Debugs IOS IKEv2 pour le site à site VPN avec PSKs dépannant TechNote

Contenu

Introduction

Ce document décrit la version 2 (IKEv2) d'échange de clés Internet (IKE) met au point sur le Cisco IOS® quand une clé pré-partagée (PSK) est utilisée. En outre, ce document fournit des informations sur la façon dont traduire certain mettent au point des lignes dans une configuration.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de l'échange de paquet pour IKEv2. Le pour en savoir plus, se rapportent à l'échange du paquet IKEv2 et à l'élimination des imperfections de niveau de Protocol.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2 (IKEv2) d'échange de clés Internet (IKE)
- Cisco IOS 15.1(1)T ou plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Principale question

L'échange de paquet dans IKEv2 est radicalement différent de l'échange de paquet dans IKEv1. Dans IKEv1 il y avait un échange phase1 clairement délimité qui s'est composé de six (6) paquets suivis d'un échange de la phase 2 qui s'est composé de trois (3) paquets ; l'échange IKEv2 est variable. Pour plus d'informations sur les différences et une explication de l'échange de paquet, référez-vous à l'échange du paquet IKEv2 et à l'élimination des imperfections de niveau de Protocol.

Configuration du routeur

Cette section répertorie les configurations utilisées dans ce document.

Routeur 1

```
interface Loopback0
ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
ip address 172.16.0.101 255.255.255.0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel destination 10.0.0.2
tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2
!
crypto ikev2 policy site-pol
proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
peer peer1
address 10.0.0.2 255.255.255.0
hostname host1
```

```
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile IKEV2-SETUP
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local KEYRNG
lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

Routeur 2

```
crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2
!
crypto ikev2 keyring KEYRNG
peer peer2
address 10.0.0.1 255.255.255.0
hostname host2
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile IKEV2-SETUP
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local KEYRNG
lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
!
interface Loopback0
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
ip address 172.16.0.102 255.255.255.0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel destination 10.0.0.1
tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

Dépannez

Debugs de routeur

Ces commandes de débogage sont utilisées dans ce document :

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Description de message du routeur 1 (demandeur)	Debugs	Description de message de Router2 (responder)
Le routeur 1 reçoit un paquet qui apparie le crypto acl pour le pair ASA 10.0.0.2. Création d'initiés SA	* 11 novembre 20:28:34.003 : IKEv2:Got un paquet de répartiteur * 11 novembre 20:28:34.003 : IKEv2 : Traitement d'un élément outre de la file d'attente de PAK * 11 novembre 19:30:34.811 : Clé pré-partagée obtenante d'IKEv2:% par l'adresse 10.0.0.2 * 11 novembre 19:30:34.811 : Proposition PHASE1-prop IKEv2:Adding au policyle de boîte à outils * 11 novembre 19:30:34.811 : IKEv2:(1) : Choisir le profil IKEV2-SETUP d'IKE * 11 novembre 19:30:34.811 : Demande d'ikev2 SA IKEv2:New admise * 11 novembre 19:30:34.811 : Compte de négociation sortant SA IKEv2:Incrementing par un	
La première paire de messages est l'échange IKE_SA_INIT. Ces messages négocient des algorithmes de chiffrement, des nonces d'échange, et font un échange de Diffie-Hellman.	* 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement DE VEILLE : EV_INIT_SA * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement I_BLD_INIT : EV_GET_IKE_POLICY * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement I_BLD_INIT : EV_SET_POLICY * 11 novembre 19:30:34.811 : ID IKEv2:(SA = stratégies configurées par 1):Setting * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement I_BLD_INIT : EV_CHK_AUTH4PKI * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement I_BLD_INIT :	
Configuration appropriée : `cryptos ikev2 distant Cisco de pre-shared-key de Cisco de gens du pays de pre-shared-key de l'adresse Internet host1 de 10.0.0.2 255.255.255.0 d'adresse du pair peer1 du keyring ikev2 KEYRNG du groupe 2 de l'intégrité sha1 du cryptage 3des aes-cbc-128 de la`		

	EV_GEN_DH_KEY * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement I_BLD_INIT : EV_NO_EVENT * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement I_BLD_INIT : EV_OK_RECD_DH_PUBKEY_RESP * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):Action : Action_Null * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement I_BLD_INIT :
proposition PHASE1-prop crypto	EV_GET_CONFIG_MODE * 11 novembre 19:30:34.811 : Demandeur IKEv2:IKEv2 - aucune données de config à introduire l'échange IKE_SA_INIT * 11 novembre 19:30:34.811 : Données de config IKEv2:No à envoyer à la boîte à outils : * 11 novembre 19:30:34.811 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) identification de message = 00000000 CurState : Événement I_BLD_INIT : EV_BLD_MSG * 11 novembre 19:30:34.811 : Charge utile spécifique de constructeur IKEv2:Construct : DELETE-REASON * 11 novembre 19:30:34.811 : Charge utile spécifique de constructeur IKEv2:Construct : (COUTUME) * 11 novembre 19:30:34.811 : IKEv2:Construct informent la charge utile : NAT_DETECTION_SOURCE_IP * 11 novembre 19:30:34.811 : IKEv2:Construct informent la charge utile : NAT_DETECTION_DESTINATION_IP
Demandeur construisant le paquet IKE_INIT_SA. Il contient : En-tête d'ISAKMP (SPI/version/flags), SAi1 (algorithme de chiffrement que le demandeur d'IKE prend en charge), KEi (valeur principale publique CAD du demandeur), et N (Nonce de demandeur).	* 11 novembre 19:30:34.811 : **ID IKEv2:(SA =** charge utile **1):Next** : SA, version : 2.0 Type d'échange : **IKE_SA_INIT,** indicateurs : Id de message de **DEMANDEUR** : 0, longueur : 344 Contenu de charge utile : Prochaine charge utile **SA** : Le KE, réservé : 0x0, longueur : 56 dernière proposition : 0x0, réservé : 0x0, longueur : 52 Proposition : 1, id de Protocol : IKE, taille SPI : 0, #trans : le bout 5 transforment : 0x3, réservé : 0x0 : longueur : 8 type : 1, réservé : 0x0, id : 3DES dernier transformez : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96

dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id :
DH_GROUP_1024_MODP/Group 2
Prochaine charge utile du KE : N, réservé : 0x0, longueur :
136
Groupe CAD : 2, réservé : 0x0
Prochaine charge utile N : VID, réservé : 0x0, longueur :
24
Prochaine charge utile VID : VID, réservé : 0x0, longueur :
23
Prochaine charge utile VID : ANNONCEZ, avez réservé :
0x0, longueur : 21
Prochaine charge utile
NOTIFY(NAT_DETECTION_SOURCE_IP) : ANNONCEZ,
avez réservé : 0x0, longueur : 28
Id de protocole de Sécurité : IKE, taille de spi : 0, type :
NAT_DETECTION_SOURCE_IP
Prochaine charge utile
NOTIFY(NAT_DETECTION_DESTINATION_IP) : AUCUN,
réservé : 0x0, longueur : 28
Id de protocole de Sécurité : IKE, taille de spi : 0, type :
NAT_DETECTION_DESTINATION_IP
* 11 novembre 19:30:34.814 : IKEv2:Got un paquet de
répartiteur
* 11 novembre 19:30:34.814 : IKEv2:Processing un
élément outre de la file d'attente de PAK
* 11 novembre 19:30:34.814 : Demande d'ikev2 SA
IKEv2:New admise
* 11 novembre 19:30:34.814 : Compte de négociation
entrant SA IKEv2:Incrementing par un
* 11 novembre 19:30:34.814 : Charge utile IKEv2:Next :
SA, version : 2.0 Type d'échange : IKE_SA_INIT,
indicateurs : Id de message de DEMANDEUR : 0, longueur
: 344
Contenu de charge utile :
Prochaine charge utile SA : Le KE, réservé : 0x0, longueur
: 56
dernière proposition : 0x0, réservé : 0x0, longueur : 52
Proposition : 1, id de Protocol : IKE, taille SPI : 0, #trans :
le bout 5 transforment : 0x3, réservé : 0x0 : longueur : 8
type : 1, réservé : 0x0, id : 3DES
dernier transformez : 0x3, réservé : 0x0 : longueur : 12
type : 1, réservé : 0x0, id : AES-CBC
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA1
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96
dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id :
DH_GROUP_1024_MODP/Group 2
Prochaine charge utile du KE : N, réservé : 0x0, longueur :
136
Groupe CAD : 2, réservé : 0x0

Le responder reçoit IKE_INIT_SA.

Le responder initie la création SA pour ce pair.

Prochaine charge utile N : VID, réservé : 0x0, longueur : 24

* 11 novembre 19:30:34.814 : Charge utile spécifique de constructeur IKEv2:Parse : Prochaine charge utile CISCO-DELETE-REASON VID : VID, réservé : 0x0, longueur : 23
* 11 novembre 19:30:34.814 : Charge utile spécifique de constructeur IKEv2:Parse : (COUTUME) prochaine charge utile VID : ANNONCEZ, avez réservé : 0x0, longueur : 21
* 11 novembre 19:30:34.814 : IKEv2:Parse informent la charge utile : Prochaine charge utile NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) : ANNONCEZ, avez réservé : 0x0, longueur : 28
Id de protocole de Sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_SOURCE_IP
* 11 novembre 19:30:34.814 : IKEv2:Parse informent la charge utile : Prochaine charge utile NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) : AUCUN, réservé : 0x0, longueur : 28
Id de protocole de Sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_DESTINATION_IP
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement DE VEILLE : EV_RECV_INIT
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_INIT : EV_VERIFY_MSG
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_INIT : EV_INSERT_SA
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_INIT : EV_GET_IKE_POLICY
* 11 novembre 19:30:34.814 : Par défaut de proposition IKEv2:Adding à la stratégie de boîte à outils
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_INIT : EV_PROC_MSG
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message

Le responder vérifie et traite le message IKE_INIT : (1) choisit la crypto suite de ceux offertes par le demandeur, (2) calcule sa propre clé secrète CAD, et (3) il calcule une valeur de skeyid, dont toutes les clés peuvent être dérivées pour cet IKE_SA. Tout sauf les en-têtes de tous les messages qui suivent sont chiffrés et authentifiés. Les clés utilisées pour la protection de cryptage et d'intégrité sont dérivées de SKEYID et sont connues en tant que : SK_e (cryptage), SK_a (authentification),

= 00000000 CurState : Événement R_INIT :
EV_DETECT_NAT
* 11 novembre 19:30:34.814 : L'ID IKEv2:(SA = la détection
1):Process NAT annoncent
* 11 novembre 19:30:34.814 : L'ID IKEv2:(SA = les
1):Processing nat détectent le src annoncent
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = adresse
1):Remote appariés
* 11 novembre 19:30:34.814 : L'ID IKEv2:(SA = les
1):Processing nat détectent le dst annoncent
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = adresse
1):Local appariés
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = NAT 1):No
trouvés
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000000 CurState : Événement R_INIT :
EV_CHK_CONFIG_MODE
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000000 CurState : Événement R_BLD_INIT :
EV_SET_POLICY
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1) :
Établissement des stratégies configurées
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000000 CurState : Événement R_BLD_INIT :
EV_CHK_AUTH4PKI
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000000 CurState : Événement R_BLD_INIT :
EV_PKI_SESH_OPEN
* 11 novembre 19:30:34.814 : ID IKEv2:(SA = 1):Opening
une session de PKI
* 11 novembre 19:30:34.815 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000000 CurState : Événement R_BLD_INIT :
EV_GEN_DH_KEY
* 11 novembre 19:30:34.815 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000000 CurState : Événement R_BLD_INIT :
EV_NO_EVENT
* 11 novembre 19:30:34.815 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000000 CurState : Événement R_BLD_INIT :
EV_OK_RECD_DH_PUBKEY_RESP

SK_d est dérivé et utilisé pour la dérivation du matériel plus loin de base pour CHILD_SAs, et un SK_e et un SK_a distincts est calculé pour chaque direction.

Configuration appropriée : `cryptos ikev2 distant Cisco de pre-shared-key de Cisco de gens du pays de pre-shared-key de l'adresse Internet host2 de 10.0.0.1 255.255.255.0 d'adresse du pair peer2 du keyring ikev2 KEYRNG du groupe 2 de l'intégrité sha1 du cryptage 3des aes-cbc-128 de la proposition PHASE1-prop crypto`

* 11 novembre 19:30:34.815 : ID IKEv2:(SA = 1):Action : Action_Null
* 11 novembre 19:30:34.815 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_BLD_INIT : **EV_GEN_DH_SECRET**
* 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_BLD_INIT : EV_NO_EVENT
* 11 novembre 19:30:34.822 : **Clé pré-partagée obtenante d'**IKEv2:% **par l'adresse 10.0.0.1**
* 11 novembre 19:30:34.822 : Par défaut de proposition IKEv2:Adding à la stratégie de boîte à outils
* 11 novembre 19:30:34.822 : IKEv2:(2) : Choisir le profil IKEV2-SETUP d'IKE
* 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_BLD_INIT : EV_OK_RECD_DH_SECRET_RESP
* 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):Action : Action_Null
* 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_BLD_INIT : **EV_GEN_SKEYID**
* 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1) : **Générez le skeyid**
* 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_BLD_INIT : EV_GET_CONFIG_MODE
* 11 novembre 19:30:34.822 : Responder IKEv2:IKEv2 - aucune données de config à introduire l'échange IKE_SA_INIT
* 11 novembre 19:30:34.822 : Données de config IKEv2:No à envoyer à la boîte à outils :
* 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_BLD_INIT : EV_BLD_MSG
* 11 novembre 19:30:34.822 : Charge utile spécifique de constructeur IKEv2:Construct : DELETE-REASON
* 11 novembre 19:30:34.822 : Charge utile spécifique de constructeur IKEv2:Construct : (COUTUME)
* 11 novembre 19:30:34.822 : IKEv2:Construct informent la charge utile : NAT_DETECTION_SOURCE_IP

* 11 novembre 19:30:34.822 : IKEv2:Construct informent la charge utile : NAT_DETECTION_DESTINATION_IP * 11 novembre 19:30:34.822 : IKEv2:Construct informent la charge utile : HTTP_CERT_LOOKUP_SUPPORTED * 11 novembre 19:30:34.822 : ID IKEv2:(SA = charge utile 1):Next : SA, version : 2.0 Type d'échange : **IKE_SA_INIT,** indicateurs : Id de message du **RESPONDER MSG-RESPONSE** : 0, longueur : 449 Contenu de charge utile : Prochaine charge utile **SA** : Le KE, réservé : 0x0, longueur : 48 dernière proposition : 0x0, réservé : 0x0, longueur : 44 Proposition : 1, id de Protocol : IKE, taille SPI : 0, #trans : le bout 4 transforment : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernier transformez : 0x0, réservé : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Group 2 Prochaine charge utile du **KE** : N, réservé : 0x0, longueur : 136 Groupe CAD : 2, réservé : 0x0 Prochaine charge utile **N** : VID, réservé : 0x0, longueur : 24 Prochaine charge utile VID : VID, réservé : 0x0, longueur : 23 Prochaine charge utile VID : ANNONCEZ, avez réservé : 0x0, longueur : 21 Prochaine charge utile NOTIFY(NAT_DETECTION_SOURCE_IP) : ANNONCEZ, avez réservé : 0x0, longueur : 28 Id de protocole de Sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_SOURCE_IP Prochaine charge utile NOTIFY(NAT_DETECTION_DESTINATION_IP) : CERTREQ, réservé : 0x0, longueur : 28 Id de protocole de Sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_DESTINATION_IP Prochaine charge utile CERTREQ : ANNONCEZ, avez réservé : 0x0, longueur : 105 Informations parasites de codage de CERT et URL de PKIX Prochaine charge utile NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) : AUCUN, réservé : 0x0, longueur : 8 Id de protocole de Sécurité : IKE, taille de spi : 0, type : HTTP_CERT_LOOKUP_SUPPORTED	Le Router2 établit le message de responder pour l'échange IKE_SA_INIT, qui est reçu par ASA1. Ce paquet contient : En-tête d'ISAKMP (version/indicateurs SPI/), algorithme SAr1(cryptographique le responder d'IKE choisit), KEr (valeur principale publique CAD du responder), et Nonce de responder.
* 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message	Le Router2 envoie le message de responder au

	= 00000000 CurState : Événement INIT_DONE : EV_DONE * 11 novembre 19:30:34.822 : L'ID IKEv2:(SA = le 1):Cisco DeleteReason Notify est activé * 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement INIT_DONE : EV_CHK4_ROLE * 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement INIT_DONE : **EV_START_TMR** * 11 novembre 19:30:34.822 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement R_WAIT_AUTH : EV_NO_EVENT * 11 novembre 19:30:34.822 : IKEv2 : **Nouvelle demande d'ikev2 SA admise** * 11 novembre 19:30:34.822 : IKEv2 : **Incrémentation du compte de négociation sortant SA par un**		routeur 1.
Le routeur 1 reçoit le paquet de réponse IKE_SA_INIT du Router2.	* 11 novembre 19:30:34.823 : IKEv2:Got un paquet de répartiteur * 11 novembre 19:30:34.823 : IKEv2:Got un paquet de répartiteur * 11 novembre 19:30:34.823 : IKEv2:Processing un élément outre de la file d'attente de PAK	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000000 CurState : Événement INIT_DONE : **EV_START_TMR**	Le responder met en marche le temporisateur pour le processus authentique.
Router1 vérifie et traite la réponse : (1) la clé secrète CAD de demandeur est calculée, et (2) le skeyid de demandeur est également généré.	* 11 novembre 19:30:34.823 : ID IKEv2:(SA = charge utile 1):Next : SA, version : 2.0 Type d'échange : IKE_SA_INIT, indicateurs : Id de message du **RESPONDER MSG-RESPONSE** : 0, longueur : 449 Contenu de charge utile : Prochaine charge utile **SA** : Le KE, réservé : 0x0, longueur : 48 dernière proposition : 0x0, réservé : 0x0, longueur : 44 Proposition : 1, id de Protocol : IKE, taille SPI : 0, #trans : le bout 4 transforment : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernier transformez : 0x0, réservé : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Group 2		

Prochaine charge utile du KE : N, réservé : 0x0, longueur : 136
Groupe CAD : 2, réservé : 0x0
Prochaine charge utile N : VID, réservé : 0x0, longueur : 24

* 11 novembre 19:30:34.823 : Charge utile spécifique de constructeur IKEv2:Parse : Prochaine charge utile CISCO-DELETE-REASON VID : VID, réservé : 0x0, longueur : 23

* 11 novembre 19:30:34.823 : Charge utile spécifique de constructeur IKEv2:Parse : (COUTUME) prochaine charge utile VID : ANNONCEZ, avez réservé : 0x0, longueur : 21

* 11 novembre 19:30:34.823 : IKEv2:Parse informent la charge utile : Prochaine charge utile NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) : ANNONCEZ, avez réservé : 0x0, longueur : 28
Id de protocole de Sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_SOURCE_IP

* 11 novembre 19:30:34.824 : IKEv2:Parse informent la charge utile : Prochaine charge utile NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) : CERTREQ, réservé : 0x0, longueur : 28
Id de protocole de Sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_DESTINATION_IP
Prochaine charge utile CERTREQ : ANNONCEZ, avez réservé : 0x0, longueur : 105
Informations parasites de codage de CERT et URL de PKIX

* 11 novembre 19:30:34.824 : IKEv2:Parse informent la charge utile : Prochaine charge utile HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) : AUCUN, réservé : 0x0, longueur : 8
Id de protocole de Sécurité : IKE, taille de spi : 0, type : HTTP_CERT_LOOKUP_SUPPORTED
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement I_WAIT_INIT : EV_RECV_INIT
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = message 1):Processing IKE_SA_INIT
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement I_PROC_INIT : EV_CHK4_NOTIFY

* 11 novembre 19:30:34.824 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000000 CurState : Événement I_PROC_INIT :
EV_VERIFY_MSG
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000000 CurState : Événement I_PROC_INIT :
EV_PROC_MSG
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000000 CurState : Événement I_PROC_INIT :
EV_DETECT_NAT
* 11 novembre 19:30:34.824 : L'ID IKEv2:(SA = la détection
1):Process NAT annoncent
* 11 novembre 19:30:34.824 : L'ID IKEv2:(SA = les
1):Processing nat détectent le src annoncent
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = adresse
1):Remote appariés
* 11 novembre 19:30:34.824 : L'ID IKEv2:(SA = les
1):Processing nat détectent le dst annoncent
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = adresse
1):Local appariés
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = NAT 1):No
trouvés
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000000 CurState : Événement I_PROC_INIT :
EV_CHK_NAT_T
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000000 CurState : Événement I_PROC_INIT :
EV_CHK_CONFIG_MODE
* 11 novembre 19:30:34.824 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000000 CurState : Événement INIT_DONE :
EV_GEN_DH_SECRET
* 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000000 CurState : Événement INIT_DONE :
EV_NO_EVENT
* 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000000 CurState : Événement INIT_DONE :
EV_OK_RECD_DH_SECRET_RESP
* 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):Action :

	Action_Null * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement INIT_DONE : **EV_GEN_SKEYID** * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1) : **Générez le skeyid** * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement INIT_DONE : EV_DONE * 11 novembre 19:30:34.831 : L'ID IKEv2:(SA = le 1):Cisco DeleteReason Notify est activé * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement INIT_DONE : EV_CHK4_ROLE * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement I_BLD_AUTH : EV_GET_CONFIG_MODE * 11 novembre 19:30:34.831 : Données de config IKEv2:Sending à la boîte à outils * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement I_BLD_AUTH : EV_CHK_EAP
L'échange des débuts IKE_AUTH de demandeur et génère la charge utile d'authentification. Le paquet IKE_AUTH contient : En-tête d'ISAKMP (version/indicateurs SPI/), IDI (l'identité du demandeur), charge utile AUTHENTIQUE, SAi2(initiates le SA-semblable à l'échange de jeu de transformations de la phase 2 dans IKEv1), et TSi et TSr (le demandeur	* 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement I_BLD_AUTH : **EV_GEN_AUTH** * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement I_BLD_AUTH : EV_CHK_AUTH_TYPE * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement I_BLD_AUTH : EV_OK_AUTH_GEN * 11 novembre 19:30:34.831 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000000 CurState : Événement I_BLD_AUTH : EV_SEND_AUTH * 11 novembre 19:30:34.831 : Charge utile spécifique de

et le responder trafiquent des sélecteurs) : Ils contiennent l'adresse source et de destination du demandeur et du responder respectivement pour expédier/recevant le trafic chiffré. La plage d'adresses spécifie que toute trafique à et de cette plage est percée un tunnel. Si la proposition semble acceptable au responder, elle renvoie les charges utiles identiques de SOLIDES TOTAUX. Le premier CHILD_SA est créé pour la paire de proxy_ID qui apparie le paquet de déclencheur.

Configuration appropriée : `les SOLIDES TOTAUX de set transform-set du crypto ipsec profile phse2-prof d'ESP-SHA-hmac des SOLIDES TOTAUX esp-3des de crypto ipsec transform-set ont placé ikev2-profile IKEV2-SETUP`

constructeur IKEv2:Construct : CISCO-GRANITE
* 11 novembre 19:30:34.831 : IKEv2:Construct informent la charge utile : INITIAL_CONTACT
* 11 novembre 19:30:34.831 : IKEv2:Construct informent la charge utile : SET_WINDOW_SIZE
* 11 novembre 19:30:34.831 : IKEv2:Construct informent la charge utile : ESP_TFC_NO_SUPPORT
* 11 novembre 19:30:34.831 : IKEv2:Construct informent la charge utile : NON_FIRST_FRAGS
Contenu de charge utile :
Prochaine charge utile VID : IDI, réservée : 0x0, longueur : 20
Prochaine charge utile **IDI** : AUTHENTIQUE, réservé : 0x0, longueur : 12
Type d'id : Ipv4 addres, réservé : 0x0 0x0
Prochaine charge utile **AUTHENTIQUE** : CFG, réservé : 0x0, longueur : 28
Méthode authentique PSK, réservée : 0x0, 0x0 réservé
Prochaine charge utile **CFG** : SA, réservée : 0x0, longueur : 309
type de cfg : CFG_REQUEST, réservé : 0x0, réservé : 0x0
* 11 novembre 19:30:34.831 : Prochaine charge utile SA : **TSi**, réservé : 0x0, longueur : 40
dernière proposition : 0x0, réservé : 0x0, longueur : 36
Proposition : 1, id de Protocol : L'ESP, taille SPI : 4, #trans : le bout 3 transforment : 0x3, réservé : 0x0 : longueur : 8
type : 1, réservé : 0x0, id : 3DES
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96
dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 5, réservé : 0x0, id : N'utilisez pas ESN
Prochaine charge utile de **TSi** : TSr, réservé : 0x0, longueur : 24
Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé
Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, longueur : 16
port de début : 0, port de fin : 65535
adr de début : 0.0.0.0, adr de fin : 255.255.255.255
Prochaine charge utile de **TSr** : ANNONCEZ, avez réservé : 0x0, longueur : 24
Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé
Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, longueur : 16
port de début : 0, port de fin : 65535
adr de début : 0.0.0.0, adr de fin : 255.255.255.255
Prochaine charge utile NOTIFY(INITIAL_CONTACT) : ANNONCEZ, avez réservé : 0x0, longueur : 8
Id de protocole de Sécurité : IKE, taille de spi : 0, type : INITIAL_CONTACT
Prochaine charge utile NOTIFY(SET_WINDOW_SIZE) :

ANNONCEZ, avez réservé : 0x0, longueur : 12
Id de protocole de Sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE
Prochaine charge utile NOTIFY(ESP_TFC_NO_SUPPORT) : ANNONCEZ, avez réservé : 0x0, longueur : 8
Id de protocole de Sécurité : IKE, taille de spi : 0, type : ESP_TFC_NO_SUPPORT
Prochaine charge utile NOTIFY(NON_FIRST_FRAGS) : AUCUN, réservé : 0x0, longueur : 8
Id de protocole de Sécurité : IKE, taille de spi : 0, type : NON_FIRST_FRAGS

* 11 novembre 19:30:34.832 : ID IKEv2:(SA = charge utile 1):Next : ENCR, version : 2.0 Type d'échange : **IKE_AUTH**, indicateurs : Id de message de **DEMANDEUR** : 1, longueur : 556
Contenu de charge utile :
Prochaine charge utile ENCR : VID, réservé : 0x0, longueur : 528

* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 **CurState :** Événement **I_WAIT_AUTH** : EV_NO_EVENT
* 11 novembre 19:30:34.832 : IKEv2:Got un paquet de répartiteur
* 11 novembre 19:30:34.832 : IKEv2:Processing un élément outre de la file d'attente de PAK
* 11 novembre 19:30:34.832 : L'ID IKEv2:(SA = le 1):Request a le mess_id 1 ; 1 prévu à 1
* 11 novembre 19:30:34.832 : **ID IKEv2:(SA =** charge utile **1):Next** : ENCR, version : 2.0 Type d'échange : **IKE_AUTH**, indicateurs : Id de message de **DEMANDEUR** : 1, longueur : 556
Contenu de charge utile :
* 11 novembre 19:30:34.832 : Charge utile spécifique de constructeur IKEv2:Parse : (COUTUME) prochaine charge utile VID : IDI, réservée : 0x0, longueur : 20
Prochaine charge utile **IDI** : AUTHENTIQUE, réservé : 0x0, longueur : 12
Type d'id : Ipv4 addres, réservé : 0x0 0x0
Prochaine charge utile **AUTHENTIQUE** : CFG, réservé : 0x0, longueur : 28
Méthode authentique PSK, réservée : 0x0, 0x0 réservé
Prochaine charge utile **CFG** : SA, réservée : 0x0, longueur : 309
type de cfg : CFG_REQUEST, réservé : 0x0, réservé : 0x0
* 11 novembre 19:30:34.832 : type d'attrib : DN IP4 internes, longueur : 0
* 11 novembre 19:30:34.832 : type d'attrib : DN IP4 internes, longueur : 0

Le Router2 reçoit et vérifie les données d'authentification reçues du routeur 1.
Configuration appropriée : `crypto MD5 de l'intégrité sha-1 de l'ESP de protocole du cryptage aes-256 de l'ESP de protocole de l'ipsec-proposition AES256 de l'ipsec ikev2`

* 11 novembre 19:30:34.832 : type d'attrib : IP4 interne NBNS, longueur : 0 * 11 novembre 19:30:34.832 : type d'attrib : IP4 interne NBNS, longueur : 0 * 11 novembre 19:30:34.832 : type d'attrib : sous-réseau IP4 interne, longueur : 0 * 11 novembre 19:30:34.832 : type d'attrib : version d'application, longueur : 257 type d'attrib : Inconnu - 28675, longueur : 0 * 11 novembre 19:30:34.832 : type d'attrib : Inconnu - 28672, longueur : 0 * 11 novembre 19:30:34.832 : type d'attrib : Inconnu - 28692, longueur : 0 * 11 novembre 19:30:34.832 : type d'attrib : Inconnu - 28681, longueur : 0 * 11 novembre 19:30:34.832 : type d'attrib : Inconnu - 28674, longueur : 0 * 11 novembre 19:30:34.832 : Prochaine charge utile **SA** : TSi, réservé : 0x0, longueur : 40 dernière proposition : 0x0, réservé : 0x0, longueur : 36 Proposition : 1, id de Protocol : L'ESP, taille SPI : 4, #trans : le bout 3 transforment : 0x3, réservé : 0x0 : longueur : 8 type : 1, réservé : 0x0, id : 3DES dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernier transformez : 0x0, réservé : 0x0 : longueur : 8 type : 5, réservé : 0x0, id : N'utilisez pas ESN Prochaine charge utile de **TSi** : TSr, réservé : 0x0, longueur : 24 Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, longueur : 16 port de début : 0, port de fin : 65535 adr de début : 0.0.0.0, adr de fin : 255.255.255.255 Prochaine charge utile de **TSr** : ANNONCEZ, avez réservé : 0x0, longueur : 24 Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, longueur : 16 port de début : 0, port de fin : 65535 adr de début : 0.0.0.0, adr de fin : 255.255.255.255	
* 11 novembre 19:30:34.832 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH : EV_RECV_AUTH * 11 novembre 19:30:34.832 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH :	Le Routeur2 établit la réponse au paquet IKE_AUTH qu'elle a reçu du routeur 1. Ce paquet de réponse contient : En-tête d'ISAKMP (version/indicateurs

EV_CHK_NAT_T
* 11 novembre 19:30:34.832 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH : EV_PROC_ID
* 11 novembre 19:30:34.832 : ID IKEv2:(SA = parameteres 1):Received valides dans l'identificateur de processus
* 11 novembre 19:30:34.832 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH : EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
* 11 novembre 19:30:34.832 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH : EV_GET_POLICY_BY_PEERID
* 11 novembre 19:30:34.833 : IKEv2:(1) : Choisir le profil IKEV2-SETUP d'IKE
* 11 novembre 19:30:34.833 : Clé pré-partagée obtenante d'IKEv2:% par l'adresse 10.0.0.1
* 11 novembre 19:30:34.833 : Clé pré-partagée obtenante d'IKEv2:% par l'adresse 10.0.0.1
* 11 novembre 19:30:34.833 : Par défaut de proposition IKEv2:Adding à la stratégie de boîte à outils
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = profil 'IKEV2-SETUP 1):Using IKEv2
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH : EV_SET_POLICY
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = stratégies configurées par 1):Setting
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH : EV_VERIFY_POLICY_BY_PEERID
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH : EV_CHK_AUTH4EAP
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_WAIT_AUTH : EV_CHK_POLREQEAP
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B

SPI/), différence interdécile (l'identité du responder), charge utile AUTHENTIQUE, SAr2(initiates le SA-semblable à l'échange de jeu de transformations de la phase 2 dans IKEv1), et TSi et TSr (le demandeur et le responder trafiquent des sélecteurs). Ils contiennent l'adresse source et de destination du demandeur et du responder respectivement pour expédier/recevant le trafic chiffré. La plage d'adresses spécifie que toute trafique à et de cette plage est percée un tunnel. Ces paramètres sont identiques à celui qui ont été reçus d'ASA1.

R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_CHK_AUTH_TYPE
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_GET_PRESHR_KEY
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_VERIFY_AUTH
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_CHK4_IC
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_CHK_REDIRECT
* 11 novembre 19:30:34.833 : L'ID IKEv2:(SA = le contrôle 1):Redirect n'est pas nécessaire, l'ignorant
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_NOTIFY_AUTH_DONE
* 11 novembre 19:30:34.833 : L'autorisation de groupe IKEv2:AAA n'est pas configurée
* 11 novembre 19:30:34.833 : L'autorisation d'utilisateur IKEv2:AAA n'est pas configurée
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_CHK_CONFIG_MODE
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_SET_RECD_CONFIG_MODE
* 11 novembre 19:30:34.833 : Données de config IKEv2:Received de boîte à outils :
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_PROC_SA_TS
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B

R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_VERIFY_AUTH : EV_GET_CONFIG_MODE
* 11 novembre 19:30:34.833 : IKEv2:Error construisant la réponse de config
* 11 novembre 19:30:34.833 : Données de config IKEv2:No à envoyer à la boîte à outils :
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_BLD_AUTH : EV_MY_AUTH_METHOD
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_BLD_AUTH : EV_GET_PRESHR_KEY
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_BLD_AUTH : EV_GEN_AUTH
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_BLD_AUTH : EV_CHK4_SIGN
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_BLD_AUTH : EV_OK_AUTH_GEN
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement R_BLD_AUTH : EV_SEND_AUTH
* 11 novembre 19:30:34.833 : Charge utile spécifique de constructeur IKEv2:Construct : CISCO-GRANITE
* 11 novembre 19:30:34.833 : IKEv2:Construct informent la charge utile : SET_WINDOW_SIZE
* 11 novembre 19:30:34.833 : IKEv2:Construct informent la charge utile : ESP_TFC_NO_SUPPORT
* 11 novembre 19:30:34.833 : IKEv2:Construct informent la charge utile : NON_FIRST_FRAGS
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = charge utile 1):Next : ENCR, version : 2.0 Type d'échange : **IKE_AUTHENTIC**, indicateurs : Id de message du **RESPONDER MSG-RESPONSE** : 1, longueur : 252 Contenu de charge utile :
Prochaine charge utile **ENCR** : VID, réservé : 0x0, longueur : 224
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-

Le responder envoie la réponse pour IKE_AUTH.

> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000001 CurState : Événement AUTH_DONE : EV_OK
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):Action :
Action_Null
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000001 CurState : Événement AUTH_DONE :
EV_PKI_SESH_CLOSE
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):Closing la
session de PKI
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000001 CurState : Événement AUTH_DONE :
EV_UPDATE_CAC_STATS
* 11 novembre 19:30:34.833 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000001 CurState : Événement AUTH_DONE :
EV_INSERT_IKE
* 11 novembre 19:30:34.834 : Index ikev2 1 MIB
IKEv2:Store, plate-forme 60
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000001 CurState : Événement AUTH_DONE :
EV_GEN_LOAD_IPSEC
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = demande
1):Asynchronous alignés
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1) :
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) identification de message
= 00000001 CurState : Événement **AUTH_DONE** :
EV_NO_EVENT

Le demandeur reçoit la réponse du responder.

* 11 novembre 19:30:34.834 : IKEv2:Got un paquet de répartiteur

* 11 novembre 19:30:34.834 : IKEv2:Processing un élément outre de la file d'attente de PAK

* 11 novembre 19:30:34.840 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement AUTH_DONE : EV_OK_RECD_LOAD_IPSEC
* 11 novembre 19:30:34.840 : ID IKEv2:(SA = 1):Action : Action_Null
* 11 novembre 19:30:34.840 : ID IKEv2:(SA = 1):SM

Le responder insère une entrée dans le TRISTE.

Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C 4 (r) identification de message = 00000001 CurState : Événement AUTH_DONE : EV_START_ACCT
* 11 novembre 19:30:34.840 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C 4 (r) identification de message = 00000001 CurState : Événement AUTH_DONE : EV_CHECK_DUPE
* 11 novembre 19:30:34.840 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C 4 (r) identification de message = 00000001 CurState : Événement AUTH_DONE : EV_CHK4_ROLE

* 11 novembre 19:30:34.834 : ID IKEv2:(SA = charge utile 1):Next : ENCR, version : 2.0 Type d'échange : **IKE_AUTH**, indicateurs : Id de message du **RESPONDER MSG-RESPONSE** : 1, longueur : 252
Contenu de charge utile :

* 11 novembre 19:30:34.834 : Charge utile spécifique de constructeur IKEv2:Parse : (COUTUME) prochaine charge utile VID : Différence interdécile, réservée : 0x0, longueur : 20

Le routeur 1 vérifie et traite les données d'authentification en ce paquet. Le routeur 1 insère alors cette SA dans son TRISTE.

Prochaine charge utile **différence interdécile** : AUTHENTIQUE, réservé : 0x0, longueur : 12
Type d'id : Ipv4 addres, réservé : 0x0 0x0
Prochaine charge utile **AUTHENTIQUE** : SA, réservée : 0x0, longueur : 28
Méthode authentique PSK, réservée : 0x0, 0x0 réservé
Prochaine charge utile **SA** : TSi, réservé : 0x0, longueur : 40
dernière proposition : 0x0, réservé : 0x0, longueur : 36
Proposition : 1, id de Protocol : L'ESP, taille SPI : 4, #trans : le bout 3 transforment : 0x3, réservé : 0x0 : longueur : 8
type : 1, réservé : 0x0, id : 3DES
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96

dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 5, réservé : 0x0, id : N'utilisez pas ESN
Prochaine charge utile de **TSi** : TSr, réservé : 0x0, longueur : 24
Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé
Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, longueur : 16
port de début : 0, port de fin : 65535
adr de début : 0.0.0.0, adr de fin : 255.255.255.255
Prochaine charge utile de **TSr** : ANNONCEZ, avez réservé : 0x0, longueur : 24
Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé
Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, longueur : 16
port de début : 0, port de fin : 65535
adr de début : 0.0.0.0, adr de fin : 255.255.255.255

* 11 novembre 19:30:34.834 : IKEv2:Parse informent la charge utile : Prochaine charge utile SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) : ANNONCEZ, avez réservé : 0x0, longueur : 12
Id de protocole de Sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE

* 11 novembre 19:30:34.834 : IKEv2:Parse informent la charge utile : Prochaine charge utile ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) : ANNONCEZ, avez réservé : 0x0, longueur : 8
Id de protocole de Sécurité : IKE, taille de spi : 0, type : ESP_TFC_NO_SUPPORT

* 11 novembre 19:30:34.834 : IKEv2:Parse informent la charge utile : Prochaine charge utile NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) : AUCUN, réservé : 0x0, longueur : 8
Id de protocole de Sécurité : IKE, taille de spi : 0, type : NON_FIRST_FRAGS

* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_WAIT_AUTH : **EV_RECV_AUTH**
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):Action : Action_Null
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_CHK4_NOTIFY

* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_PROC_MSG
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_GET_POLICY_BY_PEERID
* 11 novembre 19:30:34.834 : Proposition PHASE1-prop IKEv2:Adding à la stratégie de boîte à outils
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = profil 'IKEV2-SETUP 1):Using IKEv2
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_VERIFY_POLICY_BY_PEERID
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_CHK_AUTH_TYPE
* 11 novembre 19:30:34.834 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_GET_PRESHR_KEY
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_VERIFY_AUTH
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_CHK_EAP
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement I_PROC_AUTH : EV_NOTIFY_AUTH_DONE
* 11 novembre 19:30:34.835 : L'autorisation de groupe IKEv2:AAA n'est pas configurée
* 11 novembre 19:30:34.835 : L'autorisation d'utilisateur

IKEv2:AAA n'est pas configurée
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement I_PROC_AUTH :
EV_CHK_CONFIG_MODE
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement I_PROC_AUTH :
EV_CHK4_IC
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement I_PROC_AUTH :
EV_CHK_IKE_ONLY
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement I_PROC_AUTH :
EV_PROC_SA_TS
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement AUTH_DONE : EV_OK
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):Action :
Action_Null
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement AUTH_DONE :
EV_PKI_SESH_CLOSE
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):Closing la
session de PKI
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement AUTH_DONE :
EV_UPDATE_CAC_STATS
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement AUTH_DONE :
EV_INSERT_IKE
* 11 novembre 19:30:34.835 : Index ikev2 1 MIB
IKEv2:Store, plate-forme 60
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-
> SA : I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) identification de message
= 00000001 CurState : Événement AUTH_DONE :
EV_GEN_LOAD_IPSEC
* 11 novembre 19:30:34.835 : ID IKEv2:(SA = demande
1):Asynchronous alignés

	* 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1) : * 11 novembre 19:30:34.835 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement AUTH_DONE : EV_NO_EVENT * 11 novembre 19:30:34.835 : Message 8 IKEv2:KMI consommé. Aucune mesure prise. * 11 novembre 19:30:34.835 : Message 12 IKEv2:KMI consommé. Aucune mesure prise. * 11 novembre 19:30:34.835 : Données IKEv2:No à introduire le positionnement de config de mode. * 11 novembre 19:30:34.841 : Le traitement 0x80000002 d'ident IKEv2:Adding a associé avec SPI 0x9506D414 pour la session 8 * 11 novembre 19:30:34.841 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement AUTH_DONE : EV_OK_RECD_LOAD_IPSEC * 11 novembre 19:30:34.841 : ID IKEv2:(SA = 1):Action : Action_Null * 11 novembre 19:30:34.841 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement AUTH_DONE : EV_START_ACCT * 11 novembre 19:30:34.841 : ID IKEv2:(SA = 1):Accounting non requis * 11 novembre 19:30:34.841 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement AUTH_DONE : EV_CHECK_DUPE * 11 novembre 19:30:34.841 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement **AUTH_DONE** : EV_CHK4_ROLE		
Le tunnel est sur le demandeur et le showsREADY d'état.	* 11 novembre 19:30:34.841 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : **READYEvent** : EV_CHK_IKE_ONLY * 11 novembre 19:30:34.841 : ID IKEv2:(SA = 1):SM Trace-> SA :	* 11 novembre 19:30:34.840 : ID IKEv2:(SA = 1):SM Trace-> SA : I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement **PRÊT** : EV_R_OK * 11 novembre 19:30:34.840 : ID IKEv2:(SA = 1):SM Trace-> SA :	Le tunnel est sur le responder. Le tunnel de responder monte habituellement avant le demandeur.

I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) identification de message = 00000001 CurState : Événement PRÊT : EV_I_OK	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) identification de message = 00000001 CurState : Événement PRÊT : EV_NO_EVENT

Debugs CHILD_SA

Cet échange se compose d'une seule paire de demande/réponse et a été mentionné comme un échange de la phase 2 dans IKEv1. Il pourrait être initié par l'un ou l'autre de fin de l'IKE_SA après que les échanges initiaux soient terminés.

Description de message du routeur 1 CHILD_SA	Debugs	Description de message du Router2 CHILD_SA
Le routeur 1 initie l'échange CHILD_SA. C'est la demande CREATE_CHILD_SA. Le paquet CHILD_SA contient typiquement : • SA HDR (version.flags/type d'échange) • Ni de Nonce (facultatif) : Si le CHILD_SA est créé en tant qu'élément de l'échange initial, une deuxième charge utile et le nonce du KE ne doivent pas être envoyés) • Charge utile SA • KEi (Clé-facultatif) : La demande CREATE_CHILD_SA pourrait sur option contenir une	* 11 novembre 19:31:35.873 : IKEv2:Got un paquet de répartiteur * 11 novembre 19:31:35.873 : IKEv2:Processing un élément outre de la file d'attente de PAK * 11 novembre 19:31:35.873 : L'ID IKEv2:(SA = le 2):Request a le mess_id 3 ; 3 à 7 prévus * 11 novembre 19:31:35.873 : ID IKEv2:(SA = charge utile 2):Next : ENCR, version : 2.0 **Type d'échange : CREATE_CHILD_SA**, indicateurs : Id de message de **DEMANDEUR** : 3, longueur : 396 Contenu de charge utile : Prochaine charge utile **SA** : N, réservé : 0x0, longueur : 152 dernière proposition : 0x0, réservé : 0x0, longueur : 148 Proposition : 1, id de Protocol : IKE, taille SPI : 8, #trans : le bout 15 transforment : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernier transformez : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernier transformez : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA512 dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA384 dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA256 dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernier transformez : 0x3, réservé : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : MD5 dernier transformez : 0x3, réservé : 0x0 : longueur : 8	

charge utile du KE pour qu'un échange supplémentaire CAD active des garanties plus fortes de forward secrecy pour le CHILD_SA. Si les offres SA incluent différents groupes CAD, KEi doit être un élément du groupe que le demandeur s'attend à ce que le responder reçoive. S'il devine mal, l'échange CREATE_CHILD_SA échoue, et il devra relancer avec un KEi différent

type : 3, réservé : 0x0, id : SHA512
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA384
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA256
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : MD596
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id : DH_GROUP_1536_MODP/Group 5
dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Group 2
Prochaine charge utile **N** : Le KE, réservé : 0x0, longueur : 24
Prochaine charge utile du **KE** : ANNONCEZ, avez réservé : 0x0, longueur : 136
Groupe CAD : 2, réservé : 0x0

* 11 novembre 19:31:35.874 : IKEv2:Parse informent la charge utile : Prochaine charge utile SET_WINDOW_SIZE **NOTIFY(SET_WINDOW_SIZE)** : AUCUN, réservé : 0x0, longueur : 12
Id de protocole de Sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE

* 11 novembre 19:31:35.874 : IKEv2 : (**ID SA = 2):SM** Trace-> SA : I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement PRÊT : **EV_RECV_CREATE_CHILD**
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):Action : Action_Null
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_INIT : EV_RECV_CREATE_CHILD
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):Action : Action_Null
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_INIT : EV_VERIFY_MSG
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_INIT : EV_CHK_CC_TYPE
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM

- N (informez charge utile-facultatif). La charge utile de notification, est utilisée pour transmettre des données informationnelles, telles que des conditions d'erreurs et des transitions d'état, à un pair d'IKE. Une charge utile de notification peut apparaître

dans un message de réponse (spécifiant habituellement pourquoi une demande a été rejetée), dans un échange INFORMATIONNEL (pour signaler une erreur pas dans une demande d'IKE), ou dans n'importe quel autre message pour indiquer des capacités d'expéditeur ou pour modifier la signification de la demande. Si cet échange CREATE_CHILD_SA réintroduit SA existante autre que l'IKE_SA, la principale charge utile N du type REKEY_SA DOIT identifier SA étant réintroduite. Si cet échange CREATE_CHILD_SA ne réintroduit pas SA existante, la charge utile N DOIT être omise.

Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_IKE : **EV_REKEY_IKESA**
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_IKE : EV_GET_IKE_POLICY
* 11 novembre 19:31:35.874 : **Clé pré-partagée obtenante d'**IKEv2:% **par l'adresse 10.0.0.2**
* 11 novembre 19:31:35.874 : Clé pré-partagée obtenante d'IKEv2:% par l'adresse 10.0.0.2
* 11 novembre 19:31:35.874 : Proposition PHASE1-prop IKEv2:Adding à la stratégie de boîte à outils
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = profil 'IKEV2-SETUP 2):Using IKEv2
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_IKE : EV_PROC_MSG
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_IKE : EV_SET_POLICY
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2) : **Établissement des stratégies configurées**
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : EV_GEN_DH_KEY
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : EV_NO_EVENT
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : EV_OK_RECD_DH_PUBKEY_RESP
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):Action : Action_Null
* 11 novembre 19:31:35.874 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : **EV_GEN_DH_SECRET**
* 11 novembre 19:31:35.881 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6

R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : EV_NO_EVENT
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : EV_OK_RECD_DH_SECRET_RESP
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):Action : Action_Null
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : EV_BLD_MSG
* 11 novembre 19:31:35.882 : **IKEv2:Construct informent la charge utile** : SET_WINDOW_SIZE
Contenu de charge utile :
Prochaine charge utile **SA** : N, réservé : 0x0, longueur : 56
dernière proposition : 0x0, réservé : 0x0, longueur : 52
Proposition : 1, id de Protocol : IKE, taille SPI : 8, #trans : le bout 4 transforment : 0x3, réservé : 0x0 : longueur : 12
type : 1, réservé : 0x0, id : AES-CBC
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA1
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96
dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Group 2
Prochaine charge utile **N** : Le KE, réservé : 0x0, longueur : 24
Prochaine charge utile du **KE** : ANNONCEZ, avez réservé : 0x0, longueur : 136
Groupe CAD : 2, réservé : 0x0
Prochaine charge utile **NOTIFY(SET_WINDOW_SIZE)** : AUCUN, réservé : 0x0, longueur : 12
Id de protocole de Sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE
* 11 novembre 19:31:35.869 : IKEv2 : (**ID SA =** charge utile **2):Next** : ENCR, version : 2.0 Type d'échange : **CREATE_CHILD_SA**, indicateurs : Id de message de **DEMANDEUR** : 2, longueur : 460
Contenu de charge utile :
Prochaine charge utile ENCR : SA, réservée : 0x0, longueur : 432
* 11 novembre 19:31:35.873 : IKEv2:Construct informent la charge utile : SET_WINDOW_SIZE
Contenu de charge utile :
Prochaine charge utile **SA** : N, réservé : 0x0, longueur : 152
dernière proposition : 0x0, réservé : 0x0, longueur : 148
Proposition : 1, id de Protocol : IKE, taille SPI : 8, #trans :

Ce paquet est reçu par Router2.

le bout 15 transforment : 0x3, réservé : 0x0 : longueur : 12
type : 1, réservé : 0x0, id : AES-CBC
dernier transformez : 0x3, réservé : 0x0 : longueur : 12
type : 1, réservé : 0x0, id : AES-CBC
dernier transformez : 0x3, réservé : 0x0 : longueur : 12
type : 1, réservé : 0x0, id : AES-CBC
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA512
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA384
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA256
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA1
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : MD5
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA512
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA384
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA256
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : MD596
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id :
DH_GROUP_1536_MODP/Group 5
dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id :
DH_GROUP_1024_MODP/Group 2
Prochaine charge utile **N** : Le KE, réservé : 0x0, longueur :
24
Prochaine charge utile du **KE** : ANNONCEZ, avez réservé :
0x0, longueur : 136
Groupe CAD : 2, réservé : 0x0
Prochaine charge utile **NOTIFY(SET_WINDOW_SIZE)** :
AUCUN, réservé : 0x0, longueur : 12
Id de protocole de Sécurité : IKE, taille de spi : 0, type :
SET_WINDOW_SIZE
* 11 novembre 19:31:35.882 : IKEv2 : (**ID SA =** charge utile **2):Next** : ENCR, version : 2.0 Type d'échange : **CREATE_CHILD_SA,** indicateurs : Id de message du **RESPONDER MSG-RESPONSE** : 3, longueur : 300
Contenu de charge utile :
Prochaine charge utile **SA** : N, réservé : 0x0, longueur : 56
dernière proposition : 0x0, réservé : 0x0, longueur : 52
Proposition : 1, id de Protocol : IKE, taille SPI : 8, #trans :
le bout 4 transforment : 0x3, réservé : 0x0 : longueur : 12
type : 1, réservé : 0x0, id : AES-CBC
dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA1

Le Router2 établit maintenant la réponse pour l'échange CHILD_SA. C'est la réponse CREATE_CHILD_SA. Le paquet CHILD_SA contient typiquement :

- SA HDR (version.flags/t

dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96
dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Group 2
Prochaine charge utile **N** : Le KE, réservé : 0x0, longueur : 24
Prochaine charge utile du **KE** : ANNONCEZ, avez réservé : 0x0, longueur : 136
Groupe CAD : 2, réservé : 0x0

* 11 novembre 19:31:35.882 : IKEv2:Parse informent la charge utile : Prochaine charge utile SET_WINDOW_SIZE **NOTIFY(SET_WINDOW_SIZE)** : AUCUN, réservé : 0x0, longueur : 12
Id de protocole de Sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE

* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement **CHILD_I_WAIT** : **EV_RECV_CREATE_CHILD**
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):Action : Action_Null
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement **CHILD_I_PROC** : EV_CHK4_NOTIFY
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_PROC : **EV_VERIFY_MSG**
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_PROC : EV_PROC_MSG
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_PROC : EV_CHK4_PFS
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_PROC : EV_GEN_DH_SECRET
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message

ype d'échange)
- Nonce Ni(optional) : Si le CHILD_SA est créé en tant qu'élément de l'échange initial, une deuxième charge utile et le nonce du KE ne doivent pas être envoyés.
- Charge utile SA
- KEi (Clé-facultatif) : La demande CREATE_CHILD_SA pourrait sur option contenir une charge utile du KE pour qu'un échange supplémentaire CAD active des garanties plus fortes de forward secrecy pour le CHILD_SA. Si les offres SA incluent différents groupes CAD, KEi doit être un élément du groupe que le demandeur s'attend à ce que le responder reçoive. S'il devine mal, l'échange CREATE_CHIL

= 00000003 CurState : Événement CHILD_I_PROC : EV_NO_EVENT
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_PROC : EV_OK_RECD_DH_SECRET_RESP
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):Action : Action_Null
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_PROC : EV_CHK_IKE_REKEY
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_PROC : EV_GEN_SKEYID
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = skeyid 2):Generate
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement **CHILD_I_DONE : EV_ACTIVATE_NEW_SA**
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_DONE : EV_UPDATE_CAC_STATS
* 11 novembre 19:31:35.890 : Demande d'ikev2 SA IKEv2:New lancée
* 11 novembre 19:31:35.890 : IKEv2:Failed pour décrémenter le compte pour la négociation sortante
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_DONE : EV_CHECK_DUPE
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement CHILD_I_DONE : EV_OK
* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 CurState : Événement de SORTIE : EV_CHK_PENDING
* 11 novembre 19:31:35.890 : L'ID IKEv2:(SA = la réponse 2):Processed avec l'id de message 3, des demandes peuvent être envoyés de la plage 4 à 8

D_SA échoue, et il doit relancer avec un KEi différent.

- N (informez charge utile-facultatif) : La charge utile de notification est utilisée pour transmettre des données informationnelles, telles que des conditions d'erreurs et des transitions d'état, à un pair d'IKE. Une charge utile de notification pourrait apparaître dans un message de réponse (spécifiant habituellement pourquoi une demande a été rejetée), dans un échange informationnel (pour signaler une erreur pas dans une demande d'IKE), ou dans n'importe quel autre message pour indiquer des capacités d'expéditeur ou pour modifier la signification de la

		demande. Si cet échange CREATE_CHILD_SA réintroduit SA existante autre que l'IKE_SA, la principale charge utile N du type REKEY_SA doit identifier SA étant réintroduite. Si cet échange CREATE_CHILD_SA ne réintroduit pas SA existante, la charge utile N doit être omise.
	* 11 novembre 19:31:35.890 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) identification de message = 00000003 **CurState :** Événement de **SORTIE** : EV_NO_EVENT	Le Router2 envoie la réponse et se termine lançant nouvel ENFANT SA.
	* 11 novembre 19:31:35.882 : ID IKEv2:(SA = charge utile 2):Next : ENCR, version : 2.0 Type d'échange : **CREATE_CHILD_SA**, indicateurs : Id de message du **RESPONDER MSG-RESPONSE** : 3, longueur : 300 Contenu de charge utile : Prochaine charge utile ENCR : SA, réservée : 0x0, longueur : 272	
Le routeur 1 reçoit le paquet de réponse du Router2 et se termine lançant le CHILD_SA.	* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : **EV_CHK_IKE_REKEY** * 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_BLD_MSG : EV_GEN_SKEYID * 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2) : **Générez le skeyid** * 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message	

= 00000003 CurState : Événement CHILD_R_DONE : EV_ACTIVATE_NEW_SA
* 11 novembre 19:31:35.882 : Index ikev2 3 MIB IKEv2:Store, plate-forme 62
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_DONE : EV_UPDATE_CAC_STATS
* 11 novembre 19:31:35.882 : Demande d'ikev2 SA IKEv2:New lancée
* 11 novembre 19:31:35.882 : IKEv2:Failed pour décrémenter le compte pour la négociation entrante
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_DONE : EV_CHECK_DUPE
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_DONE : EV_OK
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement CHILD_R_DONE : EV_START_DEL_NEG_TMR
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):Action : Action_Null
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement de SORTIE : EV_CHK_PENDING
* 11 novembre 19:31:35.882 : L'ID IKEv2:(SA = la réponse 2):Sent avec l'id de message 3, des demandes peuvent être la plage reçue 4 8
* 11 novembre 19:31:35.882 : ID IKEv2:(SA = 2):SM Trace-> SA : I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) identification de message = 00000003 CurState : Événement de SORTIE : EV_NO_EVENT

Vérification de tunnel

ISAKMP

Commande

show crypto ikev2 sa detailed

Routeur 1 sorti

```
Router1#show crypto ikev2 sa  detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.0.1/500 10.0.0.2/500 none/none READY
Encr: AES-CBC, keysize: 128,
Hash: SHA96, DH Grp:2,
Auth sign: PSK, Auth verify: PSK
Life/Active Time: 120/10 sec
CE id: 1006, Session-id: 4
Status Description: Negotiation done
Local spi: E58F925107F8B73F Remote spi: AFD098F4147869DA
Local id: 10.0.0.1
Remote id: 10.0.0.2
Local req msg id: 2 Remote req msg id: 0
Local next msg id: 2 Remote next msg id: 0
Local req queued: 2 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

Sortie de Router2

```
Router2#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 10.0.0.2/500 10.0.0.1/500 none/none READY
Encr: AES-CBC, keysize: 128, Hash: SHA96,
DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 120/37 sec
CE id: 1006, Session-id: 4
Status Description: Negotiation done
Local spi: AFD098F4147869DA Remote spi: E58F925107F8B73F
Local id: 10.0.0.2
Remote id: 10.0.0.1
Local req msg id: 0 Remote req msg id: 2
Local next msg id: 0 Remote next msg id: 2
Local req queued: 0 Remote req queued: 2
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

IPsec

Commande

show crypto ipsec sa

> Remarque: Dans cette sortie, à la différence de dans IKEv1, la valeur de groupe CAD de PFS apparaît en tant que « PFS (Y/N) : N, groupe CAD : aucun » pendant la première négociation de tunnel, mais, après qu'un rekey se produise, les bonnes valeurs n'apparaît. Ce n'est pas une bogue, quoique le comportement soit décrit dans l'ID de bogue Cisco CSCug67056.

La différence entre IKEv1 et IKEv2 est que, dans ce dernier, l'enfant SAS sont créés en tant qu'élément de l'échange AUTHENTIQUE lui-même. Le groupe configuré CAD sous le crypto map serait utilisé seulement pendant le rekey. Par conséquent, vous verriez le « PFS (Y/N) : N, groupe CAD : aucun » jusqu'au premier rekey.

Avec IKEv1, vous voyez un comportement différent, parce que la création d'enfant SA se produit pendant le mode rapide, et le message CREATE_CHILD_SA a une disposition de porter la charge utile de Key Exchange qui spécifie les paramètres CAD pour dériver un nouveau secret partagé.

Routeur 1 sorti

```
Router1#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0,
local addr 10.0.0.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt:
10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt:
10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.0.1,
remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xF6083ADD(4127734493)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x6B74CB79(1802816377)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 18, flow_id: SW:18,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec):
(4276853/3592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF6083ADD(4127734493)
```

```
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 17, flow_id: SW:17,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key
lifetime (k/sec): (4276853/3592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Sortie de Router2

```
Router2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.0.2,
remote crypto endpt.: 10.0.0.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x6B74CB79(1802816377)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xF6083ADD(4127734493)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 17, flow_id: SW:17,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime
(k/sec): (4347479/3584)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x6B74CB79(1802816377)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 18, flow_id: SW:18,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
```

```
sa timing: remaining key
lifetime (k/sec): (4347479/3584)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Vous pouvez également vérifier la sortie de l'ordre de **show crypto session** sur les deux Routeurs ; cette sortie affiche l'état de session de tunnel comme UP-ACTIVE.

```
Router1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map

Router2#show cry session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map
```

Informations connexes

- Échange du paquet IKEv2 et élimination des imperfections de niveau de Protocol
- Support et documentation techniques - Cisco Systems