PSK가 있는 사이트 간 VPN에 ASA IKEv2 디버깅 사용

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)의 IKEv2(Internet Key Exchange Version 2) 디버깅에 대한 정보를 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

핵심 문제

IKEv2에서 사용되는 패킷 교환 프로세스는 IKEv1에서 사용되는 것과 근본적으로 다릅니다. IKEv1에서는 6개의 패킷으로 구성된 Phase1 교환과 3개의 패킷으로 구성된 Phase2 교환이 명확하게 구분되어 있습니다. IKEv2 교환은 가변적입니다.

> **팁**: 차이점과 패킷 교환 프로세스에 대한 자세한 내용은 IKEv2 패킷 교환 및 프로토콜 수준 디버깅을 참조하십시오.

사용되는 디버그

다음 두 디버그는 IKEv2에 사용됩니다.

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
```

ASA 컨피그레이션

이 섹션에서는 ASA1(initiator) 및 ASA2(responder)에 대한 컨피그레이션의 예를 제공합니다.

ASA1

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.0.0.1 255.255.255.0

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 192.168.1.2 255.255.255.0

crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5

access-list l2l_list extended permit ip host 192.168.1.1
  host  192.168.2.99
access-list l2l_list extended permit ip host 192.168.1.12
  host 192.168.2.99

crypto map outside_map 1 match address l2l_list
crypto map outside_map 1 set peer 10.0.0.2
crypto map outside_map 1 set ikev2 ipsec-proposal AES256
crypto map outside_map interface outside

crypto ikev2 policy 1
encryption aes-256
integrity sha
group 2
prf sha
lifetime seconds 86400
```

```
crypto ikev2 enable outside

tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

ASA2

```
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.0.0.2 255.255.255.0

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 192.168.2.1 255.255.255.0

crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5

access-list l2l_list extended permit ip host 192.168.2.99
  host 192.168.1.1
access-list l2l_list extended permit ip host 192.168.2.99
  host 192.168.1.12

crypto map outside_map 1 match address l2l_list
crypto map outside_map 1 set peer 10.0.0.1
crypto map outside_map 1 set ikev2 ipsec-proposal AES256
crypto map outside_map interface outside

crypto ikev2 policy 1
encryption aes-256
integrity sha
group 2
prf sha
lifetime seconds 86400

crypto ikev2 enable outside
tunnel-group 10.0.0.1 type ipsec-l2l
tunnel-group 10.0.0.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

디버그

이 섹션에서는 ASA1(initiator) 및 ASA2(responder) 터널 협상, 하위 SA(Security Association) 디버그 및 메시지 설명에 대해 설명합니다.

터널 협상

ASA1은 피어 ASA **10.0.0.2에** 대한 암호화 ACL(Access Control List)과 일치하는 패킷을 수신하고 SA 생성을 시작합니다.

```
IKEv2-PLAT-3: attempting to find tunnel
   group for IP: 10.0.0.2
```

```
IKEv2-PLAT-3: mapped to tunnel group 10.0.0.2
   using peer IP
IKEv2-PLAT-3: my_auth_method = 2
IKEv2-PLAT-3: supported_peers_auth_method = 2
IKEv2-PLAT-3: P1 ID = 0
IKEv2-PLAT-3: Translating IKE_ID_AUTO to = 255
IKEv2-PLAT-3: (16) tp_name set to:
IKEv2-PLAT-3: (16) tg_name set to: 10.0.0.2
IKEv2-PLAT-3: (16) tunn grp type set to: L2L
IKEv2-PLAT-5: New ikev2 sa request admitted
IKEv2-PLAT-5: Incrementing outgoing negotiating
  sa count by one
```

전송되는 메시지의 초기 쌍은 IKE_SA_INIT 교환용입니다. 이러한 메시지는 암호화 알고리즘을 협상하고 논스를 교환하며 DH(Diffie-Hellman) 교환을 수행합니다.

ASA1과 관련된 컨피그레이션은 다음과 같습니다.

```
crypto ikev2
   policy 1
encryption
aes-256
integrity sha
group 2
prf sha
lifetime seconds
  86400
crypto ikev2
  enable
  outside

Tunnel Group
matching the
identity name
s present:

tunnel-group
   10.0.0.2
   type ipsec-l2l
tunnel-group
   10.0.0.2
   ipsec-attributes
ikev2
   remote-
   authentication
   pre-shared-key
   *****
ikev2
   local-
   authentication
   pre-shared-key
  *****
```

이 Exchange에 대한 디버그 출력은 다음과 같습니다.

```
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I)
   MsgID = 00000000 CurState: IDLE Event: EV_INIT_SA
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I)
   MsgID = 00000000 CurState: I_BLD_INIT
   Event: EV_GET_IKE_POLICY
```

```
IKEv2-PROTO-3: (16): Getting configured policies
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000
   (I) MsgID = 00000000 CurState: I_BLD_INIT
   Event: EV_SET_POLICY
IKEv2-PROTO-3: (16): Setting configured policies
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I)
   MsgID = 00000000 CurState: I_BLD_INIT
   Event: EV_CHK_AUTH4PKI
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I)
   MsgID = 00000000 CurState: I_BLD_INIT
   Event: EV_GEN_DH_KEY
IKEv2-PROTO-3: (16): Computing DH public key
IKEv2-PROTO-3: (16):
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I)
   MsgID = 00000000 CurState: I_BLD_INIT
   Event: EV_NO_EVENT
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I)
   MsgID = 00000000 CurState: I_BLD_INIT
   Event: EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5: (16): Action: Action_Null
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I)
   MsgID = 00000000 CurState: I_BLD_INIT
   Event: EV_GET_CONFIG_MODE
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
```

그런 다음 ASA1은 다음을 포함하는 IKE_INIT_SA 패킷을 작성합니다.

- **ISAKMP 헤더**(SPI/버전/플래그)
- **SAi1**(IKE 개시자가 지원하는 암호화 알고리즘)
- **KEi**(개시자의 DH 공개 키 값)
- **N**(초기자 Nonce)

```
R_SPI=0000000000000000 (I) MsgID = 00000000
   CurState: I_BLD_INIT Event: EV_BLD_MSG
IKEv2-PROTO-2: (16): Sending initial message
IKEv2-PROTO-3: Tx [L 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0]
   m_id: 0x0
IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 -
   r: 0000000000000000]
IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 -
   rspi: 0000000000000000
IKEv2-PROTO-4: Next payload: SA, version: 2.0
IKEv2-PROTO-4: Exchange type: IKE_SA_INIT,
   flags: INITIATOR
IKEv2-PROTO-4: Message id: 0x0, length: 338
SA  Next payload: KE, reserved: 0x0,
   length: 48
IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0,
   length: 44  Proposal: 1, Protocol id: IKE,
   SPI size: 0, #trans: 4
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
```

```
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 2, reserved: 0x0, id: SHA1
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4:     last transform: 0x0, reserved: 0x0:
   length: 8 type: 4, reserved: 0x0,
   id: DH_GROUP_1024_MODP/Group 2
KE  Next payload: N, reserved: 0x0,
   length: 136
    DH group: 2, Reserved: 0x0
      19 65 43 45 d2 72 a7 11 b8 a4 93 3f 44 95 6c b8
     6d 5a f0 f8 1f f3 d4 b9 ff 41 7b 0d 13 90 82 cf
     34 2e 74 e3 03 6e 9e 00 88 80 5d 86 2c 4c 79 35
     ee e6 98 91 89 f3 48 83 75 09 02 f1 3c b1 7f f5
     be 05 f1 fa 7e 8a 4c 43 eb a9 2c 3a 47 c0 68 40
     f5 dd 02 9d a5 b5 a2 a6 90 64 95 fc 57 b5 69 e8
     b2 4f 8e f2 a5 05 e3 c7 17 f9 c0 e0 c8 3e 91 ed
     c1 09 23 3e e5 09 4f be 1a 6a d4 d9 fb 65 44 1d
N  Next payload: VID, reserved: 0x0,
   length: 24
     84 8b 80 c2 52 6c 4f c7 f8 08 b8 ed! 52 af a2 f4
     d5 dd d4 f4
VID  Next payload: VID, reserved: 0x0,
   length: 23

     43 49 53 43 4f 2d 44 45 4c 45 54 45 2d 52 45 41
     53 4f 4e
VID  Next payload: VID, reserved: 0x0, length: 59

     43 49 53 43 4f 28 43 4f 50 59 52 49 47 48 54 29
     26 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 32
     30 30 39 20 43 69 73 63 6f 20 53 79 73 74 65 6d
     73 2c 20 49 6e 63 2e
VID  Next payload: NONE, reserved: 0x0, length: 20
    40 48 b7 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
```

그런 다음 ASA1에서 IKE_INIT_SA 패킷을 전송합니다.

```
IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT]
   [10.0.0.1]:500->[10.0.0.2]:500
```

ASA2는 IKEV_INIT_SA 패킷을 수신합니다.

```
IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT]
   [10.0.0.1]:500->[10.0.0.2]:500
   InitSPI=0xdfa3b583a4369958 RespSPI=0x0000000000000000
   MID=00000000
```

ASA2는 해당 피어에 대한 SA 생성을 시작합니다.

```
IKEv2-PROTO-3: Rx [L 10.0.0.2:500/R
   10.0.0.1:500/VRF i0:f0] m_id: 0x0
IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 -
   r: 0000000000000000]
IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 -
   rspi: 0000000000000000
IKEv2-PROTO-4: Next payload: SA, version: 2.0
IKEv2-PROTO-4: Exchange type: IKE_SA_INIT,
   flags: INITIATOR
IKEv2-PROTO-4: Message id: 0x0, length: 338
IKEv2-PLAT-5: New ikev2 sa request admitted
```

```
IKEv2-PLAT-5: Incrementing incoming negotiating
   sa count by one
SA  Next payload: KE, reserved: 0x0, length: 48
IKEv2-PROTO-4:   last proposal: 0x0, reserved: 0x0,
   length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0,
   #trans: 4
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 2, reserved: 0x0, id: SHA1
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4:     last transform: 0x0, reserved: 0x0:
   length: 8 type: 4, reserved: 0x0,
   id: DH_GROUP_1024_MODP/Group 2
KE  Next payload: N, reserved: 0x0, length: 136
    DH group: 2, Reserved: 0x0
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: IDLE
   Event: EV_RECV_INIT
IKEv2-PROTO-5: (16): SM Trace->
  SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
```

ASA2는 IKE_INIT 메시지를 확인하고 처리합니다.

1. ASA1에서 제공하는 암호화 제품군을 선택합니다.

2. 자체 DH 비밀 키를 계산합니다.

3. 또한 이 IKE_SA에 대해 모든 키가 파생될 수 있는 SKEYID 값을 계산합니다. 다음에 오는 모든 메시지의 헤더를 제외한 모든 헤더가 암호화되고 인증됩니다. 암호화 및 무결성 보호에 사용되는 키는 SKEYID에서 파생되며 다음과 같습니다.

   SK_e는 암호화에 사용됩니다.

   SK_a는 인증에 사용됩니다.

   SK_d가 파생되어 CHILD_SAs에 대한 추가 키 재료 파생에 사용됩니다. 각 방향에 대해 별도의 SK_e와 SK_a가 산출된다.

ASA2와 관련된 컨피그레이션은 다음과 같습니다.

```
crypto ikev2
   policy 1
encryption
   aes-256
integrity sha
group 2
prf sha
lifetime seconds
   86400
crypto ikev2
   enable
   outside

Tunnel Group
matching the
identity name
```

is present:

```
tunnel-group
   10.0.0.1
   type ipsec-l2l
tunnel-group
   10.0.0.1
   ipsec-
   attributes
ikev2 remote-
   authentication
   pre-shared-key
   *****
ikev2 local-
   authentication
   pre-shared-key
  *****
```

디버그 출력은 다음과 같습니다.

```
MsgID = 00000000 CurState: R_INIT Event: EV_VERIFY_MSG
IKEv2-PROTO-3: (16): Verify SA init message
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_INIT Event: EV_INSERT_SA
IKEv2-PROTO-3: (16): Insert SA
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_INIT
   Event: EV_GET_IKE_POLICY
IKEv2-PROTO-3: (16): Getting configured policies
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_INIT Event:EV_PROC_MSG
IKEv2-PROTO-2: (16): Processing initial message
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_INIT
   Event: EV_DETECT_NAT
IKEv2-PROTO-3: (16): Process NAT discovery notify
IKEv2-PROTO-5: (16): No NAT found
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_INIT
   Event: EV_CHK_CONFIG_MODE
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_SET_POLICY
IKEv2-PROTO-3: (16): Setting configured policies
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_CHK_AUTH4PKI
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_PKI_SESH_OPEN
IKEv2-PROTO-3: (16): Opening a PKI session
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_GEN_DH_KEY
```

```
IKEv2-PROTO-3: (16): Computing DH public key
IKEv2-PROTO-3: (16):
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_NO_EVENT
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5: (16): Action: Action_Null
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_GEN_DH_SECRET
IKEv2-PROTO-3: (16): Computing DH secret key
IKEv2-PROTO-3: (16):
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_NO_EVENT
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5: (16): Action: Action_Null
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_GEN_SKEYID
IKEv2-PROTO-3: (16): Generate skeyid
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000 CurState: R_BLD_INIT
   Event: EV_GET_CONFIG_MODE
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R) MsgID = 00000000
  CurState: R_BLD_INIT Event: EV_BLD_MSG
```

그런 다음 ASA2는 ASA1에서 수신하는 IKE_SA_INIT 교환에 대한 responder 메시지를 작성합니다. 이 패킷에는 다음이 포함됩니다.

- **ISAKMP 헤더**(SPI/버전/플래그)
- **SAr1**(IKE 응답자가 선택하는 암호화 알고리즘)
- **KEr**(responder의 DH 공개 키 값)
- **응답자 논스**

디버그 출력은 다음과 같습니다.

```
IKEv2-PROTO-2: (16): Sending initial message
IKEv2-PROTO-3:   IKE Proposal: 1, SPI size: 0
   (initial negotiation),
Num. transforms: 4
AES-CBC SHA1 SHA96 DH_GROUP_1024_MODP/Group 2

IKEv2-PROTO-5: Construct Vendor Specific Payload:
   FRAGMENTATIONIKEv2-PROTO-3:
   Tx [L 10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0] m_id: 0x0
```

```
IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665]
IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 -
   rspi: 27C943C13FD94665
IKEv2-PROTO-4: Next payload: SA, version: 2.0
IKEv2-PROTO-4: Exchange type: IKE_SA_INIT,
   flags: RESPONDER MSG-RESPONSE
IKEv2-PROTO-4: Message id: 0x0, length: 338
SA  Next payload: KE, reserved: 0x0, length: 48
IKEv2-PROTO-4:   last proposal: 0x0, reserved: 0x0,
   length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0,
   #trans: 4
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 2, reserved: 0x0, id: SHA1
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4:     last transform: 0x0, reserved: 0x0:
   length: 8 type: 4, reserved: 0x0,
   id: DH_GROUP_1024_MODP/Group 2

KE  Next payload: N, reserved: 0x0, length: 136

DH group: 2, Reserved: 0x0
```

ASA2는 responder 메시지를 ASA1에 전송합니다.

```
IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT]
   [10.0.0.2]:500->[10.0.0.1]:500 InitSPI=0xdfa3b583a4369958
  RespSPI=0x27c943c13fd94665 MID=00000000
```

ASA1은 ASA2로부터 IKE_SA_INIT 응답 패킷을 수신합니다.

```
IKEv2-PLAT-4: RECV PKT
   [IKE_SA_INIT]
   [10.0.0.2]:500->
   [10.0.0.1]:500
   InitSPI=0xdfa3b583a4369958
   RespSPI=0x27c943c13fd94665
  MID=00000000
```

ASA2가 권한 부여 프로세스에 대한 타이머를 시작합니다.

```
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000
   CurState: INIT_DONE
   Event: EV_DONE
IKEv2-PROTO-3: (16):
   Fragmentation is
   enabled
IKEv2-PROTO-3: (16): Cisco
   DeleteReason Notify
   is enabled
IKEv2-PROTO-3: (16): Complete
   SA init exchange
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000
   CurState: INIT_DONE
   Event: EV_CHK4_ROLE
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000

CurState: INIT_DONE Event:
   EV_START_TMR
IKEv2-PROTO-3: (16): Starting
   timer to wait for auth
   message (30 sec)
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000000
   CurState: R_WAIT_AUTH
  Event: EV_NO_EVENT
```

ASA1은 응답을 확인하고 처리합니다.

1. 개시자 DH 비밀 키가 계산됩니다.

2. 개시자 SKEYID가 생성됩니다.

디버그 출력은 다음과 같습니다.

```
IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0]
   m_id: 0x0
IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665]
IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 -
   rspi: 27C943C13FD94665
IKEv2-PROTO-4: Next payload: SA, version: 2.0
IKEv2-PROTO-4: Exchange type: IKE_SA_INIT,
   flags: RESPONDER MSG-RESPONSE
IKEv2-PROTO-4: Message id: 0x0, length: 338

SA  Next payload: KE, reserved: 0x0, length: 48
IKEv2-PROTO-4:   last proposal: 0x0, reserved: 0x0,
   length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0,
   #trans: 4
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 2, reserved: 0x0, id: SHA1
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4:     last transform: 0x0, reserved: 0x0:
   length: 8 type: 4, reserved: 0x0,
   id: DH_GROUP_1024_MODP/Group 2
KE  Next payload: N, reserved: 0x0, length: 136
    DH group: 2, Reserved: 0x0

IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_WAIT_INIT
   Event: EV_RECV_INIT
IKEv2-PROTO-5: (16): Processing initial message
```

```
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_PROC_INIT
   Event: EV_CHK4_NOTIFY
IKEv2-PROTO-2: (16): Processing initial message
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_PROC_INIT
   Event: EV_VERIFY_MSG
IKEv2-PROTO-3: (16): Verify SA init message
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_PROC_INIT
   Event: EV_PROC_MSG
IKEv2-PROTO-2: (16): Processing initial message
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_PROC_INIT
   Event: EV_DETECT_NAT
IKEv2-PROTO-3: (16): Process NAT discovery notify
IKEv2-PROTO-3: (16): NAT-T is disabled
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_PROC_INIT
   Event: EV_CHK_NAT_T
IKEv2-PROTO-3: (16): Check NAT discovery
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_PROC_INIT
   Event: EV_CHK_CONFIG_MODE
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000000
   CurState: INIT_DONE Event: EV_GEN_DH_SECRET
IKEv2-PROTO-3: (16): Computing DH secret key
IKEv2-PROTO-3: (16):
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000000
   CurState: INIT_DONE Event: EV_NO_EVENT
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000000
   CurState: INIT_DONE Event: EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5: (16): Action: Action_Null
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000000
   CurState: INIT_DONE Event: EV_GEN_SKEYID
IKEv2-PROTO-3: (16): Generate skeyid
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: INIT_DONE Event: EV_DONE
IKEv2-PROTO-3: (16): Fragmentation is enabled
IKEv2-PROTO-3: (16): Cisco DeleteReason Notify is enabled
```

ASA 간의 IKE_INIT_SA 교환이 완료되었습니다.

```
IKEv2-PROTO-3: (16): Complete SA init exchange
```

ASA1은 IKE_AUTH 교환을 시작하고 인증 페이로드를 생성하기 시작합니다. IKE_AUTH 패킷에는 다음이 포함됩니다.

- **ISAKMP 헤더**(SPI/버전/플래그)
- **IDi**(개시자 ID)
- **인증 페이로드**
- **SAi2**(IKEv1의 2단계 변환 세트 교환과 유사한 SA를 시작)
- **TSi 및 TSr**(initiator 및 responder 트래픽 선택기)

  참고: TSi 및 TSr에는 각각 암호화된 트래픽을 전달/수신하기 위한 initiator 및 responder의 소스 및 목적지 주소가 포함되어 있습니다. 주소 범위는 해당 범위를 오가는 모든 트래픽이 터널링되도록 지정합니다. 제안이 응답자에게 허용 가능한 경우 동일한 TS 페이로드를 반환합니다.

또한 첫 번째 CHILD_SA는 트리거 패킷과 일치하는 proxy_ID 쌍에 대해 생성됩니다.

ASA1과 관련된 컨피그레이션은 다음과 같습니다.

```
crypto ipsec
   ikev2
   ipsec-proposal
   AES256
protocol esp
   encryption
   aes-256
protocol esp
   integrity
   sha-1 md5

access-list
   l2l_list
   extended
   permit ip
   host 10.0.0.2
  host 10.0.0.1
```

디버그 출력은 다음과 같습니다.

```
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_GEN_AUTH
IKEv2-PROTO-3: (16): Generate my authentication data
IKEv2-PROTO-3: (16): Use preshared key for id 10.0.0.1,
   key len 5
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_BLD_AUTH
   Event: EV_CHK_AUTH_TYPE
IKEv2-PROTO-3: (16): Get my authentication method
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_BLD_AUTH
   Event: EV_OK_AUTH_GEN
IKEv2-PROTO-3: (16): Check for EAP exchange
IKEv2-PROTO-5: (16): SM Trace->
```

```
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I)
   MsgID = 00000000 CurState: I_BLD_AUTH
   Event: EV_SEND_AUTH
IKEv2-PROTO-2: (16): Sending auth message
IKEv2-PROTO-5: Construct Vendor Specific Payload:
   CISCO-GRANITE
IKEv2-PROTO-3:   ESP Proposal: 1, SPI size: 4
   (IPSec negotiation),
Num. transforms: 4
   AES-CBC   SHA96   MD596
IKEv2-PROTO-5: Construct Notify Payload: INITIAL_CONTACT
IKEv2-PROTO-5: Construct Notify Payload: ESP_TFC_NO_SUPPORT
IKEv2-PROTO-5: Construct Notify Payload: NON_FIRST_FRAGS
IKEv2-PROTO-3: (16): Building packet for encryption;
   contents are:
VID  Next payload: IDi, reserved: 0x0, length: 20

     dd a3 b4 83 b7 01 6a 1f 3d b7 84 1a 75 e6 83 a6
IDi  Next payload: AUTH, reserved: 0x0, length: 12
    Id type: IPv4 address, Reserved: 0x0 0x0

     47 01 01 01
AUTH  Next payload: SA, reserved: 0x0, length: 28
    Auth method PSK, reserved: 0x0, reserved 0x0
Auth data&colon; 20 bytes
SA  Next payload: TSi, reserved: 0x0, length: 52
IKEv2-PROTO-4:   last proposal: 0x0, reserved: 0x0,
   length: 48 Proposal: 1, Protocol id: ESP, SPI size: 4,
   #trans: 4
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: MD596
IKEv2-PROTO-4:     last transform: 0x0, reserved: 0x0:
   length: 8 type: 5, reserved: 0x0, id:

  TSi  Next payload: TSr, reserved: 0x0, length: 24
    Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.1.1, end addr: 192.168.1.1
TSr  Next payload: NOTIFY, reserved: 0x0, length: 24
    Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.2.99, end addr: 192.168.2.99
IKEv2-PROTO-3: Tx [L 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0]
   m_id: 0x1
IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665]
IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 -
   rspi: 27C943C13FD94665

IKEv2-PROTO-4: Next payload: ENCR, version: 2.0
IKEv2-PROTO-4: Exchange type: IKE_AUTH, flags: INITIATOR
IKEv2-PROTO-4: Message id: 0x1, length: 284
ENCR  Next payload: VID, reserved: 0x0, length: 256
Encrypted data&colon; 252 bytes
```

ASA1은 IKE_AUTH 패킷을 ASA2에 전송합니다.

```
IKEv2-PLAT-4: SENT PKT [IKE_AUTH]
```

```
   [10.0.0.1]:500->[10.0.0.2]:500
   InitSPI=0xdfa3b583a4369958 RespSPI=0x27c943c13fd94665
  MID=00000001
```

ASA2는 ASA1에서 이 패킷을 수신합니다.

```
IKEv2-PLAT-4: RECV PKT [IKE_AUTH]
   [10.0.0.1]:500->[10.0.0.2]:500
   InitSPI=0xdfa3b583a4369958 RespSPI=0x27c943c13fd94665
  MID=00000001
```

ASA2는 권한 부여 타이머를 중지하고 ASA1에서 받은 인증 데이터를 확인합니다. 그런 다음 ASA1과 정확히 같은 자체 인증 데이터를 생성합니다.

ASA2와 관련된 컨피그레이션은 다음과 같습니다.

```
crypto ipsec
   ikev2
   ipsec-
   proposal
   AES256
protocol esp
   encryption
   aes-256
protocol esp
   integrity
  sha-1 md5
```

디버그 출력은 다음과 같습니다.

```
IKEv2-PROTO-3: Rx [L 10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0]
   m_id: 0x1
IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665]
IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 -
   rspi: 27C943C13FD94665
IKEv2-PROTO-4: Next payload: ENCR, version: 2.0
IKEv2-PROTO-4: Exchange type: IKE_AUTH, flags: INITIATOR
IKEv2-PROTO-4: Message id: 0x1, length: 284
IKEv2-PROTO-5: (16): Request has mess_id 1;
   expected 1 through 1 REAL Decrypted packet:
   Data&colon; 216 bytes
IKEv2-PROTO-5: Parse Vendor Specific Payload: (CUSTOM) VID
   Next payload: IDi, reserved: 0x0, length: 20

     dd a3 b4 83 b7 01 6a 1f 3d b7 84 1a 75 e6 83 a6
IDi  Next payload: AUTH, reserved: 0x0, length: 12
    Id type: IPv4 address, Reserved: 0x0 0x0

     47 01 01 01
AUTH  Next payload: SA, reserved: 0x0, length: 28
    Auth method PSK, reserved: 0x0, reserved 0x0
Auth data&colon; 20 bytes
SA  Next payload: TSi, reserved: 0x0, length: 52
IKEv2-PROTO-4:   last proposal: 0x0, reserved: 0x0,
   length: 48 Proposal: 1, Protocol id: ESP, SPI size: 4,
   #trans: 4
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: MD596
IKEv2-PROTO-4:     last transform: 0x0, reserved: 0x0:
   length: 8 type: 5, reserved: 0x0, id:
TSi  Next payload: TSr, reserved: 0x0, length: 24
    Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.1.1, end addr: 192.168.1.1
TSr  Next payload: NOTIFY, reserved: 0x0, length: 24
    Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.2.99, end addr: 192.168.2.99
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R) MsgID = 00000001
   CurState: R_WAIT_AUTH Event: EV_RECV_AUTH
IKEv2-PROTO-3: (16): Stopping timer to wait for auth
   message
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R) MsgID = 00000001
   CurState: R_WAIT_AUTH Event: EV_CHK_NAT_T
IKEv2-PROTO-3: (16): Check NAT discovery
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R) MsgID = 00000001
   CurState: R_WAIT_AUTH Event: EV_PROC_ID
IKEv2-PROTO-2: (16): Recieved valid parameteres in
   process id
IKEv2-PLAT-3: (16) peer auth method set to: 2
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R) MsgID = 00000001
   CurState: R_WAIT_AUTH
   Event: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_
   PROF_SEL
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R) MsgID = 00000001
   CurState: R_WAIT_AUTH Event: EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3: (16): Getting configured policies
IKEv2-PLAT-3: attempting to find tunnel group for
   ID: 10.0.0.1
IKEv2-PLAT-3: mapped to tunnel group 10.0.0.1 using
   phase 1 ID
IKEv2-PLAT-3: (16) tg_name set to: 10.0.0.1
IKEv2-PLAT-3: (16) tunn grp type set to: L2L
IKEv2-PLAT-3: my_auth_method = 2
IKEv2-PLAT-3: supported_peers_auth_method = 2
IKEv2-PLAT-3: P1 ID = 0
IKEv2-PLAT-3: Translating IKE_ID_AUTO to = 255

IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_WAIT_AUTH
   Event: EV_SET_POLICY
IKEv2-PROTO-3: (16): Setting configured policies
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_WAIT_AUTH
   Event: EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3: (16): Verify peer's policy
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001
   CurState: R_WAIT_AUTH Event: EV_CHK_CONFIG_MODE
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_WAIT_AUTH
   Event: EV_CHK_AUTH4EAP
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_WAIT_AUTH
   Event: EV_CHK_POLREQEAP
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_CHK_AUTH_TYPE
IKEv2-PROTO-3: (16): Get peer authentication method
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_GET_PRESHR_KEY
IKEv2-PROTO-3: (16): Get peer's preshared key for 10.0.0.1
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_VERIFY_AUTH

IKEv2-PROTO-3: (16): Verify authentication data
IKEv2-PROTO-3: (16): Use preshared key for id 10.0.0.1,
   key len 5
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_GET_CONFIG_MODE
IKEv2-PLAT-2: Build config mode reply: no request stored
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_CHK4_IC
IKEv2-PROTO-3: (16): Processing initial contact
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_CHK_REDIRECT
IKEv2-PROTO-5: (16): Redirect check is not needed,
   skipping it
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_PROC_SA_TS
IKEv2-PROTO-2: (16): Processing auth message
IKEv2-PLAT-3: Selector received from peer is accepted
IKEv2-PLAT-3: PROXY MATCH on crypto map
   outside_map seq 1
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_NO_EVENT
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_VERIFY_AUTH
   Event: EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2: (16): Processing auth message
```

ASA2는 다음을 포함하는 IKE_AUTH 패킷을 전송합니다.

- **ISAKMP 헤더**(SPI/버전/플래그)
- **IDr**(응답자 ID)

- **인증 페이로드**
- **SAr2**(IKEv1의 2단계 변환 세트 교환과 유사한 SA를 시작)
- **TSi 및 TSr**(initiator 및 responder 트래픽 선택기)

  참고: TSi 및 TSr에는 각각 암호화된 트래픽을 전달/수신하기 위한 initiator 및 responder의 소스 및 목적지 주소가 포함되어 있습니다. 주소 범위는 해당 범위를 오가는 모든 트래픽이 터널링되도록 지정합니다. 이러한 매개변수는 ASA1에서 수신한 매개변수와 동일합니다.

디버그 출력은 다음과 같습니다.

```
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_BLD_AUTH
   Event: EV_MY_AUTH_METHOD
IKEv2-PROTO-3: (16): Get my authentication method
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_BLD_AUTH
   Event: EV_GET_PRESHR_KEY
IKEv2-PROTO-3: (16): Get peer's preshared key for 10.0.0.1
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_BLD_AUTH
   Event: EV_GEN_AUTH
IKEv2-PROTO-3: (16): Generate my authentication data
IKEv2-PROTO-3: (16): Use preshared key for id 10.0.0.2,
   key len 5
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_BLD_AUTH
   Event: EV_CHK4_SIGN
IKEv2-PROTO-3: (16): Get my authentication method
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_BLD_AUTH
   Event: EV_OK_AUTH_GEN
IKEv2-PROTO-5: (16): SM Trace->
   SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001 CurState: R_BLD_AUTH
   Event: EV_SEND_AUTH
IKEv2-PROTO-2: (16): Sending auth message
IKEv2-PROTO-5: Construct Vendor Specific Payload:
   CISCO-GRANITE
IKEv2-PROTO-3:   ESP Proposal: 1, SPI size: 4 (IPSec
   negotiation),
Num. transforms: 3
   AES-CBC   SHA96
IKEv2-PROTO-5: Construct Notify Payload:
   ESP_TFC_NO_SUPPORTIKEv2-PROTO-5:
   Construct Notify Payload: NON_FIRST_FRAGSIKEv2-PROTO-3:
     (16):
Building packet for encryption; contents are:
VID  Next payload: IDr, reserved: 0x0, length: 20
     25 c9 42 c1 2c ee b5 22 3d b7 84 1a 75 e6 83 a6
IDr  Next payload: AUTH, reserved: 0x0,
   length: 12 Id type: IPv4 address, Reserved: 0x0 0x0
```

```
     51 01 01 01
AUTH  Next payload: SA, reserved: 0x0,
   length: 28 Auth method PSK, reserved: 0x0, reserved 0x0
Auth data&colon; 20 bytes
SA  Next payload: TSi, reserved: 0x0,
   length: 44 IKEv2-PROTO-4:   last proposal: 0x0,
   reserved: 0x0, length: 40
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4:     last transform: 0x0, reserved: 0x0:
   length: 8 type: 5, reserved: 0x0, id:

TSi  Next payload: TSr, reserved: 0x0,
   length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.1.1, end addr: 192.168.1.1
TSr  Next payload: NOTIFY, reserved: 0x0,
   length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.2.99, end addr: 192.168.2.99
NOTIFY(ESP_TFC_NO_SUPPORT)  Next payload: NOTIFY,
   reserved: 0x0, length: 8 Security protocol id: IKE,
   spi size: 0, type: ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS)  Next payload: NONE, reserved: 0x0,
   length: 8 Security protocol id: IKE, spi size: 0,
   type: NON_FIRST_FRAGS
IKEv2-PROTO-3: Tx [L 10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0]
   m_id: 0x1
IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665]
IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 -
   rspi: 27C943C13FD94665
IKEv2-PROTO-4: Next payload: ENCR, version: 2.0
IKEv2-PROTO-4: Exchange type: IKE_AUTH, flags:
   RESPONDER MSG-RESPONSE
IKEv2-PROTO-4: Message id: 0x1, length: 236
ENCR  Next payload: VID, reserved: 0x0, length: 208
Encrypted data&colon; 204 bytes
```

ASA2는 IKE_AUTH 패킷에 대한 응답을 전송합니다.

```
IKEv2-PLAT-4: SENT PKT [IKE_AUTH]
   [10.0.0.2]:500->[10.0.0.1]:500
   InitSPI=0xdfa3b583a4369958 RespSPI=0x27c943c13fd94665
  MID=00000001
```

ASA1이 ASA2로부터 응답을 수신합니다.

```
IKEv2-PLAT-4:
   RECV PKT [IKE_AUTH]
   [10.0.0.2]:500->
   [10.0.0.1]:500
   InitSPI=0xdfa3b583a4369958
   RespSPI=0x27c943c13fd94665
  MID=00000001
```

ASA2는 SA 데이터베이스(SAD)에 항목을 삽입합니다.

```
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001
   CurState: AUTH_DONE
   Event: EV_OK
IKEv2-PROTO-5: (16): Action:
   Action_Null
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001
   CurState: AUTH_DONE
   Event: EV_PKI_SESH_CLOSE
IKEv2-PROTO-3: (16): Closing
   the PKI session
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001
   CurState: AUTH_DONE
   Event: EV_INSERT_IKE
IKEv2-PROTO-2: (16):
   SA created;
   inserting SA into database
```

ASA1은 이 패킷의 인증 데이터를 확인 및 처리한 다음 이 SA를 SAD에 삽입합니다.

```
IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0]
   m_id: 0x1
IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665]
IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 -
   rspi: 27C943C13FD94665
IKEv2-PROTO-4: Next payload: ENCR, version: 2.0
IKEv2-PROTO-4: Exchange type: IKE_AUTH,
   flags: RESPONDER MSG-RESPONSE
IKEv2-PROTO-4: Message id: 0x1, length: 236
REAL Decrypted packet:Data&colon; 168 bytes
IKEv2-PROTO-5: Parse Vendor Specific Payload: (CUSTOM) VID
   Next payload: IDr, reserved: 0x0, length: 20

     25 c9 42 c1 2c ee b5 22 3d b7 84 1a 75 e6 83 a6
IDr  Next payload: AUTH, reserved: 0x0, length: 12
    Id type: IPv4 address, Reserved: 0x0 0x0

     51 01 01 01
AUTH  Next payload: SA, reserved: 0x0, length: 28
    Auth method PSK, reserved: 0x0, reserved 0x0
Auth data&colon; 20 bytes
SA  Next payload: TSi, reserved: 0x0, length: 44
IKEv2-PROTO-4:   last proposal: 0x0, reserved: 0x0,
   length: 40 Proposal: 1, Protocol id: ESP, SPI size: 4,
   #trans: 3
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4:     last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4:     last transform: 0x0, reserved: 0x0:
   length: 8 type: 5, reserved: 0x0, id:
```

```
   TSi  Next payload: TSr, reserved: 0x0,
   length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.1.1, end addr: 192.168.1.1
TSr  Next payload: NOTIFY, reserved: 0x0,
   length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0
    TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
    start port: 0, end port: 65535
    start addr: 192.168.2.99, end addr: 192.168.2.99
IKEv2-PROTO-5: Parse Notify Payload:
   ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT)
   Next payload: NOTIFY, reserved: 0x0, length: 8
    Security protocol id: IKE, spi size: 0,
   type: ESP_TFC_NO_SUPPORT
IKEv2-PROTO-5: Parse Notify Payload:
   NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS)  Next payload:
   NONE, reserved: 0x0, length: 8
    Security protocol id: IKE, spi size: 0,
   type: NON_FIRST_FRAGS
Decrypted packet:Data&colon; 236 bytes
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_WAIT_AUTH Event: EV_RECV_AUTH
IKEv2-PROTO-5: (16): Action: Action_Null
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_CHK4_NOTIFY
IKEv2-PROTO-2: (16): Process auth response notify
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_PROC_MSG
IKEv2-PLAT-3: (16) peer auth method set to: 2
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH
   Event: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_
   FOR_PROF_SEL
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3: (16): Getting configured policies
IKEv2-PLAT-3: connection initiated with tunnel
   group 10.0.0.2
IKEv2-PLAT-3: (16) tg_name set to: 10.0.0.2
IKEv2-PLAT-3: (16) tunn grp type set to: L2L
IKEv2-PLAT-3: my_auth_method = 2
IKEv2-PLAT-3: supported_peers_auth_method = 2
IKEv2-PLAT-3: P1 ID = 0
IKEv2-PLAT-3: Translating IKE_ID_AUTO to = 255
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3: (16): Verify peer's policy
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_CHK_AUTH_TYPE
IKEv2-PROTO-3: (16): Get peer authentication method
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_GET_PRESHR_KEY
IKEv2-PROTO-3: (16): Get peer's preshared key for 10.0.0.2
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
```

```
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_VERIFY_AUTH
IKEv2-PROTO-3: (16): Verify authentication data
IKEv2-PROTO-3: (16): Use preshared key for id 10.0.0.2,
   key len 5
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_CHK_EAP
IKEv2-PROTO-3: (16): Check for EAP exchange
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_CHK_CONFIG_MODE
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_CHK_IKE_ONLY
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: I_PROC_AUTH Event: EV_PROC_SA_TS
IKEv2-PROTO-2: (16): Processing auth message
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: AUTH_DONE Event: EV_OK
IKEv2-PROTO-5: (16): Action: Action_Null
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: AUTH_DONE Event: EV_PKI_SESH_CLOSE
IKEv2-PROTO-3: (16): Closing the PKI session
IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I) MsgID = 00000001
   CurState: AUTH_DONE Event: EV_INSERT_IKE
IKEv2-PROTO-2: (16): SA created; inserting SA into
   database
```

이제 터널이 ASA1에 대해 활성화됩니다.

```
CONNECTION
    STATUS: UP...
   peer: 10.0.0.2:500,
   phase1_id: 10.0.0.2
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I)
   MsgID = 00000001
   CurState: AUTH_DONE
  Event: EV_REGISTER_SESSION
```

이제 터널이 ASA2에 대해 활성화됩니다.

```
CONNECTION
   STATUS: UP...
   peer: 10.0.0.1:500,
   phase1_id: 10.0.0.1
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001
   CurState: AUTH_DONE
  Event: EV_REGISTER_SESSION
```

참고: responder 터널은 일반적으로 initiator 터널보다 먼저 활성화됩니다.

IKEv2 등록 프로세스는 ASA1에서 발생합니다.

```
IKEv2-PLAT-3: (16)
   connection
   auth hdl set to 15
IKEv2-PLAT-3: AAA conn
   attribute retrieval
   successfully queued
   for register session
   request.
IKEv2-PROTO-3: (16):
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (I)
   MsgID = 00000001
   CurState: AUTH_DONE
   Event: EV_NO_EVENT
IKEv2-PLAT-3: (16) idle
   timeout set to: 30
IKEv2-PLAT-3: (16) session
   timeout set to: 0
IKEv2-PLAT-3: (16) group
   policy set to
   DfltGrpPolicy
IKEv2-PLAT-3: (16) class
   attr set
IKEv2-PLAT-3: (16) tunnel
   protocol set to: 0x5c
IKEv2-PLAT-3: IPv4 filter
   ID not configured
   for connection
IKEv2-PLAT-3: (16) group
   lock set to: none
IKEv2-PLAT-3: IPv6 filter ID
   not configured
   for connection
IKEv2-PLAT-3: (16)
   connection attribues
   set valid to TRUE
IKEv2-PLAT-3: Successfully
   retrieved conn attrs
IKEv2-PLAT-3: Session
   registration after conn
   attr retrieval
   PASSED, No error
IKEv2-PLAT-3:
CONNECTION STATUS:
   REGISTERED...
   peer: 10.0.0.2:500,
  phase1_id: 10.0.0.2
```

IKEv2 등록 프로세스는 ASA2에서 발생합니다.

```
IKEv2-PLAT-3: (16)
   connection
   auth hdl set to 15
IKEv2-PLAT-3: AAA conn
   attribute retrieval
   successfully queued for
   register session request.
```

```
IKEv2-PROTO-3: (16):
IKEv2-PROTO-5: (16):
   SM Trace->
   SA: I_SPI=DFA3B583A4369958
   R_SPI=27C943C13FD94665 (R)
   MsgID = 00000001
   CurState: AUTH_DONE
   Event: EV_NO_EVENT
IKEv2-PLAT-3: (16) idle
   timeout
   set to: 30
IKEv2-PLAT-3: (16) session
   timeout
   set to: 0
IKEv2-PLAT-3: (16) group
   policy set to
   DfltGrpPolicy
IKEv2-PLAT-3: (16) class
   attr set
IKEv2-PLAT-3: (16) tunnel
   protocol set to: 0x5c
IKEv2-PLAT-3: IPv4 filter ID
   not configured
   for connection
IKEv2-PLAT-3: (16) group
   lock set to: none
IKEv2-PLAT-3: IPv6 filter ID
   not configured
   for connection
   attribues set
   valid to TRUE
IKEv2-PLAT-3: Successfully
   retrieved conn attrs
IKEv2-PLAT-3: Session
   registration after conn
   attr retrieval PASSED,
   No error
IKEv2-PLAT-3:
CONNECTION STATUS:
   REGISTERED...
   peer: 10.0.0.1:500,
  phase1_id: 10.0.0.1
```

하위 SA 디버그

> **참고**: 이 교환은 단일 요청 및 응답 쌍으로 구성되며 IKEv1에서 2단계 교환이라고 합니다. 초기 교환이 완료된 후 IKE_SA의 어느 한 쪽 끝에 시작할 수 있습니다.

ASA2는 CHILD_SA 교환을 시작합니다. CREATE_CHILD_SA 요청입니다. CHILD_SA 패킷에는 일반적으로 다음이 포함됩니다.

- **SA HDR** - version.flags 및 exchange 유형이 포함됩니다.
- **Nonce Ni**(선택 사항) - CHILD_SA가 초기 교환의 일부로 생성되는 경우 두 번째 KE(Key Exchange) 페이로드와 nonce를 보내지 않아야 합니다.
- **SA 페이로드**

- **KEi**(키-선택 사항) - CREATE_CHILD_SA 요청에는 CHILD_SA에 대한 전달 비밀성을 보다 강력하게 보장하기 위해 추가 DH 교환에 대한 KE 페이로드가 선택적으로 포함될 수 있습니다. SA에 다른 DH 그룹이 포함된 경우 KEi는 개시자가 응답자가 수락할 것으로 예상하는 그룹의 요소여야 합니다. 잘못 추측하면 CREATE_CHILD_SA 교환이 실패하고 다른 KEi로 다시 시도해야 합니다.

- **N**(Notify payload, 선택 사항) - Notify Payload는 오류 조건 및 상태 전환과 같은 정보 데이터를 IKE 피어로 전송하는 데 사용됩니다. Notify Payload(알림 페이로드)는 응답 메시지(일반적으로 요청이 거부되는 이유를 지정함), 정보 교환(IKE 요청이 아닌 오류를 보고하기 위해) 또는 다른 메시지에 나타나 발신자 기능을 나타내거나 요청의 의미를 수정할 수 있습니다. 이 CREATE_CHILD_SA 교환이 IKE_SA가 아닌 현재 SA의 키를 다시 설정하는 경우 REKEY_SA 유형의 리드 N 페이로드는 다시 입력된 SA를 식별해야 합니다. 이 CREATE_CHILD_SA 교환이 현재 SA를 리키하지 않으면 N 페이로드를 생략해야 합니다.

- **TSi 및 TSr**(선택 사항): SA가 생성된 트래픽 선택기를 표시합니다. 이 경우 호스트 192.168.1.12와 192.168.2.99 사이에 있습니다.

다음은 CREATE_CHILD_SA 디버그 출력입니다.

```
IKEv2-PLAT-5: INVALID PSH HANDLE
IKEv2-PLAT-3: attempting to find tunnel group
   for IP: 10.0.0.1
IKEv2-PLAT-3: mapped to tunnel group 10.0.0.1
   using peer IP
IKEv2-PLAT-3: my_auth_method = 2
IKEv2-PLAT-3: supported_peers_auth_method = 2
IKEv2-PLAT-3: P1 ID = 0
IKEv2-PLAT-3: Translating IKE_ID_AUTO to = 255
IKEv2-PLAT-3: (226) tp_name set to:
IKEv2-PLAT-3: (226) tg_name set to: 10.0.0.1
IKEv2-PLAT-3: (226) tunn grp type set to: L2L
IKEv2-PLAT-3: PSH cleanup
IKEv2-PROTO-5: (225): SM Trace-> SA:
   I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7
   (I) MsgID = 00000001 CurState: READY
   Event: EV_INIT_CREATE_CHILD
IKEv2-PROTO-5: (225): Action: Action_Null
IKEv2-PROTO-5: (225): SM Trace-> SA:
   I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7
   (I) MsgID = 00000001 CurState: CHILD_I_INIT
   Event: EV_INIT_CREATE_CHILD
IKEv2-PROTO-5: (225): Action: Action_Null
IKEv2-PROTO-5: (225): SM Trace-> SA:
   I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7
   (I) MsgID = 00000001 CurState: CHILD_I_IPSEC
   Event: EV_INIT_CREATE_CHILD
IKEv2-PROTO-3: (225): Check for IPSEC rekey
IKEv2-PROTO-5: (225): SM Trace-> SA:
   I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7
   (I) MsgID = 00000001 CurState: CHILD_I_IPSEC
   Event: EV_SET_IPSEC_DH_GRP
IKEv2-PROTO-3: (225): Set IPSEC DH group
IKEv2-PROTO-5: (225): SM Trace-> SA:
   I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7
   (I) MsgID = 00000001
   CurState: CHILD_I_IPSEC Event: EV_CHK4_PFS
IKEv2-PROTO-3: (225): Checking for PFS configuration
IKEv2-PROTO-5: (225): SM Trace-> SA:
   I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7
   (I) MsgID = 00000001 CurState: CHILD_I_IPSEC
   Event: EV_BLD_MSG
IKEv2-PROTO-2: (225): Sending child SA exchange
IKEv2-PROTO-3: ESP Proposal: 1, SPI size: 4
   (IPSec negotiation), num. transforms: 4
   AES-CBC SHA96 MD596
IKEv2-PROTO-3: (225): Building packet for encryption;
   contents are:
   SA Next payload: N, reserved: 0x0, length: 52
IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0,
   length: 48 Proposal: 1, Protocol id: ESP,
   SPI size: 4, #trans: 4
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
  length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: MD596
IKEv2-PROTO-4: last transform: 0x0, reserved: 0x0:
   length: 8 type: 5, reserved: 0x0, id:

N Next payload: TSi, reserved: 0x0, length: 24

2d 3e ec 11 e0 c7 5d 67 d5 23 25 76 1d 50 0d 05
fa b7 f0 48
TSi Next payload: TSr, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 192.168.2.99, end addr: 192.168.2.99
TSr Next payload: NONE, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 192.168.1.12, end addr: 192.168.1.12

IKEv2-PROTO-3: (225): Checking if request will fit in
   peer window
IKEv2-PROTO-3: Tx [L 10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0]
   m_id: 0x6
IKEv2-PROTO-3: HDR[i:FD366326E1FED6FE -
   r: A75B9B2582AAECB7]
IKEv2-PROTO-4: IKEV2 HDR ispi: FD366326E1FED6FE -
   rspi: A75B9B2582AAECB7
IKEv2-PROTO-4: Next payload: ENCR, version: 2.0
IKEv2-PROTO-4: Exchange type: CREATE_CHILD_SA,
   flags: INITIATOR
IKEv2-PROTO-4: Message id: 0x6, length: 180
ENCR Next payload: SA, reserved: 0x0, length: 152
Encrypted data&colon; 148 bytes
```

ASA2는 이 패킷을 전송하고 응답을 기다립니다.

```
IKEv2-PLAT-4: SENT PKT
   [CREATE_CHILD_SA]
   [10.0.0.2]:500->
   [10.0.0.1]:500
   InitSPI=0xfd366326e1fed6fe
   RespSPI=0xa75b9b2582aaecb7
   MID=00000006

IKEv2-PROTO-5: (225):
   SM Trace->
   SA: I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (I)
   MsgID = 00000006
   CurState: CHILD_I_WAIT
  Event: EV_NO_EVENT
```

ASA1이 패킷을 수신합니다.

```
IKEv2-PLAT-4:
   RECV PKT [CREATE_CHILD_SA]
   [10.0.0.2]:500->
   [10.0.0.1]:500
   InitSPI=0xfd366326e1fed6fe
   RespSPI=0xa75b9b2582aaecb7
   MID=00000006

IKEv2-PROTO-3: Rx
   [L 10.0.0.1:500/R
   10.0.0.2:500/VRF i0:f0]
  m_id: 0x6
```

그런 다음 ASA1은 ASA2에서 이 정확한 패킷을 수신하고 다음을 확인합니다.

```
IKEv2-PROTO-3: HDR[i:FD366326E1FED6FE -
   r: A75B9B2582AAECB7]
IKEv2-PROTO-4: IKEV2 HDR ispi: FD366326E1FED6FE -
   rspi: A75B9B2582AAECB7
IKEv2-PROTO-4: Next payload: ENCR, version: 2.0
IKEv2-PROTO-4: Exchange type: CREATE_CHILD_SA,
   flags: INITIATOR
IKEv2-PROTO-4: Message id: 0x6, length: 180
IKEv2-PROTO-5: (225): Request has mess_id 6;
   expected 6 through 6
   REAL Decrypted packet:Data&colon; 124 bytes
   SA Next payload: N, reserved: 0x0, length: 52
IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0,
   length: 48 Proposal: 1, Protocol id: ESP,
   SPI size: 4, #trans: 4
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 12 ype: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: MD596
IKEv2-PROTO-4: last transform: 0x0, reserved: 0x0:
   length: 8 type: 5, reserved: 0x0, id:

N Next payload: TSi, reserved: 0x0, length: 24

2d 3e ec 11 e0 c7 5d 67 d5 23 25 76 1d 50 0d 05
fa b7 f0 48
TSi Next payload: TSr, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 192.168.2.99, end addr: 192.168.2.99
TSr Next payload: NONE, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 192.168.1.12, end addr: 192.168.1.12
```

```
Decrypted packet:Data&colon; 180 bytes
IKEv2-PROTO-5: (225): SM Trace->
   SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R)
   MsgID = 00000006 CurState: READY
   Event: EV_RECV_CREATE_CHILD
IKEv2-PROTO-5: (225): Action: Action_Null
IKEv2-PROTO-5: (225): SM Trace->
   SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R)
   MsgID = 00000006 CurState: CHILD_R_INIT
   Event: EV_RECV_CREATE_CHILD
IKEv2-PROTO-5: (225): Action: Action_Null
IKEv2-PROTO-5: (225): SM Trace->
   SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R)
   MsgID = 00000006 CurState: CHILD_R_INIT
   Event: EV_VERIFY_MSG
IKEv2-PROTO-3: (225): Validating create child message
IKEv2-PROTO-5: (225): SM Trace->
   SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R)
   MsgID = 00000006 urState: CHILD_R_INIT
  Event: EV_CHK_CC_TYPE
```

이제 ASA1에서 CHILD_SA 교환에 대한 회신을 작성합니다. 이것은 **CREATE_CHILD_SA 응답입니다**. CHILD_SA 패킷에는 일반적으로 다음이 포함됩니다.

- **SA HDR** - version.flags 및 exchange 유형이 포함됩니다.

- **Nonce Ni**(선택 사항) - CHILD_SA가 초기 교환의 일부로 생성되는 경우 두 번째 KE 페이로드와 nonce를 보내지 않아야 합니다.

- **SA 페이로드**

- **KEi**(키, 선택 사항) - CREATE_CHILD_SA 요청은 CHILD_SA에 대한 전달 비밀성을 보다 강력하게 보장하기 위해 추가 DH 교환에 대한 KE 페이로드를 선택적으로 포함할 수 있습니다. SA에 다른 DH 그룹이 포함된 경우 KEi는 개시자가 응답자가 수락할 것으로 예상하는 그룹의 요소여야 합니다. 잘못 추측하면 CREATE_CHILD_SA 교환이 실패하며 다른 KEi로 다시 시도해야 합니다.

- **N**(Notify payload, 선택 사항) - Notify Payload는 오류 조건 및 상태 전환과 같은 정보 데이터를 IKE 피어로 전송하는 데 사용됩니다. Notify Payload(알림 페이로드)는 응답 메시지(일반적으로 요청이 거부되는 이유를 지정함), 정보 교환(IKE 요청에 없는 오류를 보고하기 위해) 또는 다른 메시지에 나타나 발신자 기능을 나타내거나 요청의 의미를 수정할 수 있습니다. 이 CREATE_CHILD_SA 교환이 IKE_SA가 아닌 현재 SA의 키를 다시 설정하는 경우 REKEY_SA 유형의 리드 N 페이로드는 다시 입력된 SA를 식별해야 합니다. 이 CREATE_CHILD_SA 교환이 현재 SA를 리키하지 않으면 N 페이로드를 생략해야 합니다.

- **TSi 및 TSr**(선택 사항) - SA가 생성된 트래픽 선택기를 표시합니다. 이 경우 호스트 192.168.1.12와 192.168.2.99 사이에 있습니다.

디버그 출력은 다음과 같습니다.

```
IKEv2-PROTO-3: (225): Check for create child
   response message type
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R)
   MsgID = 00000006 CurState: CHILD_R_IPSEC
   Event: EV_PROC_MSG
IKEv2-PROTO-2: (225): Processing child
   SA exchange
IKEv2-PLAT-3: Selector received from peer
   is accepted
IKEv2-PLAT-3: PROXY MATCH on crypto map
   outside_map seq 1
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006
   CurState: CHILD_R_IPSEC Event: EV_NO_EVENT
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000005
   CurState: EXIT Event: EV_FREE_NEG
IKEv2-PROTO-5: (225): Deleting negotiation context
   for peer message ID: 0x5
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006
   CurState: CHILD_R_IPSEC
   Event: EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-5: (225): Action: Action_Null
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006
   CurState: CHILD_R_IPSEC Event: EV_PROC_MSG
IKEv2-PROTO-2: (225): Processing child SA exchange
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R)
   MsgID = 00000006 CurState:
   CHILD_R_IPSEC Event: EV_SET_IPSEC_DH_GRP
IKEv2-PROTO-3: (225): Set IPSEC DH group
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006
   CurState: CHILD_R_IPSEC Event: EV_OK
IKEv2-PROTO-3: (225): Requesting SPI from IPSec
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006
   CurState: CHILD_R_WAIT_SPI Event: EV_OK_GOT_SPI
IKEv2-PROTO-5: (225): Action: Action_Null
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006
   CurState: CHILD_R_BLD_MSG Event: EV_CHK4_PFS
IKEv2-PROTO-3: (225): Checking for PFS configuration
IKEv2-PROTO-5: (225): SM Trace->
   SA:I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006
   CurState: CHILD_R_BLD_MSG Event: EV_BLD_MSG
IKEv2-PROTO-2: (225): Sending child SA exchange
IKEv2-PROTO-3: ESP Proposal: 1, SPI size: 4
  (IPSec negotiation),
Num. transforms: 3
AES-CBC SHA96
IKEv2-PROTO-3: (225): Building packet for encryption;
   contents are:
SA Next payload: N, reserved: 0x0, length: 44
IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0,
   length: 40
Proposal: 1, Protocol id: ESP, SPI size: 4,
   #trans: 3
```

```
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 12
type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 8
type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4: last transform: 0x0,
   reserved: 0x0: length: 8
type: 5, reserved: 0x0, id:

N Next payload: TSi, reserved: 0x0,
   length: 24

b7 6a c6 75 53 55 99 5a df ee 05
   18 1a 27 a6 cb
01 56 22 ad
TSi Next payload: TSr, reserved: 0x0,
   length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0,
   length: 16
start port: 0, end port: 65535
start addr: 192.168.2.99,
   end addr: 192.168.2.99
TSr Next payload: NONE, reserved: 0x0,
   length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0,
   length: 16
start port: 0, end port: 65535
start addr: 192.168.1.12, end addr: 192.168.1.12

IKEv2-PROTO-3: Tx
   [L 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0]
   m_id: 0x6
IKEv2-PROTO-3: HDR[i:FD366326E1FED6FE -
   r: A75B9B2582AAECB7]
IKEv2-PROTO-4: IKEV2 HDR ispi: FD366326E1FED6FE -
   rspi: A75B9B2582AAECB7
IKEv2-PROTO-4: Next payload: ENCR, version: 2.0
IKEv2-PROTO-4: Exchange type: CREATE_CHILD_SA,
   flags: RESPONDER MSG-RESPONSE
IKEv2-PROTO-4: Message id: 0x6, length: 172
ENCR Next payload: SA, reserved: 0x0,
   length: 144
Encrypted data&colon; 140 bytes
```

ASA1에서 응답을 보냅니다.

```
IKEv2-PLAT-4: SENT PKT
   [CREATE_CHILD_SA]
   [10.0.0.1]:500->
   [10.0.0.2]:500
   InitSPI=0xfd366326e1fed6fe
   RespSPI=0xa75b9b2582aaecb7
  MID=00000006
```

ASA2가 패킷을 수신합니다.

```
IKEv2-PLAT-4:
   RECV PKT [CREATE_CHILD_SA]
   [10.0.0.1]:500->
   [10.0.0.2]:500
   InitSPI=0xfd366326e1fed6fe
   RespSPI=0xa75b9b2582aaecb7
   MID=00000006

IKEv2-PROTO-3: Rx
   [L 10.0.0.2:500/R
   10.0.0.1:500/VRF i0:f0]
  m_id: 0x6
```

이제 ASA2에서 패킷을 확인합니다.

```
IKEv2-PROTO-3: HDR[i:FD366326E1FED6FE -
   r: A75B9B2582AAECB7]
IKEv2-PROTO-4: IKEV2 HDR ispi: FD366326E1FED6FE -
   rspi: A75B9B2582AAECB7
IKEv2-PROTO-4: Next payload: ENCR, version: 2.0
IKEv2-PROTO-4: Exchange type: CREATE_CHILD_SA,
   flags: RESPONDER MSG-RESPONSE
IKEv2-PROTO-4: Message id: 0x6, length: 172

REAL Decrypted packet:Data&colon; 116 bytes
SA Next payload: N, reserved: 0x0, length: 44
IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0,
   length: 40 Proposal: 1, Protocol id: ESP, SPI size: 4,
   #trans: 3
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 12 type: 1, reserved: 0x0, id: AES-CBC
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0:
   length: 8 type: 3, reserved: 0x0, id: SHA96
IKEv2-PROTO-4: last transform: 0x0,
   reserved: 0x0: length: 8 type: 5, reserved: 0x0, id:

N Next payload: TSi, reserved: 0x0,
   length: 24

b7 6a c6 75 53 55 99 5a df ee 05 18
   1a 27 a6 cb
01 56 22 ad
TSi Next payload: TSr, reserved: 0x0,
   length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0,
   length: 16
start port: 0, end port: 65535
start addr: 192.168.2.99,
   end addr: 192.168.2.99
TSr Next payload: NONE, reserved: 0x0,
   length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0,
   length: 16
start port: 0, end port: 65535
start addr: 192.168.1.12,
   end addr: 192.168.1.12

Decrypted packet:Data&colon; 172 bytes
IKEv2-PROTO-5: (225): SM Trace->
   SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I)
   MsgID = 00000006 CurState:
   CHILD_I_WAIT Event: EV_RECV_CREATE_CHILD
IKEv2-PROTO-5: (225): Action: Action_Null
IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE
```

```
   R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000006
   CurState: CHILD_I_PROC Event: EV_CHK4_NOTIFY
IKEv2-PROTO-2: (225): Processing any notify-messages
   in child SA exchange
IKEv2-PROTO-5: (225): SM Trace->
   SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I)
   MsgID = 00000006 CurState: CHILD_I_PROC
   Event: EV_VERIFY_MSG
IKEv2-PROTO-3: (225): Validating create child message
IKEv2-PROTO-5: (225): SM Trace->
   SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I)
   MsgID = 00000006 CurState: CHILD_I_PROC
   Event: EV_PROC_MSG
IKEv2-PROTO-2: (225): Processing child SA exchange
IKEv2-PROTO-5: (225): SM Trace->
   SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (
   I) MsgID = 00000006 CurState: CHILD_I_PROC
   Event: EV_CHK4_PFS
IKEv2-PROTO-3: (225): Checking for PFS configuration
IKEv2-PROTO-5: (225): SM Trace-> SA:
   I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I)
   MsgID = 00000006 CurState: CHILD_I_PROC
   Event: EV_CHK_IKE_REKEY
IKEv2-PROTO-3: (225): Checking if IKE SA rekey
IKEv2-PROTO-5: (225): SM Trace-> SA:
   I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I)
   MsgID = 00000006 CurState: CHILD_I_PROC
   Event: EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3: (225): Load IPSEC key material
IKEv2-PLAT-3: PROXY MATCH on crypto map outside_map seq 1
IKEv2-PLAT-3: (225) DPD Max Time will be: 10
IKEv2-PLAT-3: (225) DPD Max Time will be: 10
```

ASA1은 이 하위 SA 항목을 SAD에 삽입합니다.

```
IKEv2-PROTO-5: (225):
   SM Trace->
   SA: I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R)
   MsgID = 00000006
   CurState: CHILD_R_DONE
   Event: EV_OK

IKEv2-PROTO-2: (225):
   SA created; inserting
   SA into database

IKEv2-PROTO-5: (225):
   SM Trace->
   SA: I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (R)
   MsgID = 00000006 CurState:
   CHILD_R_DONE
  Event: EV_START_DEL_NEG_TMR
```

ASA2는 이 하위 SA 항목을 SAD에 삽입합니다.

```
IKEv2-PROTO-5: (225):
   SM Trace->
   SA: I_SPI=FD366326E1FED6FE
   R_SPI=A75B9B2582AAECB7 (I)
   MsgID = 00000006
   CurState: CHILD_I_DONE
   Event: EV_OK

IKEv2-PROTO-2: (225):
   SA created;
  inserting SA into database
```

터널 확인

ISAKMP(Internet Security Association and Key Management Protocol) 및 IPSec 터널 컨피그레이션을 확인하려면 이 섹션에 제공된 정보를 사용합니다.

ISAKMP

ISAKMP를 확인하려면 다음 명령을 입력합니다.

```
show crypto isakmp sa det
```

ASA1

ASA1의 출력은 다음과 같습니다.

```
ASA1(config)#show cry isa sa det
There are no IKEv1 SAs

IKEv2 SAs:Session-id:99220, Status:UP-ACTIVE, IKE count:1, CHILD count:2

Tunnel-id Local Remote Status Role
1889403559 10.0.0.1/500 10.0.0.2/500 READY RESPONDER

Encr: 3DES, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/195 sec
Session-id: 99220
Status Description: Negotiation done
Local spi: A75B9B2582AAECB7 Remote spi: FD366326E1FED6FE
Local id: 10.0.0.1
Remote id: 10.0.0.2
Local req mess id: 14 Remote req mess id: 16
Local next mess id: 14 Remote next mess id: 16
Local req queued: 14 Remote req queued: 16
Local window: 1 Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is not detected
Child sa: local selector 192.168.1.12/0 - 192.168.1.12/65535
remote selector 192.168.2.99/0 - 192.168.2.99/65535
ESP spi in/out: 0x8564387d/0x8717a5a
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
Child sa: local selector 192.168.1.1/0 - 192.168.1.1/65535
remote selector 192.168.2.99/0 - 192.168.2.99/65535
ESP spi in/out: 0x74756292/0xf0d97b2a
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
```

ASA2

ASA2의 출력은 다음과 같습니다.

```
ASA2(config)#show cry isa sa det

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:99220, Status:UP-ACTIVE, IKE count:1, CHILD count:2

Tunnel-id                Local               Remote    Status        Role
472237395         10.0.0.2/500         10.0.0.1/500     READY   INITIATOR
     Encr: 3DES, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/190 sec
     Session-id: 99220
     Status Description: Negotiation done
     Local spi: FD366326E1FED6FE       Remote spi: A75B9B2582AAECB7
     Local id: 10.0.0.2
     Remote id: 10.0.0.1
     Local req mess id: 16             Remote req mess id: 13
     Local next mess id: 16            Remote next mess id: 13
     Local req queued: 16              Remote req queued: 13
     Local window: 1                   Remote window: 1
     DPD configured for 10 seconds, retry 2
     NAT-T is not detected
Child sa: local selector  192.168.2.99/0 - 192.168.2.99/65535
         remote selector 192.168.1.12/0 - 192.168.1.12/65535
         ESP spi in/out: 0x8717a5a/0x8564387d
         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
Child sa: local selector  192.168.2.99/0 - 192.168.2.99/65535
         remote selector 192.168.1.1/0 - 192.168.1.1/65535
         ESP spi in/out: 0xf0d97b2a/0x74756292
         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

IPSec을 확인하려면 다음 명령을 입력합니다.

```
show crypto ipsec sa
```

ASA1

ASA1의 출력은 다음과 같습니다.

```
ASA1(config)#show cry ipsec sa
interface: outside
   Crypto map tag: outside_map, seq num: 1, local addr: 10.0.0.1

     access-list l2l_list extended permit ip host 192.168.1.1
       host 192.168.2.99
      local ident (addr/mask/prot/port):
         (192.168.1.1/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (
         192.168.2.99/255.255.255.255/0/0)
      current_peer: 10.0.0.2

      #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
      #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 3, #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.: 10.0.0.1/500, remote crypto endpt.:
         10.0.0.2/500
      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: F0D97B2A
      current inbound spi : 74756292

    inbound esp sas:
      spi: 0x74756292 (1953850002)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 137990144, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4008959/28628)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000000F
   outbound esp sas:
     spi: 0xF0D97B2A (4040784682)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, }
        slot: 0, conn_id: 137990144, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4147199/28628)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
          0x00000000 0x00000001

   Crypto map tag: outside_map, seq num: 1, local addr: 10.0.0.1

     access-list l2l_list extended permit ip host 192.168.1.12
       host 192.168.2.99
     local ident (addr/mask/prot/port): (
       192.168.1.12/255.255.255.255/0/0)
     remote ident (addr/mask/prot/port):
       (192.168.2.99/255.255.255.255/0/0)
     current_peer: 10.0.0.2
     #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
     #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 3, #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.: 10.0.0.1/500, remote crypto
       endpt.: 10.0.0.2/500
     path mtu 1500, ipsec overhead 74, media mtu 1500
     current outbound spi: 08717A5A
     current inbound spi : 8564387D

   inbound esp sas:
     spi: 0x8564387D (2237937789)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, }
        slot: 0, conn_id: 137990144, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4285439/28734)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000000F
   outbound esp sas:
     spi: 0x08717A5A (141654618)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, }
        slot: 0, conn_id: 137990144, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4055039/28734)
        IV size: 16 bytes
        replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ASA2

ASA2의 출력은 다음과 같습니다.

```
ASA2(config)#show cry ipsec sa
interface: outside
   Crypto map tag: outside_map, seq num: 1, local addr: 10.0.0.2

     access-list l2l_list extended permit ip host 192.168.2.99 host
       192.168.1.12
     local ident (addr/mask/prot/port):
       (192.168.2.99/255.255.255.255/0/0)
     remote ident (addr/mask/prot/port):
       (192.168.1.12/255.255.255.255/0/0)
     current_peer: 10.0.0.1

     #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
     #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 3, #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.: 10.0.0.2/500, remote crypto
       endpt.: 10.0.0.1/500
     path mtu 1500, ipsec overhead 74, media mtu 1500
     current outbound spi: 8564387D
     current inbound spi : 08717A5A

   inbound esp sas:
     spi: 0x08717A5A (141654618)
```

```
      transform: esp-aes-256 esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 137973760, crypto-map: outside_map
      sa timing: remaining key lifetime (kB/sec): (4193279/28770)
      IV size: 16 bytes         replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x0000000F
 outbound esp sas:
   spi: 0x8564387D (2237937789)
      transform: esp-aes-256 esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 137973760, crypto-map: outside_map
      sa timing: remaining key lifetime (kB/sec): (4055039/28770)
      IV size: 16 bytes         replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x00000001

Crypto map tag: outside_map, seq num: 1, local addr: 10.0.0.2

  access-list l2l_list extended permit ip host 192.168.2.99
    host 192.168.1.1
  local ident (addr/mask/prot/port): (
    192.168.2.99/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port):
    (192.168.1.1/255.255.255.255/0/0)
  current_peer: 10.0.0.1
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 3, #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.: 10.0.0.2/500, remote crypto
    endpt.: 10.0.0.1/500
  path mtu 1500, ipsec overhead 74, media mtu 1500
  current outbound spi: 74756292
  current inbound spi : F0D97B2A

inbound esp sas:
  spi: 0xF0D97B2A (4040784682)
     transform: esp-aes-256 esp-sha-hmac no compression
     in use settings ={L2L, Tunnel, }
     slot: 0, conn_id: 137973760, crypto-map: outside_map
     sa timing: remaining key lifetime (kB/sec): (4285439/28663)
     IV size: 16 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x0000000F
outbound esp sas:
  spi: 0x74756292 (1953850002)
     transform: esp-aes-256 esp-sha-hmac no compression
     in use settings ={L2L, Tunnel, }
     slot: 0, conn_id: 137973760, crypto-map: outside_map
     sa timing: remaining key lifetime (kB/sec): (4331519/28663)
     IV size: 16 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

show crypto isakmp sa 명령의 출력과 동일한 출력을 제공하는 **show crypto ikev2 sa 명령**의 **출력도** 확인할 수 있습니다.

```
IKEv2 SAs:

Session-id:99220, Status:UP-ACTIVE, IKE count:1, CHILD count:2

Tunnel-id                Local               Remote   Status        Role
1889403559         10.0.0.1/500         10.0.0.2/500    READY   RESPONDER
     Encr: 3DES, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/179 sec
Child sa: local selector  192.168.1.12/0 - 192.168.1.12/65535
         remote selector 192.168.2.99/0 - 192.168.2.99/65535
         ESP spi in/out: 0x8564387d/0x8717a5a
Child sa: local selector  192.168.1.1/0 - 192.168.1.1/65535
         remote selector 192.168.2.99/0 - 192.168.2.99/65535
         ESP spi in/out: 0x74756292/0xf0d97b2a
```

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

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