEND_AUTH
IKEv2-PROTO-2:(6):**EAP 교환 후 피어를 확인하기 위해 AUTH 전송**
IKEv2-PROTO-3: ESP 제안:1, SPI 크기:4(IPSec 협상),
번호.변형:3
 AES-CBC SHA96
IKEv2-PROTO-5:구성 알림 페이로드:ESP_TFC_NO_SUPPORTIKEv2-PROT
림 페이로드:NON_FIRST_FRAGSIKEv2-PROTO-3:(6):암호화를 위한 패킷 구
AUTH 다음 페이로드:CFG, 예약됨:0x0, 길이:28
 인증 방법 PSK, 예약됨:0x0, 예약됨 0x0
인증 데이터(&P);20바이트
CFG 다음 페이로드:SA, 예약됨:0x0, 길이:4196
 cfg 유형:**CFG_REPLY,** 예약됨:0x0, 예약됨:0x0

atrib 유형:내부 IP4 주소, 길이:4

 + 01 01 01 01
atrib 유형:내부 IP4 넷마스크, 길이:4

 + 00 00 00 00
atrib 유형:내부 주소 만료, 길이:4

 + 00 00 00 00
atrib 유형:애플리케이션 버전, 길이:16

 41 53 41 20 31 30 30 2 37 28 36 29 31 31 36 00
atrib 유형:알 수 없음 - 28704, 길이:4

 + 00 00 00 00
atrib 유형:알 수 없음 - 28705, 길이:4

 + 00 00 07 08
atrib 유형:알 수 없음 - 28706, 길이:4

 + 00 00 07 08
atrib 유형:알 수 없음 - 28707, 길이:1

 01
atrib 유형:알 수 없음 - 28709, 길이:4

 00 00 00 1e
atrib 유형:알 수 없음 - 28710, 길이:4

 + 00 00 00 14
atrib 유형:알 수 없음 - 28684, 길이:1

 01
atrib 유형:알 수 없음 - 28711, 길이:2

 05 7e
atrib 유형:알 수 없음 - 28679, 길이:1

 00
atrib 유형:알 수 없음 - 28683, 길이:4

```
   80 0b 00 01
  atrib 유형:알 수 없음 - 28725, 길이:1

   00
  atrib 유형:알 수 없음 - 28726, 길이:1

   00
  atrib 유형:알 수 없음 - 28727, 길이:4056

   3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31
   2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54
   46 2d 38 22 3f 3e 3c 63 6f 6e 66 69 67 2d 61 75
   74 68 20 63 6c 69 65 6e 74 3d 22 76 70 6e 22 20
   74 79 70 65 3d 22 63 6f 6d 70 6c 65 74 65 22 3e
   3c 76 65 72 73 69 6f 6e 20 77 68 6f 3d 22 73 67
   22 3e 31 30 30 2e 37 28 36 29 31 31 36 3c 2f 76
   65 72 73 69 6f 6e 3c 73 65 73 73 69 6f 6e 2d
   69 64 3e 38 31 39 32 3c 2f 73 65 73 73 69 6f 6e
<snip>
   72 6f 66 69 6c 65 2d 6d 61 6e 69 66 65 73 74 3e
   3c 2f 63 6f 6e 66 69 67 3e 3c 2f 63 6f 6e 66 69
   67 2d 61 75 74 68 3e 00
  atrib 유형:알 수 없음 - 28729, 길이:1

   00
 SA 다음 페이로드:TSi, 예약됨:0x0, 길이:44
IKEv2-PROTO-4:   마지막 제안:0x0, 예약됨:0x0, 길이:40
 제안:1, 프로토콜 ID:ESP, SPI 크기:4, #trans:3
IKEv2-PROTO-4:     마지막 변환:0x3, 예약됨:0x0:길이:12
   유형:1, 예약됨:0x0, id:AES-CBC
IKEv2-PROTO-4:     마지막 변환:0x3, 예약됨:0x0:길이:8
   유형:3, 예약됨:0x0, id:SHA96
IKEv2-PROTO-4:     마지막 변환:0x0, 예약됨:0x0:길이:8
   유형:5, 예약됨:0x0, id:

 TSi 다음 페이로드:TSr, 예약됨:0x0, 길이:24
   TS 수:1, 예약됨 0x0, 예약됨 0x0
   TS 유형:TS_IPV4_ADDR_RANGE, proto id:0, 길이:16
   시작 포트:0, 끝 포트:65535
   시작 주소:10.2.2.1, 끝 주소:10.2.2.1
 TSr 다음 페이로드:알림, 예약됨:0x0, 길이:24
   TS 수:1, 예약됨 0x0, 예약됨 0x0
   TS 유형:TS_IPV4_ADDR_RANGE, proto id:0, 길이:16
   시작 포트:0, 끝 포트:65535
   시작 주소:0.0.0.0, 끝 주소:255.255.255.255
IKEv2-PROTO-3:Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id:0x
IKEv2-PROTO-3:HDR[i:58AFF71141BA436B - r:FC696330E6B94D7F]
IKEv2-PROTO-4:IKEV2 HDR ispi:58AFF71141BA436B - rspi:FC696330E6B9
IKEv2-PROTO-4:다음 페이로드:ENCR, 버전:2.0
IKEv2-PROTO-4:Exchange 유형:IKE_AUTH, 플래그:응답자 메시지-응답
IKEv2-PROTO-4:메시지 ID:0x5, 길이:4396
 ENCR 다음 페이로드:AUTH, 예약됨:0x0, 길이:4368
```

ASA는 9개의 패킷으로 조각화된 이 IKE_AUTH 응답 메시지를 전송합니다 .IKE_AUTH 교환이 완료되었습니다.

암호화된 데이터(&F);4364바이트
IKEv2-PROTO-5:(6):패킷 조각화, MTU 프래그먼트:544, **프래그먼트 수:9**, 조각
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PLAT-4:보낸 PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7d=00000000000
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:AUTH_DONE
:EV_확인
IKEv2-PROTO-5:(6):작업:작업_Null
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:**AUTH_DONE**
:EV_PKI_SESH_CLOSE
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnagent

설명:기능:ikev2_log
파일:.\ikev2_anyconnect_ossl.cpp
줄:2730
IPsec 연결이 설정되었습니다.
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnagent

설명:IPsec 세션 등록:
암호화:AES-CBC
PRF:SHA1
HMAC:SHA96
로컬 인증 방법:PSK
원격 인증 방법:PSK
시퀀스 ID:0
키 크기:192
DH 그룹:1
키 재설정 시간:4294967초

로컬 주소:192.168.1.1
원격 주소:10.0.0.1
로컬 포트:4500
원격 포트:4500
세션 ID:1
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnui

설명:**보안 게이트웨이에 구성된 프로파일은 다음과 같습니다.**Anyconnect-ikev
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnui

설명:사용자에게 전송된 메시지 유형 정보:
VPN 세션을 설정하는 중...
****
—IKE_AUTH 교환 종료—
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpndownloader

설명:기능:ProfileMgr::loadProfiles
파일:..\Api\ProfileMgr.cpp
줄:148
로드된 프로필:
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConn
Mobility Client\Profile\anyconnect-ikev2.xml
****
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpndownloader

설명:현재 기본 설정:
서비스 사용 안 함:거짓
인증서 저장소 재정의:거짓
인증서 저장소:모두
사전 연결 메시지 표시:거짓
자동 연결 시작:거짓
OnConnect 최소화:참
로컬 LAN 액세스:거짓
자동 다시 연결:참
자동 다시 연결 동작:연결 끊기일시 중지
로그온 사용:거짓
자동 업데이트:참

RSASecurIDI통합:자동
Windows 로그온 적용:단일 로컬 로그온
WindowsVPNE설정:로컬 사용자만
프록시 설정:네이티브
로컬 프록시 연결 허용:참
PPExclusion:사용 안 함
PPExclusionServerIP:
자동 VPNP정책:거짓
신뢰할 수 있는 네트워크 정책:연결 끊기
신뢰할 수 없는 네트워크 정책:연결
신뢰할 수 있는 DNSD도메인:
신뢰할 수 있는 DNSS서버:
AlwaysOn:거짓
연결 실패 정책:닫힘
CaptivePortal교정 허용:거짓
CaptivePortalRemediationTimeout:5
마지막 VPNL로컬 리소스 규칙 적용:거짓
VPNDisconnect 허용:참
스크립팅활성화:거짓
TerminateScriptOnNextEvent:거짓
PostSBLOnConnectScript 사용:참
자동 인증서 선택:참
로그오프 유지:거짓
사용자 적용:동일사용자전용
자동서버선택활성화:거짓
자동 서버 선택개선:20
자동 서버 선택 일시 중지 시간:4
인증 시간 초과:12
SafeWordSofToken통합:거짓
IPsecOverSSL 허용:거짓
ClearSmartcardPin:참
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnui

설명:사용자에게 전송된 메시지 유형 정보:
VPN 설정 - 시스템을 검사하는 중...
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnui

설명:사용자에게 전송된 메시지 유형 정보:
VPN 설정 - VPN 어댑터를 활성화하는 중...
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnagent

설명:기능:CVirtualAdapter::DoRegistryRepair
파일:.\WindowsVirtualAdapter.cpp
줄:1869
VA 제어 키를 찾았습니다.SYSTEM\CurrentControlSet\ENUM\ROOT\NET\00
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnagent

설명:**새 네트워크 인터페이스가 탐지되었습니다.**
****
날짜:04/23/2013
시간:16:25:07
유형:정보
출처:acvpnagent

설명:기능:CRouteMgr::logInterfaces
파일:.\RouteMgr.cpp
줄:2076
호출된 함수:log인터페이스
반환 코드:0(0x000000000)
설명:IP 주소 인터페이스 목록:
10.2.2.1
192.168.1.1
****
날짜:04/23/2013
시간:16:25:08
유형:정보
출처:acvpnagent

설명:호스트 구성:
공용 주소:192.168.1.1
공용 마스크:255.255.255.0
개인 주소:10.2.2.1
전용 마스크:255.0.0.0
개인 IPv6 주소:해당 없음
프라이빗 IPv6 마스크:해당 없음
원격 피어:10.0.0.1(TCP 포트 443, UDP 포트 500), 10.0.0.1(UDP 포트 4500)
사설 네트워크:없음
공용 네트워크:없음
터널 모드:예
****

연결이 SA(Security Association) 데이터베이스에 입력되고 상태가 REGISTERED입니다.또한 ASA는 CAC(Common Access Card) 통계, 중복 SA의 존재 여부, DPD(Dead Peer Detection) 등의 값을 설정하는 등의 몇 가지 검사를 수행합니다.

IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:AUTH_DONE
:**EV_INSERT_IKE**
IKEv2-PROTO-2:(6):**SA 생성;데이터베이스에 SA 삽입**
IKEv2-PLAT-3:
연결 상태:UP... 피어:192.168.1.1:25171, phase1_id:*$AnyConnect클라이언트
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:AUTH_DONE
:**EV_REGISTER_SESSION**
IKEv2-PLAT-3:(6) **사용자 이름 설정:아누**

IKEv2-PLAT-3:
연결 상태:등록됨... 피어:192.168.1.1:25171, **phase1_id:*$AnyConnect클라이**
IKEv2-PROTO-3:(6):DPD 초기화 중, 10초 동안 구성
IKEv2-PLAT-3:(6) mib_index 설정:4501
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:AUTH_DONE
:EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3:(6):IPSEC 키 자료 로드
IKEv2-PLAT-3:암호화 맵:동적 맵 동적 맵 맵 시퀀스 1000에서 일치
IKEv2-PLAT-3:(6) **DPD 최대 시간:**30
IKEv2-PLAT-3:(6) **DPD 최대 시간:**30
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:AUTH_DONE
:EV_START_ACCT
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:AUTH_DONE
:EV_CHECK_DUPLES
IKEv2-PROTO-3:(6):**중복 SA 확인**
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:AUTH_DONE
:EV_CHK4_ROLE
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:READY 이벤
:EV_R_UPDATE_CAC_STATS
IKEv2-PLAT-5:새 ikev2 sa 요청이 활성화됨
IKEv2-PLAT-5:수신 협상에 대한 감소 수
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:READY 이벤
인
IKEv2-PROTO-3:(6):협상 컨텍스트를 삭제하는 시작 타이머
IKEv2-PROTO-5:(6):SM 추적-> SA:I_SPI=58AFF71141BA436B
R_SPI=FC69630E6B94D7F(R) MsgID = 00000000005 Cur상태:READY 이벤
:EV_NO_이벤트
IKEv2-PLAT-2:SPI 0x77EE5348에 대한 PFKEY 추가 SA를 받았습니다. 오류
IKEv2-PLAT-2:SPI 0x30B848A4에 대한 PFKEY 업데이트 SA를 받았습니다.
****

날짜:04/23/2013
시간:16:25:08
유형:정보
출처:acvpnagent

설명:**VPN 연결이 설정되었으며 이제 데이터를 전달할 수 있습니다.**
****

날짜:04/23/2013
시간:16:25:08
유형:정보
출처:acvpnui

설명:사용자에게 전송된 메시지 유형 정보:
VPN 설정 - 시스템 구성 중...
****

날짜:04/23/2013
시간:16:25:08

유형:정보
출처:acvpnui

설명:사용자에게 전송된 메시지 유형 정보:
VPN을 설정하는 중...
****
날짜:04/23/2013
시간:16:25:37
유형:정보
출처:acvpnagent

파일:.\IPsecProtocol.cpp
줄:945
IPsec 터널이 설정됨
****

터널 확인

AnyConnect

show vpn-sessiondb detail anyconnect 명령의 샘플 출력은 다음과 같습니다.

```
Session Type: AnyConnect Detailed

Username     : Anu                    Index        : 2
Assigned IP  : 10.2.2.1                Public IP    : 192.168.1.1
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : AES192 AES256          Hashing      : none SHA1 SHA1
Bytes Tx     : 0                      Bytes Rx     : 11192
Pkts Tx      : 0                      Pkts Rx      : 171
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : ASA-IKEV2              Tunnel Group : ASA-IKEV2
Login Time   : 22:06:24 UTC Mon Apr 22 2013
Duration     : 0h:02m:26s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 192.168.1.1
  Encryption   : none                   Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
  Client Type  : AnyConnect
Client Ver   : 3.0.1047
IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 25171                  UDP Dst Port : 4500
```

```
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : AES192                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86254 Seconds
  PRF          : SHA1                  D/H Group    : 1
  Filter Name  :
  Client OS    : Windows
IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 10.2.2.1/255.255.255.255/0/0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28654 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607990 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
  Bytes Tx     : 0                     Bytes Rx     : 11192
  Pkts Tx      : 0                     Pkts Rx      : 171
 NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 146 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
Redirect URL :
```

ISAKMP

show crypto ikev2 sa 명령의 샘플 출력은 다음과 같습니다.

```
ASA-IKEV2#  show crypto ikev2 sa

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
     Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
   Life/Active Time: 86400/112 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
```

show crypto ikev2 sa detail 명령의 샘플 출력은 다음과 같습니다.

```
ASA-IKEV2# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
      Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
      Life/Active Time: 86400/98 sec
      Session-id: 2
      Status Description: Negotiation done
      Local spi: FC696330E6B94D7F       Remote spi: 58AFF71141BA436B
      Local id: hostname=ASA-IKEV2
      Remote id: *$AnyConnectClient$*
      Local req mess id: 0              Remote req mess id: 9
```

```
      Local next mess id: 0             Remote next mess id: 9
      Local req queued: 0               Remote req queued: 9       Local window:
1                  Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is detected  outside
      Assigned host addr: 10.2.2.1
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
         AH spi in/out: 0x0/0x0
         CPI in/out: 0x0/0x0
           Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPSec

show crypto ipsec sa 명령의 샘플 출력은 다음과 같습니다.

```
ASA-IKEV2# show crypto ipsec sa
interface: outside
    Crypto map tag: dynmap, seq num: 1000, local addr: 10.0.0.1

   local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
      current_peer: 192.168.1.1, username: Anu
      dynamic allocated peer ip: 10.2.2.1

     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 163, #pkts decrypt: 108, #pkts verify: 108
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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: 55

     local crypto endpt.: 10.0.0.1/4500, remote crypto endpt.: 192.168.1.1/25171
      path mtu 1488, ipsec overhead 82, media mtu 1500
      current outbound spi: 77EE5348
      current inbound spi : 30B848A4

  inbound esp sas:
     spi: 0x30B848A4 (817383588)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={RA, Tunnel,  NAT-T-Encaps, }
        slot: 0, conn_id: 8192, crypto-map: dynmap
        sa timing: remaining key lifetime (sec): 28685
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
        0xFFAD6BED 0x7ABFD5BF
    outbound esp sas:
      spi: 0x77EE5348 (2012107592)
         transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={RA, Tunnel,  NAT-T-Encaps, }
         slot: 0, conn_id: 8192, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28685
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
         0x00000000 0x00000001
```

관련 정보

- RFC 4306, IKEv2(Internet Key Exchange) 프로토콜
- RFC 3748, EAP(Extensible Authentication Protocol)
- RFC 5996, IKEv2(Internet Key Exchange Protocol Version 2)
- 기술 지원 및 문서 – Cisco Systems