Utiliser les débogages ASA IKEv2 pour VPN site à site avec PSK

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Problème de base
- Débogages utilisés
- Configurations ASA
  - ASA1
  - ASA2
- Déboguages
  - Négociation de tunnel
  - Débogages SA enfant
- Vérification du tunnel
  - ISAKMP
    - ASA1
    - ASA2
  - IPSEC
    - ASA1
    - ASA2
- Informations connexes

Introduction

Ce document décrit les informations sur les débogages IKEv2 (Internet Key Exchange Version 2) sur l'appliance de sécurité adaptatif Cisco (ASA).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème de base

Le processus d’échange de paquets utilisé dans IKEv2 est radicalement différent de celui utilisé dans IKEv1. Avec IKEv1, il y a un échange de phase 1 clairement délimité qui se compose de six paquets, puis il y a un échange de phase 2 qui se compose de trois paquets. L'échange IKEv2 est variable.

 Conseil : Pour plus d'informations détaillées sur les différences et une explication du processus d'échange de paquets, référez-vous à Échange de paquets IKEv2 et débogage au niveau du protocole.

Débogages utilisés

Ces deux débogages sont utilisés pour IKEv2 :

<#root>

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

Configurations ASA

Cette section fournit des exemples de configuration pour ASA1 (l'initiateur) et ASA2 (le répondeur).

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 *****
```

Déboguages

Cette section décrit la négociation de tunnel ASA1 (initiateur) et ASA2 (répondeur) ainsi que les débogages et les descriptions de message de l'association de sécurité enfant.

Négociation de tunnel

ASA1 reçoit un paquet qui correspond à la liste de contrôle d'accès (ACL) de chiffrement pour l'homologue ASA 10.0.0.2 et lance la création de SA :

<#root>

```
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

La paire initiale de messages qui sont envoyés est destinée à l'échange IKE_SA_INIT. Ces messages négocient les algorithmes cryptographiques, échangent des nonces et effectuent un échange Diffie-Hellman (DH).

Voici la configuration appropriée pour ASA1 :

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

Voici le résultat du débogage pour cet échange :

<#root>

```
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
```

ASA1 crée ensuite le paquet IKE_INIT_SA, qui contient :

- En-tête ISAKMP (SPI/version/indicateurs)
- SAi1 (algorithme cryptographique pris en charge par l'initiateur IKE)
- KEi (valeur de clé publique DH de l'initiateur)
- N (Initiator Nonce)

<#root>

```
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
```

Le paquet IKE_INIT_SA est ensuite envoyé par ASA1 :

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

ASA2 reçoit le paquet IKEV_INIT_SA :

```
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 lance la création de SA pour cet homologue :

<#root>

```
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 vérifie et traite le message IKE_INIT :

1. Il choisit la suite de chiffrement parmi celles offertes par ASA1.
2. Il calcule sa propre clé secrète DH.
3. Il calcule également une valeur SKEYID à partir de laquelle toutes les clés peuvent être dérivées pour cette IKE_SA. Tous les en-têtes de tous les messages qui suivent, à l'exception de ceux, sont chiffrés et authentifiés. Les clés utilisées pour le cryptage et la protection de l'intégrité sont dérivées de SKEYID et sont appelées :
    - SK_e est utilisé pour le chiffrement.
    - SK_a est utilisé pour l'authentification.
    - SK_d est dérivé et utilisé pour la dérivation d'autres éléments de clé pour les associations de sécurité enfant. Un SK_e et un SK_a distincts sont calculés pour chaque direction.

Voici la configuration appropriée pour ASA2 :

```
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 *****
```

Voici le résultat du débogage :

<#root>

```
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
```

ASA2 génère ensuite le message du répondeur pour l'échange IKE_SA_INIT, qui est reçu par ASA1. Ce paquet contient :

- En-tête ISAKMP (SPI/ version/indicateurs)
- SAr1 (algorithme cryptographique choisi par le répondeur IKE)
- KEr (valeur de clé publique DH du répondeur)
- Nonce du répondeur

Voici le résultat du débogage :

<#root>

```
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
```

ASA2 envoie le message du répondeur à ASA1 :

```
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 reçoit le paquet de réponse IKE_SA_INIT de ASA2 :

```
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 démarre le minuteur pour le processus d'autorisation :

<#root>

```
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 vérifie et traite la réponse :

1. La clé secrète DH de l'initiateur est calculée.
2. L'initiateur SKEYID est généré.

Voici le résultat du débogage :

<#root>

```
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
```

L'échange IKE_INIT_SA entre les ASA est maintenant terminé :

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

ASA1 démarre l'échange IKE_AUTH et commence à générer la charge utile d'authentification. Le paquet IKE_AUTH contient :

- En-tête ISAKMP (SPI/ version/indicateurs)
- IDi (identité de l'initiateur)

- données utiles AUTH
- SAi2 (initie la SA - similaire à l'échange d'ensemble de transformation de phase 2 dans IKEv1)
- TSi et TSr (sélecteurs de trafic initiateur et répondeur)

Remarque : Le TSi et le TSr contiennent respectivement l'adresse source et l'adresse de destination de l'initiateur et du répondeur pour transférer/recevoir le trafic chiffré. La plage d'adresses indique que tout le trafic en provenance et à destination de cette plage est tunnellisé. Si la proposition est acceptable pour le répondeur, elle renvoie des charges utiles TS identiques.

En outre, la première CHILD_SA est créée pour la paire proxy_ID qui correspond au paquet déclencheur.

Voici la configuration appropriée pour ASA1 :

```
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
```

Voici le résultat du débogage :

<#root>

```
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
```

ASA1 envoie le paquet IKE_AUTH à 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 reçoit ce paquet de ASA1 :

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

ASA2 arrête le minuteur d'autorisation et vérifie les données d'authentification reçues d'ASA1. Il génère ensuite ses propres données d'authentification, exactement comme ASA1.

Voici la configuration appropriée pour ASA2 :

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

Voici le résultat du débogage :

<#root>

```
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
```

ASA2 envoie le paquet IKE_AUTH, qui contient :

- En-tête ISAKMP (SPI/ version/indicateurs)
- IDr. (identité du répondeur)
- données utiles AUTH
- SAr2 (initie la SA - similaire à l'échange d'ensemble de transformation de phase 2 dans IKEv1)
- TSi et TSr (sélecteurs de trafic initiateur et répondeur)

Remarque : Le TSi et le TSr contiennent respectivement l'adresse source et l'adresse de destination de l'initiateur et du répondeur pour transférer/recevoir le trafic chiffré. La plage

---

d’adresses indique que tout le trafic en provenance et à destination de cette plage est tunnellisé. Ces paramètres sont identiques à ceux reçus de l'ASA1.

Voici le résultat du débogage :

<#root>

```
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
```

ASA2 envoie la réponse pour le paquet IKE_AUTH :

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

ASA1 reçoit la réponse de ASA2 :

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

ASA2 insère une entrée dans la base de données SA (SAD) :

<#root>

```
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 vérifie et traite les données d'authentification dans ce paquet, puis insère cette SA dans son SAD :

<#root>

```
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

Le tunnel est maintenant actif pour ASA1 :

<#root>

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
```

Le tunnel est maintenant actif pour ASA2 :

<#root>

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
```

Remarque : Le tunnel du répondeur devient généralement actif avant le tunnel de l'initiateur.

Le processus d'enregistrement IKEv2 se produit sur ASA1 :

<#root>

```
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
```

Le processus d'enregistrement IKEv2 se produit sur ASA2 :

<#root>

```
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
```

Débogages SA enfant

Remarque : Cet échange se compose d'une seule paire requête/réponse et est appelé échange de phase 2 dans IKEv1. Il peut être initié par l'une ou l'autre des extrémités de IKE_SA une fois les échanges initiaux terminés.

ASA2 initie l'échange CHILD_SA. Il s'agit de la demande CREATE_CHILD_SA. Le paquet

CHILD_SA contient généralement :

- SA HDR : contient le fichier version.flags et le type d'échange.
- Nonce Ni (facultatif) - Si CHILD_SA est créé dans le cadre de l'échange initial, une seconde charge utile d'échange de clé (KE) et nonce ne doivent pas être envoyés.
- Charge utile SA
- KEi (Key-optional) - La requête CREATE_CHILD_SA peut éventuellement contenir une charge utile KE pour un échange DH supplémentaire afin de permettre des garanties plus solides de confidentialité de transfert pour CHILD_SA. Si les offres SA incluent différents groupes DH, alors le KEi doit être un élément du groupe que l'initiateur attend du répondeur qu'il accepte. S'il devine mal, l'échange CREATE_CHILD_SA échoue et il doit réessayer avec un autre KEi.
- N (Notify payload, facultatif) : la fonction Notify payload est utilisée pour transmettre des données d'information, telles que des conditions d'erreur et des transitions d'état, à un homologue IKE. Un message Notify Payload peut apparaître dans un message de réponse (qui indique généralement pourquoi une demande est rejetée), dans un échange d'informations (afin de signaler une erreur qui ne se trouve pas dans une demande IKE) ou dans tout autre message afin d'indiquer les capacités de l'expéditeur ou afin de modifier la signification de la demande. Si cet échange CREATE_CHILD_SA redéfinit une SA actuelle autre que la SA IKE, la charge utile N principale de type REKEY_SA doit identifier la SA qui est redéfinie. Si cet échange CREATE_CHILD_SA ne redonne pas de clé à une SA actuelle, alors la charge utile N doit être omise.
- TSi et TSr (en option) : Affiche les sélecteurs de trafic pour lesquels l'association de sécurité est créée. Dans ce cas, il se situe entre les hôtes 192.168.1.12 et 192.168.2.99.

Voici le résultat du débogage de CREATE_CHILD_SA :

<#root>

```
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
```

ASA2 envoie ce paquet et attend la réponse :

<#root>

```
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 reçoit le paquet :

<#root>

```
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
```

ASA1 reçoit alors ce paquet exact de ASA2 et le vérifie :

<#root>

```
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 crée maintenant la réponse pour l'échange CHILD_SA. Il s'agit de la réponse CREATE_CHILD_SA. Le paquet CHILD_SA contient généralement :

- SA HDR : contient le fichier version.flags et le type d'échange.
- Nonce Ni (facultatif) - Si la CHILD_SA est créée dans le cadre de l'échange initial, une seconde charge utile KE et nonce ne doivent pas être envoyées.
- Charge utile SA
- KEi (Key, optional) - La requête CREATE_CHILD_SA peut éventuellement contenir une charge utile KE pour un échange DH supplémentaire afin de permettre des garanties plus solides de confidentialité de transfert pour CHILD_SA. Si les offres SA incluent différents groupes DH, alors le KEi doit être un élément du groupe que l'initiateur attend du répondeur qu'il accepte. S'il devine mal, l'échange CREATE_CHILD_SA échoue et il doit réessayer avec un autre KEi.
- N (Notify payload, facultatif) : cette fonction est utilisée pour transmettre des données d'information, telles que des conditions d'erreur et des transitions d'état, à un homologue IKE. Un message Notify Payload peut apparaître dans un message de réponse (qui indique généralement pourquoi une demande est rejetée), dans un échange d'informations (afin de signaler une erreur qui ne figure pas dans une demande IKE) ou dans tout autre message afin d'indiquer les capacités de l'expéditeur ou afin de modifier la signification de la demande. Si cet échange CREATE_CHILD_SA redéfinit une SA actuelle autre que la SA IKE, la charge utile N principale de type REKEY_SA doit identifier la SA qui est redéfinie. Si cet échange CREATE_CHILD_SA ne redonne pas de clé à une SA actuelle, la charge utile N doit être omise.
- TSi et TSr (facultatif) : affiche les sélecteurs de trafic pour lesquels l'association de sécurité est créée. Dans ce cas, il se situe entre les hôtes 192.168.1.12 et 192.168.2.99.

Voici le résultat du débogage :

<#root>

```
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
```

ASA1 envoie la réponse :

<#root>

```
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 reçoit le paquet :

<#root>

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 vérifie maintenant le paquet :

<#root>

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&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
```

ASA1 insère cette entrée SA enfant dans le SAD :

<#root>

```
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 insère cette entrée SA enfant dans le SAD :

<#root>

```
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
```

Vérification du tunnel

Utilisez les informations fournies dans cette section afin de vérifier les configurations du protocole ISAKMP (Internet Security Association and Key Management Protocol) et du tunnel IPSec.

ISAKMP

Afin de vérifier l'ISAKMP, entrez cette commande :

<#root>

```
show crypto isakmp sa det
```

ASA1

Voici le résultat pour ASA1 :

<#root>

```
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

Voici le résultat pour ASA2 :

<#root>

```
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

Afin de vérifier l'IPSec, entrez cette commande :

<#root>

show crypto ipsec sa

ASA1

Voici le résultat pour ASA1 :

<#root>

```
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

Voici le résultat pour ASA2 :

<#root>

```
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
```

Vous pouvez également vérifier le résultat de la commande show crypto ikev2 sa, qui fournit un résultat identique au résultat de la commande show crypto isakmp sa :

```
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
```

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.