

Utilizar depuraciones IKEv2 de ASA para VPN de sitio a sitio con PSK

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema principal](#)

[Depuraciones utilizadas](#)

[Configuraciones ASA](#)

[ASA1](#)

[ASA2](#)

[Depuraciones](#)

[Negociación de túnel](#)

[Depuraciones SA secundarias](#)

[Verificación del túnel](#)

[ISAKMP](#)

[ASA1](#)

[ASA2](#)

[IPSec](#)

[ASA1](#)

[ASA2](#)

[Información Relacionada](#)

Introducción

Este documento describe información sobre las depuraciones de Intercambio de claves de Internet versión 2 (IKEv2) en el Cisco Adaptive Security Appliance (ASA).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema principal

El proceso de intercambio de paquetes que se utiliza en IKEv2 es radicalmente diferente del que se utiliza en IKEv1. Con IKEv1, hay un intercambio de fase 1 claramente delimitado que consta de seis paquetes seguidos de un intercambio de fase 2 que consta de tres paquetes. El intercambio IKEv2 es variable.

Sugerencia: para obtener información más detallada sobre las diferencias y una explicación del proceso de intercambio de paquetes, consulte [Intercambio de Paquetes IKEv2 y Depuración de Nivel de Protocolo](#).

Depuraciones utilizadas

Estas dos depuraciones se utilizan para IKEv2:

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

Configuraciones ASA

Esta sección proporciona ejemplos de configuraciones para ASA1 (el iniciador) y ASA2 (el respondedor).

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 121_list extended permit ip host 192.168.2.99
host 192.168.1.1
access-list 121_list extended permit ip host 192.168.2.99
host 192.168.1.12

crypto map outside_map 1 match address 121_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 *****
```

Depuraciones

En esta sección se describen los debugs y las descripciones de mensajes de la negociación del túnel ASA1 (iniciador) y ASA2 (respondedor) y de la asociación de seguridad secundaria (SA).

Negociación de túnel

ASA1 recibe un paquete que coincide con la lista de control de acceso (ACL) crypto para el par ASA 10.0.0.2 e inicia la creación de SA:

```
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
```

El par inicial de mensajes que se envían son para el intercambio IKE_SA_INIT. Estos mensajes negocian los algoritmos criptográficos, intercambian nonces y realizan un intercambio Diffie-Hellman (DH).

Esta es la configuración relevante para 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
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
  *****
```

Este es el resultado de la depuración para este intercambio:

```

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
A continuación, ASA1 genera el paquete IKE_INIT_SA, que contiene:

```

- Encabezado ISAKMP (SPI/version/flags)
- SAi1 (algoritmo criptográfico que admite el iniciador IKE)
- KEi (valor de clave pública DH del iniciador)
- N (Iniciador 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

A continuación, ASA1 envía el paquete IKE_INIT_SA:

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

ASA2 recibe el paquete 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 inicia la creación de SA para ese par:

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 verifica y procesa el mensaje IKE_INIT:

1. Elige el conjunto de cifrado de los que ofrece ASA1.
2. Computa su propia clave secreta DH.
3. También calcula un valor SKEYID, del cual se pueden derivar todas las claves para este IKE_SA. Todos los encabezados de todos los mensajes que vienen después, excepto los que vienen a continuación, están cifrados y autenticados. Las claves que se utilizan para la protección de la integridad y el cifrado se derivan de SKEYID y se conocen como:

SK_e se utiliza para el cifrado.

SK_a se utiliza para la autenticación.

SK_d se deriva y se utiliza para derivar material de claves adicional para CHILD_SAs. Se calcula un SK_e y un SK_a separados para cada dirección.

Esta es la configuración relevante para 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
    *****
```

Este es el resultado de la depuración:

```
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 R_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

```

A continuación, ASA2 genera el mensaje de respuesta para el intercambio IKE_SA_INIT, que recibe ASA1. Este paquete contiene:

- **Encabezado ISAKMP** (SPI/versión/indicadores)
- **SAR1** (algoritmo criptográfico que elige el respondedor IKE)
- **KEr** (valor de clave pública DH del respondedor)
- **Responder Nonce**

Este es el resultado de la depuración:

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 envía el mensaje de respuesta a 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 recibe el paquete de respuesta IKE_SA_INIT del 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 inicia el temporizador para el proceso de autorización:

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 verifica y procesa la respuesta:

1. Se calcula la clave secreta DH del iniciador.
2. Se generará el ID ESQUEYA del iniciador.

Este es el resultado de la depuración:

```
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

El intercambio IKE_INIT_SA entre los ASA ha finalizado:

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

ASA1 inicia el intercambio IKE_AUTH y comienza a generar la carga útil de autenticación. El paquete IKE_AUTH contiene:

- **Encabezado ISAKMP** (SPI/versión/indicadores)
- **IDI** (identidad del iniciador)
- **carga de AUTH**
- **SAI2** (inicia SA, similar al intercambio de conjunto de transformación de fase 2 en IKEv1)
- **TSi y TSr** (selectores de tráfico de iniciador y respondedor)

Nota: TSi y TSr contienen la dirección de origen y de destino del iniciador y el respondedor respectivamente para reenviar/recibir tráfico cifrado. El rango de direcciones especifica que todo el tráfico hacia y desde ese rango se tuneliza. Si la propuesta es aceptable para el respondedor, devuelve cargas útiles de TS idénticas.

Además, el primer CHILD_SA se crea para el par proxy_ID que coincide con el paquete de desencadenador.

Esta es la configuración relevante para 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
```

Este es el resultado de la depuración:

```
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&colon; 252 bytes
```

ASA1 envía el paquete IKE_AUTH a 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 recibe este paquete 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 detiene el temporizador de autorización y verifica los datos de autenticación que se reciben de ASA1. A continuación, genera sus propios datos de autenticación, exactamente igual que ASA1.

Esta es la configuración relevante para ASA2:

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

Este es el resultado de la depuración:

```
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; 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_REC'D_IPSEC_RESP
IKEv2-PROTO-2: (16): Processing auth message
```

ASA2 envía el paquete IKE_AUTH, que contiene:

- **Encabezado ISAKMP** (SPI/versión/indicadores)
- **IDr** (identidad del respondedor)
- **carga de AUTH**
- **SAr2** (inicia SA, similar al intercambio de conjunto de transformación de fase 2 en IKEv1)
- **TSi y TSr** (selectores de tráfico de iniciador y respondedor)

Nota: TSi y TSr contienen la dirección de origen y de destino del iniciador y el respondedor respectivamente para reenviar/recibir tráfico cifrado. El rango de direcciones especifica que todo el tráfico hacia y desde ese rango se tuneliza. Estos parámetros son idénticos a los recibidos de ASA1.

Este es el resultado de la depuración:

```
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; 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 envía la respuesta para el paquete 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 recibe la respuesta 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 inserta una entrada en la base de datos SA (SAD):

```
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 verifica y procesa los datos de autenticación en este paquete, y luego inserta esta SA en su 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&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; 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**

El túnel está ahora activo para ASA1:

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

El túnel está ahora activo para ASA2:

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
```

Nota: El túnel del respondedor generalmente se activa antes del túnel del iniciador.

El proceso de registro de IKEv2 ocurre en ASA1:

```
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

El proceso de registro de IKEv2 ocurre en ASA2:

```
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
  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: 10.0.0.1:500,
  phase1_id: 10.0.0.1
```

Depuraciones SA secundarias

Nota: Este intercambio consta de un solo par de solicitud y respuesta, y se denomina intercambio de fase 2 en IKEv1. Puede ser iniciado por cualquiera de los extremos de IKE_SA después de que se completen los intercambios iniciales.

ASA2 inicia el intercambio CHILD_SA. Esta es la solicitud CREATE_CHILD_SA. El paquete CHILD_SA normalmente contiene:

- **SA HDR:** contiene version.flags y el tipo de intercambio.
- **Nonce Ni** (opcional): si se crea CHILD_SA como parte del intercambio inicial, no se debe enviar una segunda carga útil de intercambio de claves (KE) ni nonce.
- **Carga útil de SA**
- **KEi** (clave opcional): la solicitud CREATE_CHILD_SA puede contener opcionalmente una carga útil KE para un intercambio DH adicional con el fin de habilitar garantías más sólidas de confidencialidad de reenvío para CHILD_SA. Si las ofertas SA incluyen diferentes grupos DH, el KEi debe ser un elemento del grupo que el iniciador espera que acepte el respondedor. Si se calcula que no es correcto, el intercambio CREATE_CHILD_SA falla y tiene que volver a intentarlo con una KEi diferente.
- **N** (carga útil de notificación, opcional): la carga útil de notificación se utiliza para transmitir datos informativos, como condiciones de error y transiciones de estado, a un par IKE. Una carga útil de notificación puede aparecer en un mensaje de respuesta (normalmente específica por qué se rechaza una solicitud), en un intercambio de información (para informar de un error que no está en una solicitud IKE) o en cualquier otro mensaje para indicar las capacidades del remitente o para modificar el significado de la solicitud. Si este intercambio CREATE_CHILD_SA regenera una SA actual distinta de IKE_SA, la carga útil de N de lead de tipo REKEY_SA debe identificar la SA que se regenera. Si este intercambio CREATE_CHILD_SA no vuelve a generar una SA actual, se debe omitir la carga N.
- **TSi y TSr** (opcional): Muestra los selectores de tráfico para los que se crea la SA. En este caso, está entre los hosts 192.168.1.12 y 192.168.2.99.

A continuación se muestra el resultado de la depuración CREATE_CHILD_SA:

```
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 envía este paquete y espera la respuesta:

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 recibe el paquete:

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 recibe este paquete exacto de ASA2 y lo verifica:

```
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: 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 ahora genera la respuesta para el intercambio CHILD_SA. Esta es la **respuesta CREATE_CHILD_SA**. El paquete CHILD_SA normalmente contiene:

- **SA HDR**: contiene version.flags y el tipo de intercambio.
- **Nonce Ni** (opcional): Si se crea CHILD_SA como parte del intercambio inicial, no se debe enviar una segunda carga KE ni nonce.
- **Carga útil de SA**
- **KEi** (clave, opcional): la solicitud CREATE_CHILD_SA puede contener opcionalmente una carga útil KE para un intercambio DH adicional con el fin de habilitar garantías más sólidas de confidencialidad de reenvío para CHILD_SA. Si las ofertas SA incluyen diferentes grupos DH, el KEi debe ser un elemento del grupo que el iniciador espera que acepte el respondedor. Si se calcula que no es correcto, el intercambio CREATE_CHILD_SA falla y debe volver a intentarlo con una KEi diferente.
- **N** (carga útil de notificación, opcional): la carga útil de notificación se utiliza para transmitir datos informativos, como condiciones de error y transiciones de estado, a un par IKE. Una carga útil de notificación puede aparecer en un mensaje de respuesta (normalmente

especifica por qué se rechaza una solicitud), en un intercambio de información (para informar de un error que no está en una solicitud IKE) o en cualquier otro mensaje para indicar las capacidades del remitente o para modificar el significado de la solicitud. Si este intercambio CREATE_CHILD_SA regenera una SA actual distinta de IKE_SA, la carga útil de N de lead de tipo REKEY_SA debe identificar la SA que se regenera. Si este intercambio CREATE_CHILD_SA no vuelve a generar una SA actual, se debe omitir la carga N.

- **TSi y TSr (opcional):** Muestra los selectores de tráfico para los que se crea la SA. En este caso, está entre los hosts 192.168.1.12 y 192.168.2.99.

Este es el resultado de la depuración:

```
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: 140 bytes

ASA1 envía la respuesta:

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 recibe el paquete:

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 ahora verifica el paquete:

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 inserta esta entrada SA secundaria en el 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 inserta esta entrada SA secundaria en el 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
```

Verificación del túnel

Utilice la información que se proporciona en esta sección para verificar las configuraciones de túnel IPsec y del protocolo ISAKMP (Internet Security Association and Key Management Protocol).

ISAKMP

Para verificar el ISAKMP, ingrese este comando:

```
show crypto isakmp sa det
```

ASA1

Este es el resultado para ASA1:

```
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

Este es el resultado para ASA2:

```
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

Para verificar el IPSec, ingrese este comando:

```
show crypto ipsec sa
```

ASA1

Este es el resultado para ASA1:

```
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

Este es el resultado para ASA2:

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 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
```

También puede verificar el resultado del comando **show crypto ikev2 sa**, que proporciona un resultado que es idéntico al resultado del comando **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				

Información Relacionada

- [Asistencia técnica y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).