Dépannage des débogages IKEv2 IOS pour VPN site à site avec PSK

Table des matières

Introduction

Ce document décrit les débogages d'Internet Key Exchange version 2 (IKEv2) sur Cisco IOS® lorsqu'une clé non partagée (PSK) est utilisée.

Conditions préalables

Exigences

Cisco vous recommande de connaître l'échange de paquets pour IKEv2. Pour plus d'informations, référez-vous à Échange de paquets IKEv2 et débogage au niveau du protocole.

Composants utilisés

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

- Internet Key Exchange Version 2 (IKEv2)
- Cisco IOS 15.1(1)T ou version ultérieure

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

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

Informations générales

Ce document fournit des informations sur la façon de traduire certaines lignes de débogage dans une configuration.

Problème principal

L'échange de paquets dans IKEv2 est radicalement différent de l'échange de paquets dans IKEv1. Dans IKEv1, il y avait un échange de phase 1 clairement délimité qui se composait de six (6) paquets, puis d'un échange de phase 2 qui se composait de trois (3) paquets ; l'échange IKEv2 est variable. Pour plus d'informations sur les différences et une explication de l'échange de paquets, référez-vous à Échange de paquets IKEv2 et débogage au niveau du protocole.

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
```

Dépannage

Débogages du routeur

Les commandes debug suivantes sont utilisées dans ce document :

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

Description du message Router 1 (Initiator)	Déboguages	Descrip messa route (répon
Le routeur 1 reçoit un paquet qui correspond à la liste de contrôle d'accès cryptée pour l'homologue ASA 10.0.0.2. Initie la création SA	*Nov 11 20:28:34.003: IKEv2:Réception d'un paquet du répartiteur *Nov 11 20:28:34.003: IKEv2:Traitement d'un élément hors de la file d'attente de pak *Nov 11 19:30:34.811: IKEv2:% Obtention de la clé pré-partagée par adresse 10.0.0.2 *Nov 11 19:30:34.811: IKEv2:Ajout de la proposition PHASE1-prop à la stratégie de boîte à outils *Nov 11 19:30:34.811: IKEv2:(1): Choix du profil IKE IKEV2-SETUP *Nov 11 19:30:34.811: IKEv2:Nouvelle requête d'IKEv2 sa admise *Nov 11 19:30:34.811: IKEv2:Incrémentation du nombre de SSA de négociation sortante par 1	
La première paire de messages est l'échange IKE_SA_INIT. Ces messages négocient des algorithmes cryptographiques, échangent des nonces et	*Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState : IDLE Event: EV_INIT_SA *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState : I_BLD_INIT Événement : EV_GET_IKE_POLICY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event:EV_SET_POLICY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):Définition des stratégies configurées *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA:	

effectuent un échange Diffie-Hellman. Configuration appropriée : `crypto ikev2 proposition PHASE1-prop encryption 3des aes-cbc-128 intégrité sha1 groupe 2crypto 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`	I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState : I_BLD_INIT Événement : EV_CHK_AUTH4PKI *11 nov. 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event:EV_GEN_DH_KEY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_NO_EVENT *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState : I_BLD_INIT Événement : EV_OK_RECD_DH_PUBKEY_RESP *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):Action: Action_Null *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState : I_BLD_INIT Événement : EV_GET_CONFIG_MODE *Nov 11 19:30:34.811: IKEv2:IKEv2 initiator - aucune donnée de configuration à envoyer dans IKE_SA_INIT exch *Nov 11 19:30:34.811: IKEv2:Aucune donnée de configuration à envoyer à la boîte à outils : *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState : I_BLD_INIT Événement : EV_BLD_MSG *Nov 11 19:30:34.811: IKEv2:Charge utile spécifique au constructeur de construction: DELETE-REASON *Nov 11 19:30:34.811: IKEv2:Construct Vendor Specific Payload: (CUSTOM) *Nov 11 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP	
Initiateur créant le paquet IKE_INIT_SA. Il contient : l'en-tête ISAKMP (SPI/version/flags), SAi1 (algorithme cryptographique pris en charge par l'initiateur IKE), KEi (valeur de clé publique DH de l'initiateur) et N (nom de l'initiateur).	*Nov 11 19:30:34.811: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Type d'échange : IKE_SA_INIT, indicateurs : INITIATOR ID de message : 0, longueur : 344 Contenu de la charge utile : SA Charge utile suivante : KE, réservée : 0x0, longueur : 56 dernière proposition : 0x0, réservée : 0x0, longueur : 52 Proposition : 1, ID de protocole : IKE, taille SPI : 0, #trans : 5 dernière transformation : 0x3, réservé : 0x0 : longueur : 8 type : 1, réservé : 0x0, id : 3DES dernière transformation : 0x3, réservée : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x0, réservée : 0x0 : longueur : 8	

	type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Groupe 2 KE Charge utile suivante : N, réservée : 0x0, longueur : 136 Groupe DH : 2, Réservé : 0x0 N Charge utile suivante : VID, réservé : 0x0, longueur : 24 VID Charge utile suivante : VID, réservé : 0x0, longueur : 23 VID Charge utile suivante : NOTIFY, réservé : 0x0, longueur : 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 28 ID de protocole de sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Charge utile suivante : AUCUNE, réservée : 0x0, longueur : 28 ID de protocole de sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_DESTINATION_IP	
----------L'initiateur a envoyé IKE_INIT_SA ---------->		
	*Nov 11 19:30:34.814: IKEv2:Réception d'un paquet du répartiteur *Nov 11 19:30:34.814: IKEv2:Traitement d'un élément hors de la file d'attente de pak *Nov 11 19:30:34.814: IKEv2:Nouvelle requête d'IKEv2 sa admise *Nov 11 19:30:34.814: IKEv2:Incrémentation d'un pour le nombre de SA de négociation entrante	Le répon reçoit IKE_INIT
	*Nov 11 19:30:34.814: IKEv2:Next payload: SA, version: 2.0 Type d'échange : IKE_SA_INIT, indicateurs : INITIATOR ID de message : 0, longueur : 344 Contenu de la charge utile : SA Charge utile suivante : KE, réservée : 0x0, longueur : 56 dernière proposition : 0x0, réservée : 0x0, longueur : 52 Proposition : 1, ID de protocole : IKE, taille SPI : 0, #trans : 5 dernière transformation : 0x3, réservé : 0x0 : longueur : 8 type : 1, réservé : 0x0, id : 3DES dernière transformation : 0x3, réservée : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Groupe 2 KE Charge utile suivante : N, réservée : 0x0, longueur : 136 Groupe DH : 2, Réservé : 0x0 N Charge utile suivante : VID, réservé : 0x0, longueur : 24 *Nov 11 19:30:34.814: IKEv2:Analyser la charge utile spécifique au	Le répon lance la c de SA po homologu

	fournisseur: CISCO-DELETE-REASON VID Charge utile suivante : VID, réservé: 0x0, longueur: 23 *Nov 11 19:30:34.814: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Prochaine charge utile : NOTIFY, réservé : 0x0, longueur : 21 *Nov 11 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Prochaine charge utile : NOTIFY, réservé : 0x0, longueur : 28 ID de protocole de sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Prochaine charge utile : NONE, réservé : 0x0, longueur : 28 ID de protocole de sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_DESTINATION_IP	
	*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: IDLE Event:EV_RECV_INIT *11 nov. 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:EV_VERIFY_MSG *11 nov. 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:EV_INSERT_SA *11 nov. 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:EV_GET_IKE_POLICY *Nov 11 19:30:34.814: IKEv2:Ajout de la proposition par défaut à la stratégie de boîte à outils *11 nov. 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:EV_PROC_MSG *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_INIT Événement : EV_DETECT_NAT *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Process NAT discovery notify *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Traitement de la détection NAT src notify *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):Adresse distante correspondante *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Traitement de la détection nat dst notify *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):Adresse locale correspondante	Le répon vérifie et message IKE_INIT choisit la cryptage celles off l'initiateur calcule sa clé secrè (3) calcul valeur sk partir de toutes les peuvent é dérivées cette IKE Tous les de tous le message suivent s chiffrés e authentifi l'exceptio en-têtes. utilisées cryptage protection

	*Nov 11 19:30:34.814: IKEv2:(ID SA = 1):NAT introuvable *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_INIT Événement : EV_CHK_CONFIG_MODE *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Événement : EV_SET_POLICY *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Définition des stratégies configurées *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Événement : EV_CHK_AUTH4PKI *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Événement : EV_PKI_SESH_OPEN *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):Ouverture d'une session PKI *11 nov. 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:EV_GEN_DH_KEY *Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Événement : EV_NO_EVENT *11 nov. 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Event:EV_OK_RECD_DH_PUBKEY_RESP *Nov 11 19:30:34.815: IKEv2:(ID SA = 1):Action: Action_Null *11 nov. 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:EV_GEN_DH_SECRET *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Événement : EV_NO_EVENT *Nov 11 19:30:34.822: IKEv2:% Obtention de la clé pré-partagée par l'adresse 10.0.0.1 *Nov 11 19:30:34.822: IKEv2:Ajout de la proposition par défaut à la stratégie de boîte à outils *Nov 11 19:30:34.822: IKEv2:(2): Choix du profil IKE IKEV2-SETUP *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Événement : EV_OK_RECD_DH_SECRET_RESP *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):Action: Action_Null *11 nov. 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =	l'intégrité dérivées SKEYID connues nom de : (cryptage (authentif SK_d est et utilisée dérivation matériel cryptage suppléme pour CHI et un SK_ SK_a sép sont calcu chaque d Configura appropri : crypto i propositi PHASE1-pr encryptio aes-cbc-1 intégrité groupe 2 ikev2 key KEYRNG pe address 1 255.255.2 hostname pre-share local cis shared-ke cisco

	00000000 CurState: R_BLD_INIT Event:EV_GEN_SKEYID *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Generate skeyid *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Événement : EV_GET_CONFIG_MODE *Nov 11 19:30:34.822: IKEv2:IKEv2 responder - aucune donnée de configuration à envoyer dans IKE_SA_INIT exch *Nov 11 19:30:34.822: IKEv2:Aucune donnée de configuration à envoyer à la boîte à outils : *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_BLD_INIT Événement : EV_BLD_MSG *Nov 11 19:30:34.822: IKEv2:Charge utile spécifique au constructeur de construction: DELETE-REASON *Nov 11 19:30:34.822: IKEv2:Construct Vendor Specific Payload: (CUSTOM) *Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP *Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED	
	*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Type d'échange : IKE_SA_INIT, indicateurs : RESPONDER MSG-RESPONSE ID de message : 0, longueur : 449 Contenu de la charge utile : SA Charge utile suivante : KE, réservée : 0x0, longueur : 48 dernière proposition : 0x0, réservée : 0x0, longueur : 44 Proposition : 1, ID de protocole : IKE, taille SPI : 0, #trans : 4 dernière transformation : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Groupe 2 KE Charge utile suivante : N, réservée : 0x0, longueur : 136 Groupe DH : 2, Réservé : 0x0 N Charge utile suivante : VID, réservé : 0x0, longueur : 24 VID Charge utile suivante : VID, réservé : 0x0, longueur : 23 VID Charge utile suivante : NOTIFY, réservé : 0x0, longueur : 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 28	Le routeu génère le message répondeu l'échange IKE_SA_ est reçu p ASA1. Ce contient : ISAKMP Header(S version/fl SAr1(algo cryptogra choisi par répondeu KEr(DH p Key value responde Respond Nonce.

	ID de protocole de sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Charge utile suivante : CERTREQ, réservé : 0x0, longueur : 28 ID de protocole de sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_DESTINATION_IP CHARGE UTILE CERTREQ suivante : NOTIFY, réservée : 0x0, longueur : 105 Codage de certificat Hachage et URL de PKIX NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Charge utile suivante : AUCUNE, réservée : 0x0, longueur : 8 ID de protocole de sécurité : IKE, taille de spi : 0, type : HTTP_CERT_LOOKUP_SUPPORTED		
	*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : INIT_DONE Événement : EV_DONE *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Cisco DeleteReason Notify est activé *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : INIT_DONE Événement : EV_CHK4_ROLE *11 nov. 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Event:EV_START_TMR. *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : R_WAIT_AUTH Événement : EV_NO_EVENT *Nov 11 19:30:34.822: IKEv2:Nouvelle requête IKEv2 sa admise *Nov 11 19:30:34.822: IKEv2:Incrémentation du nombre de messages sortants de négociation par 1		Le routeu envoie le message réponse a routeur 1
<----------Le répondeur a envoyé IKE_INIT_SA ----------			
Le routeur 1 reçoit le paquet de réponse IKE_SA_INIT du routeur 2.	*Nov 11 19:30:34.823: IKEv2:Réception d'un paquet du répartiteur *Nov 11 19:30:34.823: IKEv2:Réception d'un paquet du répartiteur *Nov 11 19:30:34.823: IKEv2:Traitement d'un élément hors de la file d'attente de pak	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState : INIT_DONE, événement : EV_START_TMR	Le répon démarre minuteur processu

Le routeur 1 vérifie et traite la réponse : (1) la clé secrète DH de l'initiateur est calculée et (2) l'ID de clé DH de l'initiateur est également généré.	*Nov 11 19:30:34.823: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Type d'échange : IKE_SA_INIT, indicateurs : RESPONDER MSG-RESPONSE ID de message : 0, longueur : 449 Contenu de la charge utile : SA Charge utile suivante : KE, réservée : 0x0, longueur : 48 dernière proposition : 0x0, réservée : 0x0, longueur : 44 Proposition : 1, ID de protocole : IKE, taille SPI : 0, #trans : 4 dernière transformation : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Groupe 2 KE Charge utile suivante : N, réservée : 0x0, longueur : 136 Groupe DH : 2, Réservé : 0x0 N Charge utile suivante : VID, réservé : 0x0, longueur : 24 *Nov 11 19:30:34.823: IKEv2:Analyser la charge utile spécifique au fournisseur: CISCO-DELETE-REASON VID Charge utile suivante : VID, réservé: 0x0, longueur: 23 *Nov 11 19:30:34.823: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Prochaine charge utile : NOTIFY, réservé : 0x0, longueur : 21 *Nov 11 19:30:34.823: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Prochaine charge utile : NOTIFY, réservé : 0x0, longueur : 28 ID de protocole de sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.824: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Prochaine charge utile : CERTREQ, réservée : 0x0, longueur : 28 ID de protocole de sécurité : IKE, taille de spi : 0, type : NAT_DETECTION_DESTINATION_IP CHARGE UTILE CERTREQ suivante : NOTIFY, réservée : 0x0, longueur : 105 Codage de certificat Hachage et URL de PKIX *Nov 11 19:30:34.824: IKEv2:Parse Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED	

NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Prochaine charge utile : AUCUNE, réservée : 0x0, longueur : 8
ID de protocole de sécurité : IKE, taille de spi : 0, type : HTTP_CERT_LOOKUP_SUPPORTED

*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : I_WAIT_INIT Événement : EV_RECV_INIT
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Traitement du message IKE_SA_INIT
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_CHK4_NOTIFY
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_VERIFY_MSG
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_PROC_MSG
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_DETECT_NAT
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Process NAT discovery notify
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Traitement de la détection NAT src notify
*Nov 11 19:30:34.824: IKEv2:(ID SA = 1):Adresse distante correspondante
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Traitement de la détection nat dst notify
*Nov 11 19:30:34.824: IKEv2:(ID SA = 1):Adresse locale correspondante
*Nov 11 19:30:34.824: IKEv2:(ID SA = 1):NAT introuvable
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : I_PROC_INIT Événement : EV_CHK_NAT_T
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Event: EV_CHK_CONFIG_MODE
*11 nov. 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event:EV_GEN_DH_SECRET
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_NO_EVENT
*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : INIT_DONE Event:

	EV_OK_RECD_DH_SECRET_RESP *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):Action: Action_Null *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : INIT_DONE Event:EV_GEN_SKEYID *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):Generate skeyid *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : INIT_DONE Événement : EV_DONE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):Cisco DeleteReason Notify est activé *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : INIT_DONE Événement : EV_CHK4_ROLE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : I_BLD_AUTH Événement : EV_GET_CONFIG_MODE *Nov 11 19:30:34.831: IKEv2:Envoi des données de configuration à la boîte à outils *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : I_BLD_AUTH Événement : EV_CHK_EAP	
L'initiateur démarre l'échange IKE_AUTH et génère la charge utile d'authentification. Le paquet IKE_AUTH contient : l'en-tête ISAKMP (SPI/ version/flags), IDi (identité de l'initiateur), la charge utile AUTH, SAi2 (initie le SA-similaire à l'échange d'ensemble de transformation de phase 2 dans IKEv1), et TSi et	*11 nov. 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event:EV_GEN_AUTH *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : I_BLD_AUTH Événement : EV_CHK_AUTH_TYPE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : I_BLD_AUTH Événement : EV_OK_AUTH_GEN *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState : I_BLD_AUTH Événement : EV_SEND_AUTH *Nov 11 19:30:34.831: IKEv2:Construct Vendor Specific Payload: CISCO-GRANITE *Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: INITIAL_CONTACT *Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *Nov 11 19:30:34.831: IKEv2:Construct Notify Payload:	

TSr (sélecteurs de trafic de l'initiateur et du répondeur). Ils contiennent l'adresse source et l'adresse de destination de l'initiateur et du répondeur, respectivement, pour l'acheminement/la réception du trafic chiffré. La plage d'adresses indique que tout le trafic en provenance et à destination de cette plage est tunnellisé. Si la proposition est acceptable pour le répondeur, il renvoie des données utiles TS identiques. La première CHILD_SA est créée pour la paire proxy_ID qui correspond au paquet déclencheur. Configuration appropriée : `crypto ipsec transform-set TS esp-3des esp-sha-hmac crypto ipsec profile phase2-prof set transform-set TS set ikev2-profile IKEV2-SETUP`	NON_FIRST_FRAGS Contenu de la charge utile : VID Charge utile suivante : IDi, réservée : 0x0, longueur : 20 IDi Charge utile suivante : AUTH, réservée : 0x0, longueur : 12 Type d'ID : adresse IPv4, Réservé : 0x0 0x0 AUTH Charge utile suivante : CFG, réservée : 0x0, longueur : 28 Méthode d'authentification PSK, réservée : 0x0, réservée 0x0 CFG Charge utile suivante : SA, réservée : 0x0, longueur : 309 cfg type : CFG_REQUEST, réservé : 0x0, réservé : 0x0 *Nov 11 19:30:34.831: SA Prochaine charge utile : TSi, réservée : 0x0, longueur : 40 dernière proposition : 0x0, réservée : 0x0, longueur : 36 Proposition : 1, ID de protocole : ESP, taille SPI : 4, #trans : 3 dernière transformation : 0x3, réservé : 0x0 : longueur : 8 type : 1, réservé : 0x0, id : 3DES dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 5, réservé : 0x0, id : Ne pas utiliser ESN TSi Charge utile suivante : TSr, réservée : 0x0, longueur : 24 Nombre de services techniques : 1, réservé 0x0, réservé 0x0 Type TS : TS_IPV4_ADDR_RANGE, ID de protocole : 0, longueur : 16 port de début : 0, port de fin : 65535 adresse de début : 0.0.0.0, adresse de fin : 255.255.255.255 TSr Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 24 Nombre de services techniques : 1, réservé 0x0, réservé 0x0 Type TS : TS_IPV4_ADDR_RANGE, ID de protocole : 0, longueur : 16 port de début : 0, port de fin : 65535 adresse de début : 0.0.0.0, adresse de fin : 255.255.255.255 NOTIFY(INITIAL_CONTACT) Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 8 ID de protocole de sécurité : IKE, taille de spi : 0, type : INITIAL_CONTACT NOTIFY(SET_WINDOW_SIZE) Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 12 ID de protocole de sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE NOTIFY(ESP_TFC_NO_SUPPORT) Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 8 ID de protocole de sécurité : IKE, taille spi : 0, type : ESP_TFC_NO_SUPPORT NOTIFY(NON_FIRST_FRAGS) Charge utile suivante : AUCUNE, réservée : 0x0, longueur : 8 ID de protocole de sécurité : IKE, taille de spi : 0, type :	

	NON_FIRST_FRAGS *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Type d'échange : IKE_AUTH, indicateurs : INITIATOR ID de message : 1, longueur : 556 Contenu de la charge utile : ENCR Charge utile suivante : VID, réservé : 0x0, longueur : 528 *11 nov. 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 CurState : I_WAIT_AUTH Événement : EV_NO_EVENT	
----------L'initiateur a envoyé IKE_AUTH ---------->		
	*Nov 11 19:30:34.832: IKEv2:Réception d'un paquet du répartiteur *Nov 11 19:30:34.832: IKEv2:Traitement d'un élément hors de la file d'attente de pak *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):La demande a mess_id 1 ; attendu de 1 à 1 *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Type d'échange : IKE_AUTH, indicateurs : INITIATOR ID de message : 1, longueur : 556 Contenu de la charge utile : *Nov 11 19:30:34.832: IKEv2:Analyser la charge utile spécifique au fournisseur: (PERSONNALISÉ) VID Charge utile suivante : IDi, réservée: 0x0, longueur: 20 IDi Charge utile suivante : AUTH, réservée : 0x0, longueur : 12 Type d'ID : adresse IPv4, Réservé : 0x0 0x0 AUTH Charge utile suivante : CFG, réservée : 0x0, longueur : 28 Méthode d'authentification PSK, réservée : 0x0, réservée 0x0 CFG Charge utile suivante : SA, réservée : 0x0, longueur : 309 cfg type : CFG_REQUEST, réservé : 0x0, réservé : 0x0 *Nov 11 19:30:34.832: type d'attrib : DNS IP4 interne, longueur : 0 *Nov 11 19:30:34.832: type d'attrib : DNS IP4 interne, longueur : 0 *Nov 11 19:30:34.832: type d'attrib : NBNS IP4 interne, longueur : 0 *Nov 11 19:30:34.832: type d'attrib : NBNS IP4 interne, longueur : 0 *Nov 11 19:30:34.832: type d'attribut : sous-réseau IP4 interne, longueur : 0 *Nov 11 19:30:34.832: type d'attrib : version de l'application, longueur : 257 type d'attrib : inconnu - 28675, longueur : 0 *Nov 11 19:30:34.832: type d'attrib : Inconnu - 28672, longueur : 0 *Nov 11 19:30:34.832: type d'attrib : Inconnu - 28692, longueur : 0 *Nov 11 19:30:34.832: type d'attrib : Inconnu - 28681, longueur : 0 *Nov 11 19:30:34.832: type d'attrib : Inconnu - 28674, longueur : 0 *Nov 11 19:30:34.832: SA Charge utile suivante : TSi, réservé : 0x0,	Le routeu reçoit et v données d'authent reçues du 1. Configura appropri crypto ip ikev2 ips propositi AES256 pr esp encry aes-256 p esp integ sha-1 md5

	longueur : 40 dernière proposition : 0x0, réservée : 0x0, longueur : 36 Proposition : 1, ID de protocole : ESP, taille SPI : 4, #trans : 3 dernière transformation : 0x3, réservé : 0x0 : longueur : 8 type : 1, réservé : 0x0, id : 3DES dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 5, réservé : 0x0, id : Ne pas utiliser ESN TSi Charge utile suivante : TSr, réservée : 0x0, longueur : 24 Nombre de services techniques : 1, réservé 0x0, réservé 0x0 Type TS : TS_IPV4_ADDR_RANGE, ID de protocole : 0, longueur : 16 port de début : 0, port de fin : 65535 adresse de début : 0.0.0.0, adresse de fin : 255.255.255.255 TSr Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 24 Nombre de services techniques : 1, réservé 0x0, réservé 0x0 Type TS : TS_IPV4_ADDR_RANGE, ID de protocole : 0, longueur : 16 port de début : 0, port de fin : 65535 adresse de début : 0.0.0.0, adresse de fin : 255.255.255.255	
	*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_RECV_AUTH *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_CHK_NAT_T *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_PROC_ID *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Reçu des paramètres valides dans l'ID de processus *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_GET_POLICY_BY_PEERID *Nov 11 19:30:34.833: IKEv2:(1): Choix du profil IKE IKEV2-SETUP *Nov 11 19:30:34.833: IKEv2:% Obtention de la clé pré-partagée par l'adresse 10.0.0.1 *Nov 11 19:30:34.833: IKEv2:% Obtention de la clé pré-partagée par l'adresse 10.0.0.1 *Nov 11 19:30:34.833: IKEv2:Ajout de la proposition par défaut à la	Le routeu génère la réponse paquet IKE_AUT reçu du r Ce paque réponse ISAKMP Header(S version/fl IDr.(respo identity), payload, SAr2(initi similaire l'échange d'ensemb transform phase 2 IKEv1), e TSr(Initia Sélecteu de répon contienne l'adresse

	stratégie de boîte à outils *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Utilisation du profil IKEv2 'IKEV2-SETUP' *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_SET_POLICY *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Définition des stratégies configurées *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_VERIFY_POLICY_BY_PEERID *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_CHK_AUTH4EAP *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_WAIT_AUTH Événement : EV_CHK_POLREQEAP *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_CHK_AUTH_TYPE *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_GET_PRESHR_KEY *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_VERIFY_AUTH *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_CHK4_IC *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_CHK_REDIRECT *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):La vérification de redirection n'est pas nécessaire, elle est ignorée *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_NOTIFY_AUTH_DONE *Nov 11 19:30:34.833: L'autorisation de groupe IKEv2:AAA n'est pas configurée	et l'adres destinatio l'initiateu répondeu respectiv pour l'achemin réception chiffré. La d'adresse indique q le trafic e provenan destinatio cette plag tunnelisé paramètr identique qui a été ASA1.

*Nov 11 19:30:34.833: L'autorisation utilisateur IKEv2:AAA n'est pas configurée
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_SET_RECD_CONFIG_MODE
*Nov 11 19:30:34.833: IKEv2:Données de configuration reçues de la boîte à outils :
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_PROC_SA_TS
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_VERIFY_AUTH Événement : EV_GET_CONFIG_MODE
*Nov 11 19:30:34.833: IKEv2:Erreur de construction de la réponse de configuration
*Nov 11 19:30:34.833: IKEv2:Aucune donnée de configuration à envoyer à la boîte à outils :
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_BLD_AUTH Événement : EV_MY_AUTH_METHOD
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_BLD_AUTH Événement : EV_GET_PRESHR_KEY
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_BLD_AUTH Événement : EV_GEN_AUTH
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_BLD_AUTH Événement : EV_CHK4_SIGN
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_BLD_AUTH Événement : EV_OK_AUTH_GEN
*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : R_BLD_AUTH Événement : EV_SEND_AUTH
*Nov 11 19:30:34.833: IKEv2:Construct Vendor Specific Payload: CISCO-GRANITE

	*Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS		
	*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Type d'échange : IKE_AUTH, indicateurs : RESPONDER MSG-RESPONSE ID de message : 1, longueur : 252 Contenu de la charge utile : ENCR Charge utile suivante : VID, réservé : 0x0, longueur : 224 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_OK *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):Action: Action_Null *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_PKI_SESH_CLOSE *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):fermeture de la session PKI *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_UPDATE_CAC_STATS *11 nov. 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Event:EV_INSERT_IKE *Nov 11 19:30:34.834: IKEv2:Store mib index ikev2 1, plate-forme 60 *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_GEN_LOAD_IPSEC *Nov 11 19:30:34.834: IKEv2:(ID SA = 1):Requête asynchrone mise en file d'attente *Nov 11 19:30:34.834: IKEv2:(ID SA = 1): *11 nov. 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_NO_EVENT		Le répon envoie la pour IKE_
<----------Le répondeur a envoyé IKE_AUTH----------			
L'initiateur reçoit une réponse du répondeur.	*Nov 11 19:30:34.834: IKEv2:Réception d'un paquet du répartiteur *Nov 11 19:30:34.834:	*Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState :	Le répon insère un dans le D

	IKEv2:Traitement d'un élément hors de la file d'attente de pak	AUTH_DONE Événement : EV_OK_RECD_LOAD_IPSEC *Nov 11 19:30:34.840: IKEv2:(ID SA = 1):Action: Action_Null *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Event: EV_START_ACCT *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_CHECK_DUPE *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_CHK4_ROLE	
Le routeur 1 vérifie et traite les données d'authentification dans ce paquet. Le routeur 1 insère ensuite cette SA dans son SAD.	*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Type d'échange : IKE_AUTH, indicateurs : RESPONDER MSG-RESPONSE ID de message : 1, longueur : 252 Contenu de la charge utile : *Nov 11 19:30:34.834: IKEv2:Analyser la charge utile spécifique au fournisseur: (PERSONNALISÉ) VID Charge utile suivante : IDr., réservée: 0x0, longueur: 20 IDr. Charge utile suivante : AUTH, réservée : 0x0, longueur : 12 Type d'ID : adresse IPv4, Réservé : 0x0 0x0 AUTH Charge utile suivante : SA, réservée : 0x0, longueur : 28 Méthode d'authentification PSK, réservée : 0x0, réservée 0x0 SA Charge utile suivante : TSi, réservée : 0x0, longueur : 40 dernière proposition : 0x0, réservée : 0x0, longueur : 36 Proposition : 1, ID de protocole : ESP, taille SPI : 4, #trans : 3 dernière transformation : 0x3, réservé : 0x0 : longueur : 8 type : 1, réservé : 0x0, id : 3DES dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96		

dernière transformation : 0x0, réservée : 0x0 : longueur : 8
type : 5, réservé : 0x0, id : Ne pas utiliser ESN
TSi Charge utile suivante : TSr, réservée : 0x0, longueur : 24
Nombre de services techniques : 1, réservé 0x0, réservé 0x0
Type TS : TS_IPV4_ADDR_RANGE, ID de protocole : 0, longueur : 16
port de début : 0, port de fin : 65535
adresse de début : 0.0.0.0, adresse de fin : 255.255.255.255
TSr Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 24
Nombre de services techniques : 1, réservé 0x0, réservé 0x0
Type TS : TS_IPV4_ADDR_RANGE, ID de protocole : 0, longueur : 16
port de début : 0, port de fin : 65535
adresse de début : 0.0.0.0, adresse de fin : 255.255.255.255

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Prochaine charge utile : NOTIFY, réservé : 0x0, longueur : 12
ID de protocole de sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) Prochaine charge utile : NOTIFY, réservé : 0x0, longueur : 8
ID de protocole de sécurité : IKE, taille spi : 0, type : ESP_TFC_NO_SUPPORT

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) Prochaine charge utile : NONE, réservé : 0x0, longueur : 8
ID de protocole de sécurité : IKE, taille de spi : 0, type : NON_FIRST_FRAGS

*11 nov. 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_WAIT_AUTH Event:EV_RECV_AUTH
*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):Action: Action_Null
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_CHK4_NOTIFY
*11 nov. 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:EV_PROC_MSG
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL

*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_GET_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:Ajout de la proposition PHASE1-prop à la stratégie de boîte à outils
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Utilisation du profil IKEv2 'IKEV2-SETUP'
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_VERIFY_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_GET_PRESHR_KEY
*11 nov. 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:EV_VERIFY_AUTH
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_CHK_EAP
*11 nov. 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:EV_NOTIFY_AUTH_DONE
*Nov 11 19:30:34.835: L'autorisation de groupe IKEv2:AAA n'est pas configurée
*Nov 11 19:30:34.835: L'autorisation utilisateur IKEv2:AAA n'est pas configurée
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_CHK4_IC
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : I_PROC_AUTH Événement : EV_CHK_IKE_ONLY
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_PROC_SA_TS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA:

I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):Action: Action_Null
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_PKI_SESH_CLOSE
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):fermeture de la session PKI
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_UPDATE_CAC_STATS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_INSERT_IKE
*Nov 11 19:30:34.835: IKEv2:Store mib index ikev2 1, plate-forme 60
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_GEN_LOAD_IPSEC
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):Requête asynchrone mise en file d'attente

*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_NO_EVENT
*Nov 11 19:30:34.835: message IKEv2:KMI 8 consommé. Aucune action entreprise.
*Nov 11 19:30:34.835: message IKEv2:KMI 12 consommé. Aucune action entreprise.
*Nov 11 19:30:34.835: IKEv2:Aucune donnée à envoyer dans le jeu de configuration du mode.
*Nov 11 19:30:34.841: IKEv2:Ajout du handle d'identité 0x80000002 associé à SPI 0x9506D414 pour la session 8

*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : AUTH_DONE Événement : EV_OK_RECD_LOAD_IPSEC
*Nov 11 19:30:34.841: IKEv2:(ID SA = 1):Action: Action_Null
*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_START_ACCT
*Nov 11 19:30:34.841: IKEv2:(ID SA = 1):Comptabilité non requise
*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =

	00000001 CurState : AUTH_DONE Événement : EV_CHECK_DUPE *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : AUTH_DONE Event: EV_CHK4_ROLE		
Le tunnel est activé sur l'initiateur et l'état affiche READY.	*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : READYEvent: EV_CHK_IKE_ONLY *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState : READY Event: EV_I_OK	*Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: READY Event: EV_R_OK *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState : READY Event: EV_NO_EVENT	Le tunnel sur le rép Le tunnel répondeu apparaît généralen avant l'ini

Débogages CHILD_SA

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

Description du message CHILD_SA du routeur 1	Déboguages	Description du message CHILD_SA du routeur 2
Le routeur 1 initie l'échange CHILD_SA. Il s'agit de la demande CREATE_CHILD_SA. Le paquet CHILD_SA contient généralement : • SA HDR (version.flags/type exchange) • Nonce Ni (facultatif) : si CHILD_SA est créé dans le cadre de l'échange initial, une seconde charge utile KE et nonce ne doivent pas être envoyés)	*Nov 11 19:31:35.873: IKEv2:Réception d'un paquet du répartiteur *Nov 11 19:31:35.873: IKEv2:Traitement d'un élément hors de la file d'attente de pak *Nov 11 19:31:35.873: IKEv2:(SA ID = 2):La demande a mess_id 3 ; attendu du 3 au 7 *Nov 11 19:31:35.873: IKEv2:(SA ID = 2):Next payload: ENCR, version: 2.0 Type d'échange : CREATE_CHILD_SA, indicateurs : INITIATOR ID de message : 3, longueur : 396 Contenu de la charge utile :	

• Charge utile SA • KEi (Key-optional) : la demande CREATE_CHILD_SA peut éventuellement contenir une charge utile KE pour un échange DH supplémentaire afin de permettre des garanties plus solides de confidentialité de transfert pour CHILD_SA. Si les offres SA incluent différents groupes DH, KEi doit être un élément du groupe que l'initiateur attend du répondeur qu'il accepte. S'il devine mal, l'échange CREATE_CHILD_SA échoue et il peut réessayer avec un autre KEi • N(Notify payload-optional). La fonctionnalité Notify Payload permet de transmettre des données d'information, telles que des conditions d'erreur et des transitions d'état, à un homologue IKE. Un message Notify Payload peut apparaître dans un message de réponse (généralement il spécifie pourquoi une demande a été	SA Charge utile suivante : N, réservée : 0x0, longueur : 152 dernière proposition : 0x0, réservée : 0x0, longueur : 148 Proposition : 1, ID de protocole : IKE, taille SPI : 8, #trans : 15 dernière transformation : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA512 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA384 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA256 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : MD5 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA512 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA384 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA256 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : MD596	

rejetée), dans un échange d'INFORMATIONS (pour signaler une erreur qui ne se trouve pas dans une demande IKE), ou dans tout autre message pour indiquer les capacités de l'expéditeur ou pour modifier la signification de la demande.Si cet échange CREATE_CHILD_SA effectue une nouvelle saisie d'une association de sécurité existante autre que l'association de sécurité IKE_SA, l'élément N payload principal de type REKEY_SA DOIT identifier l'association de sécurité en cours de nouvelle saisie. Si cet échange CREATE_CHILD_SA n'est pas une nouvelle saisie d'une SA existante, la charge utile N DOIT être omise.	dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1536_MODP/Group 5 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Groupe 2 N Charge utile suivante : KE, réservée : 0x0, longueur : 24 KE Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 136 Groupe DH : 2, Réservé : 0x0 *Nov 11 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Prochaine charge utile : NONE, réservé : 0x0, longueur : 12 ID de protocole de sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE *11 nov 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : READY Event: EV_RECV_CREATE_CHILD *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):Action: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_INIT Événement : EV_RECV_CREATE_CHILD *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):Action: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_INIT Événement : EV_VERIFY_MSG	

	*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_INIT Événement : EV_CHK_CC_TYPE *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_IKE Événement : EV_REKEY_IKESA *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_IKE Événement : EV_GET_IKE_POLICY *Nov 11 19:31:35.874: IKEv2:% Obtention de la clé pré-partagée par l'adresse 10.0.0.2 *Nov 11 19:31:35.874: IKEv2:% Obtention de la clé pré-partagée par l'adresse 10.0.0.2 *Nov 11 19:31:35.874: IKEv2:Ajout de la proposition PHASE1-prop à la stratégie de boîte à outils *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Utilisation du profil IKEv2 'IKEV2-SETUP' *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_IKE Événement : EV_PROC_MSG *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_IKE Événement : EV_SET_POLICY *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Définition des stratégies configurées *Nov 11 19:31:35.874: IKEv2:(SA ID =	

	2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Événement : EV_GEN_DH_KEY *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Événement : EV_NO_EVENT *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Événement : EV_OK_RECD_DH_PUBKEY_RESP *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):Action: Action_Null *11 nov. 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Event:EV_GEN_DH_SECRET *Nov 11 19:31:35.881: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Événement : EV_NO_EVENT *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Événement : EV_OK_RECD_DH_SECRET_RESP *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):Action: Action_Null	

	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Événement : EV_BLD_MSG *Nov 11 19:31:35.882: IKEv2:ConstructNotify Payload: SET_WINDOW_SIZE Contenu de la charge utile : SA Charge utile suivante : N, réservée : 0x0, longueur : 56 dernière proposition : 0x0, réservée : 0x0, longueur : 52 Proposition : 1, ID de protocole : IKE, taille SPI : 8, #trans : 4 dernière transformation : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Groupe 2 N Charge utile suivante : KE, réservée : 0x0, longueur : 24 KE Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 136 Groupe DH : 2, Réservé : 0x0 NOTIFY(SET_WINDOW_SIZE) Charge utile suivante : AUCUNE, réservée : 0x0, longueur : 12 ID de protocole de sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE	
	*Nov 11 19:31:35.869: IKEv2:(SA ID = 2):Next payload: ENCR, version: 2.0 Type d'échange : CREATE_CHILD_SA, indicateurs : INITIATOR ID de message :	Ce paquet est reçu par le routeur 2.

	2, longueur : 460 Contenu de la charge utile : ENCR Charge utile suivante : SA, réservée : 0x0, longueur : 432 *Nov 11 19:31:35.873: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE Contenu de la charge utile : SA Charge utile suivante : N, réservée : 0x0, longueur : 152 dernière proposition : 0x0, réservée : 0x0, longueur : 148 Proposition : 1, ID de protocole : IKE, taille SPI : 8, #trans : 15 dernière transformation : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA512 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA384 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA256 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : MD5 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA512 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA384 dernière transformation : 0x3, réservée : 0x0 : longueur : 8	

	type : 3, réservé : 0x0, id : SHA256 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : MD596 dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1536_MODP/Group 5 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Groupe 2 N Charge utile suivante : KE, réservée : 0x0, longueur : 24 KE Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 136 Groupe DH : 2, Réservé : 0x0 NOTIFY(SET_WINDOW_SIZE) Charge utile suivante : AUCUNE, réservée : 0x0, longueur : 12 ID de protocole de sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE	
	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Next payload: ENCR, version: 2.0 Type d'échange : CREATE_CHILD_SA, indicateurs : RESPONDER MSG-RESPONSE ID de message : 3, longueur : 300 Contenu de la charge utile : SA Charge utile suivante : N, réservée : 0x0, longueur : 56 dernière proposition : 0x0, réservée : 0x0, longueur : 52 Proposition : 1, ID de protocole : IKE, taille SPI : 8, #trans : 4 dernière transformation : 0x3, réservé : 0x0 : longueur : 12 type : 1, réservé : 0x0, id : AES-CBC dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 2, réservé : 0x0, id : SHA1	Le routeur 2 génère maintenant la réponse pour l'échange CHILD_SA. Il s'agit de la réponse CREATE_CHILD_SA. Le paquet CHILD_SA contient généralement : • SA HDR (version.flags/type exchange) • Nonce Ni (facultatif) : si la CHILD_SA est créée dans le cadre de l'échange initial, une seconde charge utile KE et nonce ne doivent pas être envoyées.

	dernière transformation : 0x3, réservée : 0x0 : longueur : 8 type : 3, réservé : 0x0, id : SHA96 dernière transformation : 0x0, réservée : 0x0 : longueur : 8 type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Groupe 2 N Charge utile suivante : KE, réservée : 0x0, longueur : 24 KE Charge utile suivante : NOTIFY, réservée : 0x0, longueur : 136 Groupe DH : 2, Réservé : 0x0 *Nov 11 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Prochaine charge utile : NONE, réservé : 0x0, longueur : 12 ID de protocole de sécurité : IKE, taille de spi : 0, type : SET_WINDOW_SIZE *11 nov. 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_WAIT Événement : EV_RECV_CREATE_CHILD *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):Action: Action_Null *11 nov 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_CHK4_NOTIFY *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_VERIFY_MSG *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6	• Charge utile SA • KEi (Key-optional) : la demande CREATE_CHILD_SA peut éventuellement contenir une charge utile KE pour un échange DH supplémentaire afin de permettre des garanties plus solides de confidentialité de transfert pour CHILD_SA. Si les offres SA incluent différents groupes DH, KEi doit être un élément du groupe que l'initiateur attend du répondeur qu'il accepte. S'il devine mal, l'échange CREATE_CHILD_SA échoue et il doit réessayer avec un autre KEi. • N (Notify payload-optional) : cette fonction est utilisée pour transmettre des données d'information, telles que des conditions d'erreur et des transitions d'état, à un homologue IKE. Un message Notify Payload peut apparaître dans un message de réponse (il indique généralement pourquoi une demande a été

	R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_PROC_MSG *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_CHK4_PFS *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_GEN_DH_SECRET *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_NO_EVENT *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_OK_RECD_DH_SECRET_RESP *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):Action: Action_Null *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_CHK_IKE_REKEY *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_PROC Événement : EV_GEN_SKEYID *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Generate skeyid *11 nov. 19:31:35.890: IKEv2:(SA ID =	rejetée), dans un échange d'informations (pour signaler une erreur qui ne se trouve pas dans une demande IKE) ou dans tout autre message pour indiquer les capacités de l'expéditeur ou pour modifier la signification de la demande. Si cet échange CREATE_CHILD_SA effectue une nouvelle saisie d'une association de sécurité existante autre que l'association de sécurité IKE_SA, la charge utile N principale de type REKEY_SA doit identifier l'association de sécurité en cours de nouvelle saisie. Si cet échange CREATE_CHILD_SA n'est pas une nouvelle saisie d'une SA existante, la charge utile N doit être omise. Le routeur 2 envoie la réponse et termine l'activation de la nouvelle SA ENFANT.

	2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_DONE Événement : EV_ACTIVATE_NEW_SA *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_DONE Événement : EV_UPDATE_CAC_STATS *Nov 11 19:31:35.890: IKEv2:Nouvelle requête IKEv2 sa activée *Nov 11 19:31:35.890: IKEv2:Échec de la décrémentation du nombre pour la négociation sortante *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_DONE Événement : EV_CHECK_DUPE *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState : CHILD_I_DONE Événement : EV_OK *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: EXIT Event: EV_CHK_PENDING *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Réponse traitée avec l'ID de message 3, les requêtes peuvent être envoyées de la plage 4 à 8 *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: EXIT Event: EV_NO_EVENT	

Le routeur 1 reçoit le paquet de réponse du routeur 2 et termine l'activation de CHILD_SA.	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Charge utile suivante : ENCR, version : 2.0 Type d'échange : CREATE_CHILD_SA, indicateurs : RESPONDER MSG-RESPONSE ID de message : 3, longueur : 300 Contenu de la charge utile : ENCR Charge utile suivante : SA, réservée : 0x0, longueur : 272 *11 nov. 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Event:EV_CHK_IKE_REKEY *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_BLD_MSG Événement : EV_GEN_SKEYID *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Generate skeyid *11 nov. 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_DONE Event:EV_ACTIVATE_NEW_SA *Nov 11 19:31:35.882: IKEv2:Store mib index ikev2 3, plate-forme 62 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_DONE Événement : EV_UPDATE_CAC_STATS *Nov 11 19:31:35.882: IKEv2:Nouvelle requête IKEv2 sa activée *Nov 11 19:31:35.882: IKEv2:Échec de la réduction du nombre pour la négociation entrante	

	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_DONE Event : EV_CHECK_DUPE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_DONE Événement : EV_OK *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState : CHILD_R_DONE Événement : EV_START_DEL_NEG_TMR *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):Action: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: EXIT Event: EV_CHK_PENDING *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Réponse envoyée avec l'ID de message 3, les requêtes peuvent être acceptées de la plage 4 à 8 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: EXIT Event: EV_NO_EVENT	

Vérification du tunnel

ISAKMP

Commande

<#root>

show crypto ikev2 sa detailed

Sortie du routeur 1

<#root>

```
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 du routeur 2

<#root>

```
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

<#root>

show crypto ipsec sa

Remarque : dans cette sortie, contrairement à IKEv1, la valeur du groupe PFS DH apparaît sous la forme « PFS (Y/N) : N, DH group : none » lors de la première négociation de tunnel, mais, après une nouvelle clé, les bonnes valeurs apparaissent. Il ne s'agit pas d'un bogue, même si le comportement est décrit dans l'ID de bogue Cisco CSCug67056. (Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations ou aux outils Cisco internes.)
La différence entre IKEv1 et IKEv2 est que, dans ce dernier cas, les SA enfant sont créées dans le cadre de l'échange AUTH lui-même. Le groupe DH configuré sous la crypto-carte ne serait utilisé que lors de la nouvelle clé. Par conséquent, vous verriez 'PFS (Y/N) : N, DH group : none' jusqu'à la première nouvelle clé.
Avec IKEv1, vous voyez un comportement différent, car la création d'une association de sécurité enfant se produit en mode rapide et le message CREATE_CHILD_SA dispose d'une provision pour transporter la charge utile d'échange de clé qui spécifie les paramètres DH pour dériver un nouveau secret partagé.

Sortie du routeur 1

<#root>

```
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 du routeur 2

```
<#root>
```

```
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 le résultat de la commande show crypto session sur les deux routeurs ; ce résultat montre l'état de session de tunnel comme UP-ACTIVE.

<#root>

```
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 de paquets IKEv2 et débogage au niveau du protocole
- Assistance technique de Cisco et téléchargements

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

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