

对具有PSK的站点到站点VPN使用ASA IKEv2调试

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[核心问题](#)

[使用的调试](#)

[ASA配置](#)

[ASA1](#)

[ASA2](#)

[调试](#)

[隧道协商](#)

[子SA调试](#)

[隧道验证](#)

[ISAKMP](#)

[ASA1](#)

[ASA2](#)

[IPsec](#)

[ASA1](#)

[ASA2](#)

[相关信息](#)

简介

本文档介绍有关思科自适应安全设备(ASA)上的互联网密钥交换版本2(IKEv2)调试的信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

核心问题

IKEv2中使用的数据包交换过程与IKEv1中使用的数据包交换过程截然不同。使用IKEv1时，有一个明确分界的第1阶段交换，包含六个数据包，然后是包含三个数据包的第2阶段交换。IKEv2交换是可变的。

提示：有关差异的更多详细信息以及数据包交换过程的说明，请参阅[IKEv2数据包交换和协议级调试](#)。

使用的调试

以下两个调试用于IKEv2:

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

ASA配置

本节提供ASA1 (启动器) 和ASA2 (响应器) 的示例配置。

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 *****
```

调试

本节介绍ASA1 (发起方) 和ASA2 (响应方) 隧道协商以及子级安全关联(SA)调试和消息说明。

隧道协商

ASA1收到与对等体ASA 10.0.0.2的加密访问控制列表(ACL)匹配的数据包，然后启动SA创建：

```
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

发送的初始消息对用于IKE_SA_INIT交换。这些消息会协商加密算法、交换失效并执行Diffie-Hellman(DH)交换。

以下是ASA1的相关配置：

```
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
  *****
```

以下是此交换的调试输出：

```
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_REC'D_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
ASA1随后构建IKE_INIT_SA数据包，其中包含：

```

- **ISAKMP报头 (SPI/版本/标志)**
- **SAi1 (IKE发起程序支持的加密算法)**
- **KEi (发起方的DH公钥值)**
- **N(发起方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
```

然后，ASA1会发送IKE_INIT_SA数据包：

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

ASA2接收IKEV_INIT_SA数据包：

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

ASA2启动该对等体的SA创建：

```
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)

```

ASA2验证并处理IKE_INIT消息：

1. 它从ASA1提供的加密套件中选择加密套件。
2. 它计算自己的DH密钥。
3. 它还计算SKEY ID值，从中可以派生此IKE_SA的所有密钥。除后面的所有邮件的报头外，所有邮件都经过加密和身份验证。用于加密和完整性保护的密钥源自SKEY ID，称为：

SK_e用于加密。

SK_a用于身份验证。

SK_d是派生的，用于为CHILD_SA派生进一步的密钥材料。为每个方向计算单独的SK_e和SK_a。

以下是ASA2的相关配置：

```

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
  *****
```

以下是调试输出：

```
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_REC'D_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_REC'D_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

```

然后，ASA2会为ASA1收到的IKE_SA_INIT交换构建响应方消息。此数据包包含：

- ISAKMP报头 (SPI/版本/标志)
- SA_r1(IKE响应器选择的加密算法)
- KE_r (响应方的DH公钥值)
- 响应器Nonce

以下是调试输出：

```

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 -
rsp: 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
```

ASA2向ASA1发送响应方消息：

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

ASA1收到来自ASA2的IKE_SA_INIT响应数据包：

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

ASA2启动授权过程的计时器：

```
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
```

ASA1验证并处理响应：

1. 计算启动器DH密钥。

2. 生成启动器SKYID。

以下是调试输出：

```
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 -
rspci: 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_REC'D_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之间的IKE_INIT_SA交换现已完成 :
```

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

ASA1启动IKE_AUTH交换并开始生成身份验证负载。IKE_AUTH数据包包含 :

- ISAKMP报头 (SPI/版本/标志)
- IDi(发起方身份)

- AUTH负载
- SAI2 (启动SA — 类似于IKEv1中的第2阶段转换集交换)
- TSi和TSr(发起方和响应方流量选择器)

注意:TSi和TSr分别包含发起方和响应方的源地址和目的地址，以转发/接收加密流量。地址范围指定进出该范围的所有流量都通过隧道传输。如果响应方可以接受该建议，它将返回相同的TS负载。

此外，为与触发数据包匹配的proxy_ID对创建第一个CHILD_SA。

以下是ASA1的相关配置：

```
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
```

以下是调试输出：

```
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: 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: 252 bytes
```

ASA1将IKE_AUTH数据包发送到ASA2:

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

ASA2从ASA1接收此数据包:

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

ASA2停止授权计时器并验证从ASA1收到的身份验证数据。然后，它会生成自己的身份验证数据，与ASA1完全相同。

以下是ASA2的相关配置：

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

以下是调试输出：

```
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: 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: 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
ASA2发送IKE_AUTH数据包，其中包含：

```

- ISAKMP报头 (SPI/版本/标志)
- IDr.(响应方身份)
- AUTH负载
- SAR2 (启动SA — 类似于IKEv1中的第2阶段转换集交换)

• TSi和TSr(发起方和响应方流量选择器)

注意:TSi和TSr分别包含发起方和响应方的源地址和目的地址，以转发/接收加密流量。地址范围指定进出该范围的所有流量都通过隧道传输。这些参数与从ASA1接收的参数相同。

以下是调试输出：

```
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: 204 bytes

ASA2发送IKE_AUTH数据包的响应 :

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

ASA1收到来自ASA2的响应 :

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

ASA2在SA数据库(SAD)中插入条目 :

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**

ASA1验证并处理此数据包中的身份验证数据，然后将此SA插入其SAD:

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: 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: 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: 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
```

隧道现在对ASA1处于活动状态：

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
```

隧道现在对ASA2处于活动状态：

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
```

注意：响应方隧道通常在发起方隧道之前变为活动状态。

IKEv2注册过程在ASA1上发生：

```
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 attributes
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注册过程发生在ASA2上 :

```
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
```

子SA调试

注：此交换由单个请求和响应对组成，在IKEv1中称为2阶段。初始交换完成后，IKE_SA的任一端均可发起此协议。

ASA2启动CHILD_SA交换。这是CREATE_CHILD_SA请求。CHILD_SA数据包通常包含：

- **SA HDR** -它包含version.flags和交换类型。
- **Nonce Ni(可选)** — 如果将CHILD_SA创建为初始交换的一部分，则不得发送第二个密钥交换(KE)负载和nonce。
- **SA负载**
- **KEi(Key-optional)**- CREATE_CHILD_SA请求可以选择性地包含用于附加DH交换的KE负载，以便为CHILD_SA启用更强的前向保密保证。如果SA提供包括不同的DH组，则KEi必须是发起方期望响应方接受的组的元素。如果它猜测错误，CREATE_CHILD_SA交换将失败，并且必须使用其他KEi重试。
- **N (通知负载，可选)** — 通知负载，用于将信息数据（例如错误条件和状态转换）传输到IKE对等体。通知负载可以出现在响应消息（通常指定请求被拒绝的原因）、信息交换（以便报

告不在IKE请求中的错误)或任何其他消息中,以便指示发送方功能或修改请求的含义。如果此CREATE_CHILD_SA交换重新生成除IKE_SA之外的当前SA的密钥,REKEY_SA类型的前N个负载必须标识重新生成密钥的SA。如果此CREATE_CHILD_SA交换不为当前SA重新生成密钥,则必须省略N个负载。

- **TSi和TSr (可选)**: 显示为其创建SA的流量选择器。在本例中,它位于主机192.168.1.12和192.168.2.99之间。

以下是CREATE_CHILD_SA调试输出:

```
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 -
rsp: 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: 148 bytes
ASA2发送此数据包并等待响应 :

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

ASA1接收数据包 :

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
```

然后，ASA1从ASA2收到此确切的数据包并对其进行验证：

```
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
```

ASA1现在为CHILD_SA交换构建应答。这是CREATE_CHILD_SA响应。CHILD_SA数据包通常包含：

- **SA HDR** -它包含version.flags和交换类型。
- **Nonce Ni**(可选) — 如果创建CHILD_SA作为初始交换的一部分，则不得发送第二个KE负载和nonce。
- **SA负载**
- **KEi** (Key , 可选) — CREATE_CHILD_SA请求可以选择性地包含用于附加DH交换的KE负载，以便为CHILD_SA启用更强的前向保密保证。如果SA提供包括不同的DH组，则KEi必须是发起方期望响应方接受的组的元素。如果它猜测错误，则CREATE_CHILD_SA交换将失败，并且必须使用其他KEi重试。
- **N** (通知负载 , 可选) — 通知负载用于将信息数据 (例如错误条件和状态转换) 传输到IKE对等体。通知负载可以出现在响应消息 (通常指定请求被拒绝的原因)、信息交换 (以报告不在IKE请求中的错误) 或任何其他消息中，以指示发送方功能或修改请求的含义。如果此CREATE_CHILD_SA交换重新生成除IKE_SA之外的当前SA的密钥，REKEY_SA类型的前N个负载必须标识重新生成密钥的SA。如果此CREATE_CHILD_SA交换不为当前SA重新生成密钥，则必须省略N个负载。
- **TSi和TSr** (可选) — 显示为其创建SA的流量选择器。在本例中，它位于主机192.168.1.12和192.168.2.99之间。

以下是调试输出：

```
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_REC'D_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 -
rsp: 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: 140 bytes

ASA1发送响应 :

IKEv2-PLAT-4: **SENT PKT**

[CREATE_CHILD_SA]

[10.0.0.1]:500->

[10.0.0.2]:500

InitSPI=0xfd366326e1fed6fe

RespSPI=0xa75b9b2582aaecb7

MID=00000006

ASA2接收数据包 :

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

ASA2现在验证数据包 :

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: 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: 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
```

ASA1将此子SA条目插入SAD:

```
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
```

ASA2将此子SA条目插入SAD:

```
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
```

隧道验证

使用本节提供的信息验证Internet安全关联和密钥管理协议(ISAKMP)和IPSec隧道配置。

ISAKMP

要验证ISAKMP，请输入以下命令：

```
show crypto isakmp sa det
```

ASA1

以下是ASA1的输出：

```
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

以下是ASA2的输出：

```
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

要验证IPSec，请输入以下命令：

```
show crypto ipsec sa
```

ASA1

以下是ASA1的输出：

```
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, #rcv 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 121_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

以下是ASA2的输出：

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

  access-list 121_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 121_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
```

您还可以检查show crypto ikev2 sa命令的输出，该命令提供的输出与show crypto isakmp sa命令的输出相同：

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

相关信息

- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。