Règles de sélection IOS IKEv1/IKEv2 pour les keyings et les profils - Guide de dépannage

Contenu

Introduction

Ce document décrit l'utilisation de plusieurs touches pour plusieurs profils ISAKMP (Internet Security Association and Key Management Protocol) dans un scénario VPN LAN à LAN du logiciel Cisco IOS®. Il couvre le comportement du logiciel Cisco IOS Version 15.3T ainsi que les problèmes potentiels lors de l'utilisation de plusieurs touches.

Deux scénarios sont présentés, basés sur un tunnel VPN avec deux profils ISAKMP sur chaque routeur. Chaque profil possède une sonnerie différente avec la même adresse IP associée. Les scénarios montrent que le tunnel VPN ne peut être initié qu'à partir d'un côté de la connexion en raison de la sélection et de la vérification du profil.

Les sections suivantes du document récapitulent les critères de sélection du profil de la clé pour l'initiateur de l'échange de clés Internet (IKE) et le répondeur IKE. Lorsque différentes adresses IP sont utilisées par la sonnerie sur le répondeur IKE, la configuration fonctionne correctement, mais l'utilisation de la même adresse IP crée le problème présenté dans le premier scénario.

Les sections suivantes expliquent pourquoi la présence d'une combinaison de touches par défaut (configuration globale) et de touches spécifiques peut entraîner des problèmes et pourquoi l'utilisation du protocole Internet Key Exchange Version 2 (IKEv2) évite ce problème.

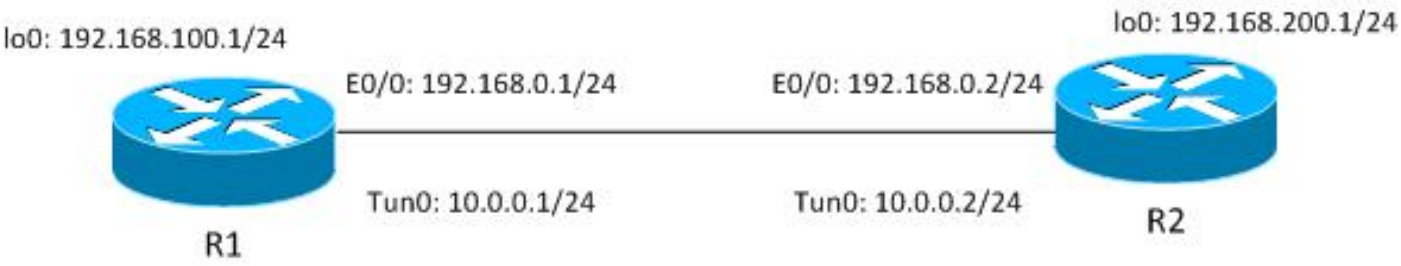
Les dernières sections présentent les critères de sélection du profil IKE pour l'initiateur et le répondeur IKE, ainsi que les erreurs typiques qui se produisent lorsqu'un profil incorrect est sélectionné.

Configuration

> **Remarques :**
>
> Certaines commandes d'affichage (« show ») sont offertes par l'outil « Cisco CLI Analyzer » réservé aux clients inscrits. Utilisez cet outil pour obtenir une analyse des rapports produits par ces commandes.
>
> Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Topologie

Les routeurs R1 (R1) et R2 (R2) utilisent des interfaces VTI (Virtual Tunnel Interface) (Generic Routing Encapsulation [GRE]) afin d'accéder à ses bouclages. Cette VTI est protégée par le protocole IPSec (Internet Protocol Security).



R1 et R2 ont deux profils ISAKMP, chacun avec une sonnerie différente. Tous les sonneries ont le même mot de passe.

Réseau et VPN de R1

La configuration du réseau et du VPN de R1 est la suivante :

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.2 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2

crypto isakmp profile profile1
   keyring keyring1
   match identity address 192.168.0.102 255.255.255.255 !non existing host
crypto isakmp profile profile2
   keyring keyring2
```

```
  match identity address 192.168.0.2 255.255.255.255 !R2
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile profile1
 set transform-set TS
 set isakmp-profile profile2
!
interface Loopback0
 description Simulate LAN
 ip address 192.168.100.1 255.255.255.0
!
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.

ip route 192.168.200.0 255.255.255.0 10.0.0.2
```

Réseau et VPN de R2

La configuration du réseau R2 et du VPN est la suivante :

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.1 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.1 key cisco
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2

crypto isakmp profile profile1
   keyring keyring1
   match identity address 192.168.0.1 255.255.255.255 !R1
crypto isakmp profile profile2
   keyring keyring2
   match identity address 192.168.0.100 255.255.255.255 !non existing host
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile profile1
 set transform-set TS
 set isakmp-profile profile1
!
interface Loopback0
 ip address 192.168.200.1 255.255.255.0
!
interface Tunnel1
 ip address 10.0.0.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.1
 tunnel protection ipsec profile profile1
!
```

```
interface Ethernet0/0
 ip address 192.168.0.2 255.255.255.0

ip route 192.168.100.0 255.255.255.0 10.0.0.1
```

Toutes les sonneries utilisent la même adresse IP homologue et le mot de passe cisco.

Sur R1, le profil 2 est utilisé pour la connexion VPN. Profile2 est le deuxième profil de la configuration, qui utilise la deuxième frappe de la configuration. Comme vous le verrez, l'ordre des touches est critique.

Exemples de scénarios

Dans le premier scénario, R1 est l'initiateur ISAKMP. Le tunnel négocie correctement et le trafic est protégé comme prévu.

Le deuxième scénario utilise la même topologie, mais R2 est l'initiateur ISAKMP lorsque la négociation de phase1 échoue.

Internet Key Exchange Version 1 (IKEv1) a besoin d'une clé pré-partagée pour le calcul de la clé, qui est utilisée afin de déchiffrer/chiffrer le paquet en mode principal 5 (MM5) et les paquets IKEv1 suivants. La clé est dérivée du calcul Diffie-Hellman (DH) et de la clé pré-partagée. Cette clé pré-partagée doit être déterminée après la réception de MM3 (répondeur) ou MM4 (initiateur), afin que la clé, utilisée dans MM5/MM6, puisse être calculée.

Pour le répondeur ISAKMP dans MM3, le profil ISAKMP spécifique n'est pas encore déterminé car cela se produit après la réception de l'IKEID dans MM5. À la place, toutes les sonneries de clés sont recherchées pour une clé pré-partagée et la première ou la meilleure sonnerie correspondante de la configuration globale est sélectionnée. Cette clé est utilisée afin de calculer la clé qui est utilisée pour le déchiffrement de MM5 et le chiffrement de MM6. Après avoir déterminé le déchiffrement de MM5 et après avoir déterminé le profil ISAKMP et la sonnerie associée, le répondeur ISAKMP effectue une vérification si la même sonnerie a été sélectionnée ; si la même sonnerie n'est pas sélectionnée, la connexion est abandonnée.

Ainsi, pour le répondeur ISAKMP, vous devez utiliser une seule clé avec plusieurs entrées chaque fois que possible.

R1 comme initiateur IKE (correct)

Ce scénario décrit ce qui se produit lorsque R1 est l'initiateur IKE :

1. Utilisez ces débogages pour R1 et R2 :

```
R1# debug crypto isakmp
R1# debug crypto ipsec
R1# debug crypto isakmp aaa
```

2. R1 lance le tunnel, envoie le paquet MM1 avec des propositions de stratégie et reçoit MM2 en réponse. MM3 est ensuite préparé :

```
R1#ping 192.168.200.1 source lo0 repeat 1
Type escape sequence to abort.
```

```
Sending 1, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1

*Jun 19 10:04:24.826: IPSEC(sa_request): ,
 (key eng. msg.) OUTBOUND local= 192.168.0.1:500, remote= 192.168.0.2:500,
   local_proxy= 192.168.0.1/255.255.255.255/47/0,
   remote_proxy= 192.168.0.2/255.255.255.255/47/0,
   protocol= ESP, transform= esp-aes esp-sha256-hmac  (Tunnel),
   lifedur= 3600s and 4608000kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Jun 19 10:04:24.826: ISAKMP:(0): SA request profile is profile2
*Jun 19 10:04:24.826: ISAKMP: Found a peer struct for 192.168.0.2, peer
port 500
*Jun 19 10:04:24.826: ISAKMP: Locking peer struct 0xF483A970, refcount 1
for isakmp_initiator
*Jun 19 10:04:24.826: ISAKMP: local port 500, remote port 500
*Jun 19 10:04:24.826: ISAKMP: set new node 0 to QM_IDLE
*Jun 19 10:04:24.826: ISAKMP:(0):insert sa successfully sa = F474C2E8
*Jun 19 10:04:24.826: ISAKMP:(0):Can not start Aggressive mode, trying
Main mode.
*Jun 19 10:04:24.826: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-07 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-03 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-02 ID
*Jun 19 10:04:24.826: ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC,
IKE_SA_REQ_MM
*Jun 19 10:04:24.826: ISAKMP:(0):Old State = IKE_READY  New State =
IKE_I_MM1

*Jun 19 10:04:24.826: ISAKMP:(0): beginning Main Mode exchange
*Jun 19 10:04:24.826: ISAKMP:(0): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_NO_STATE
*Jun 19 10:04:24.826: ISAKMP:(0):Sending an IKE IPv4 Packet.
*Jun 19 10:04:24.827: ISAKMP (0): received packet from 192.168.0.2 dport
500 sport 500 Global (I) MM_NO_STATE
*Jun 19 10:04:24.827: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.827: ISAKMP:(0):Old State = IKE_I_MM1  New State =
IKE_I_MM2

*Jun 19 10:04:24.827: ISAKMP:(0): processing SA payload. message ID = 0
*Jun 19 10:04:24.827: ISAKMP:(0): processing vendor id payload
*Jun 19 10:04:24.827: ISAKMP:(0): vendor ID seems Unity/DPD but major 69
mismatch
*Jun 19 10:04:24.827: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 10:04:24.827: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.827: ISAKMP:(0): local preshared key found
*Jun 19 10:04:24.827: ISAKMP : Looking for xauth in profile profile2
*Jun 19 10:04:24.827: ISAKMP:(0):Checking ISAKMP transform 1 against
priority 10 policy
*Jun 19 10:04:24.827: ISAKMP:      encryption 3DES-CBC
*Jun 19 10:04:24.827: ISAKMP:      hash MD5
*Jun 19 10:04:24.827: ISAKMP:      default group 2
*Jun 19 10:04:24.827: ISAKMP:      auth pre-share
*Jun 19 10:04:24.827: ISAKMP:      life type in seconds
*Jun 19 10:04:24.827: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Jun 19 10:04:24.827: ISAKMP:(0):atts are acceptable. Next payload is 0
*Jun 19 10:04:24.827: ISAKMP:(0):Acceptable atts:actual life: 0
*Jun 19 10:04:24.827: ISAKMP:(0):Acceptable atts:life: 0
*Jun 19 10:04:24.827: ISAKMP:(0):Fill atts in sa vpi_length:4
*Jun 19 10:04:24.827: ISAKMP:(0):Fill atts in sa life_in_seconds:86400
*Jun 19 10:04:24.827: ISAKMP:(0):Returning Actual lifetime: 86400
*Jun 19 10:04:24.827: ISAKMP:(0)::Started lifetime timer: 86400.
```

```
*Jun 19 10:04:24.827: ISAKMP:(0): processing vendor id payload
*Jun 19 10:04:24.827: ISAKMP:(0): vendor ID seems Unity/DPD but major 69
mismatch
*Jun 19 10:04:24.827: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 10:04:24.827: ISAKMP:(0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.827: ISAKMP:(0):Old State = IKE_I_MM2  New State =
IKE_I_MM2

*Jun 19 10:04:24.828: ISAKMP:(0): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_SA_SETUP
```

Dès le départ, R1 sait que le profil ISAKMP2 doit être utilisé car il est lié sous le profil IPSec utilisé pour cette VTI.

Par conséquent, la sonnerie correcte (keyring2) a été sélectionnée. La clé pré-partagée de keyring2 est utilisée comme matériau de frappe pour les calculs DH lors de la préparation du paquet MM3.

3. Lorsque R2 reçoit ce paquet MM3, il ne sait toujours pas quel profil ISAKMP doit être utilisé, mais il a besoin d'une clé pré-partagée pour la génération DH. C’est pourquoi R2 recherche toutes les sonneries de clés afin de trouver la clé pré-partagée pour cet homologue :

```
*Jun 19 10:04:24.828: ISAKMP (0): received packet from 192.168.0.1 dport
500 sport 500 Global (R) MM_SA_SETUP
*Jun 19 10:04:24.828: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.828: ISAKMP:(0):Old State = IKE_R_MM2  New State =
IKE_R_MM3

*Jun 19 10:04:24.828: ISAKMP:(0): processing KE payload. message ID = 0
*Jun 19 10:04:24.831: ISAKMP:(0): processing NONCE payload. message ID = 0
*Jun 19 10:04:24.831: ISAKMP:(0):found peer pre-shared key matching
192.168.0.1
```

La clé de 192.168.0.1 a été trouvée dans la première sonnerie définie (keyring1).

4. R2 prépare ensuite le paquet MM4 avec des calculs DH et avec la clé cisco de keyring1 :

```
*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID is DPD
*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): speaking to another IOS box!
*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID seems Unity/DPD but major
32 mismatch
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID is XAUTH
*Jun 19 10:04:24.831: ISAKMP:received payload type 20
*Jun 19 10:04:24.831: ISAKMP (1011): His hash no match - this node
outside NAT
*Jun 19 10:04:24.831: ISAKMP:received payload type 20
*Jun 19 10:04:24.831: ISAKMP (1011): No NAT Found for self or peer
*Jun 19 10:04:24.831: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.831: ISAKMP:(1011):Old State = IKE_R_MM3  New State =
IKE_R_MM3

*Jun 19 10:04:24.831: ISAKMP:(1011): sending packet to 192.168.0.1 my_port
500 peer_port 500 (R) MM_KEY_EXCH
```

```
*Jun 19 10:04:24.831: ISAKMP:(1011):Sending an IKE IPv4 Packet.
```

5. Lorsque R1 reçoit MM4, il prépare le paquet MM5 avec IKEID et la clé correcte sélectionnée précédemment (à partir de keyring2) :

```
*Jun 19 10:04:24.831: ISAKMP (0): received packet from 192.168.0.2 dport
500 sport 500 Global (I) MM_SA_SETUP
*Jun 19 10:04:24.831: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.831: ISAKMP:(0):Old State = IKE_I_MM3  New State =
IKE_I_MM4

*Jun 19 10:04:24.831: ISAKMP:(0): processing KE payload. message ID = 0
*Jun 19 10:04:24.837: ISAKMP:(0): processing NONCE payload. message ID = 0
*Jun 19 10:04:24.837: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): vendor ID is Unity
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): vendor ID is DPD
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): speaking to another IOS box!
*Jun 19 10:04:24.837: ISAKMP:received payload type 20
*Jun 19 10:04:24.838: ISAKMP (1011): His hash no match - this node
outside NAT
*Jun 19 10:04:24.838: ISAKMP:received payload type 20
*Jun 19 10:04:24.838: ISAKMP (1011): No NAT Found for self or peer
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_I_MM4  New State =
IKE_I_MM4

*Jun 19 10:04:24.838: ISAKMP:(1011):Send initial contact
*Jun 19 10:04:24.838: ISAKMP:(1011):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.1
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 10:04:24.838: ISAKMP:(1011):Total payload length: 12
*Jun 19 10:04:24.838: ISAKMP:(1011): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_KEY_EXCH
```

6. Le paquet MM5, qui contient l'IKEID 192.168.0.1, est reçu par R2. À ce stade, R2 sait à quel profil ISAKMP le trafic doit être lié (la commande **match identity** address) :

```
*Jun 19 10:04:24.838: ISAKMP (1011): received packet from 192.168.0.1 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_R_MM4  New State =
IKE_R_MM5

*Jun 19 10:04:24.838: ISAKMP:(1011): processing ID payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.1
       protocol     : 17
       port         : 500
       length       : 12
```

```
*Jun 19 10:04:24.838: ISAKMP:(0):: peer matches profile1 profile
*Jun 19 10:04:24.838: ISAKMP:(1011):Found ADDRESS key in keyring keyring1
*Jun 19 10:04:24.838: ISAKMP:(1011): processing HASH payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP:(1011): processing NOTIFY INITIAL_CONTACT
protocol 1
       spi 0, message ID = 0, sa = 0xF46295E8
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
       authenticated
*Jun 19 10:04:24.838: ISAKMP:(1011):SA has been authenticated with
192.168.0.1
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
       authenticated
```

7. R2 effectue maintenant une vérification si la sonnerie qui a été sélectionnée aveuglément pour le paquet MM4 est identique à la sonnerie configurée pour le profil ISAKMP maintenant choisi. Étant donné que keyring1 est le premier de la configuration, il a été sélectionné précédemment et il est maintenant sélectionné. La validation a réussi et le paquet MM6 peut être envoyé :

```
*Jun 19 10:04:24.838: ISAKMP:(1011):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.2
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 10:04:24.838: ISAKMP:(1011):Total payload length: 12
*Jun 19 10:04:24.838: ISAKMP:(1011): sending packet to 192.168.0.1
my_port 500 peer_port 500 (R) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Sending an IKE IPv4 Packet.
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_R_MM5  New State =
IKE_P1_COMPLETE
```

8. R1 reçoit MM6 et n'a pas besoin d'effectuer la vérification de la sonnerie de clés car elle était connue du premier paquet ; l'initiateur connaît toujours le profil ISAKMP à utiliser et la clé associée à ce profil. L'authentification a réussi et la phase 1 se termine correctement :

```
*Jun 19 10:04:24.838: ISAKMP (1011): received packet from 192.168.0.2
dport 500 sport 500 Global (I) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011): processing ID payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.2
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 10:04:24.838: ISAKMP:(1011): processing HASH payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
        authenticated
*Jun 19 10:04:24.838: ISAKMP:(1011):SA has been authenticated with
192.168.0.2
*Jun 19 10:04:24.838: ISAKMP AAA: Accounting is not enabled
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
*Jun 19 10:04:24.839: ISAKMP:(1011):Old State = IKE_I_MM5  New State =
```

```
IKE_I_MM6

*Jun 19 10:04:24.839: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.839: ISAKMP:(1011):Old State = IKE_I_MM6  New State =
IKE_I_MM6

*Jun 19 10:04:24.843: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Jun 19 10:04:24.843: ISAKMP:(1011):Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE

*Jun 19 10:04:24.843: ISAKMP:(1011):beginning Quick Mode exchange, M-ID
of 2816227709
```

9. La phase 2 démarre normalement et est terminée.

Ce scénario fonctionne correctement uniquement en raison de l'ordre correct des trousseaux de clés définis sur R2. Le profil qui doit être utilisé pour la session VPN utilise la combinaison de touches qui a été la première dans la configuration.

R2 en tant qu'initiateur IKE (incorrect)

Ce scénario décrit ce qui se produit lorsque R2 lance le même tunnel et explique pourquoi le tunnel ne sera pas établi. Certains journaux ont été supprimés afin de mettre l'accent sur les différences entre cet exemple et l'exemple précédent :

1. R2 lance le tunnel :

```
R2#ping 192.168.100.1 source lo0 repeat 1
```

2. Comme R2 est l'initiateur, le profil ISAKMP et le trousseau de clés sont connus. La clé pré-partagée de keyring1 est utilisée pour les calculs DH et est envoyée dans MM3. R2 reçoit MM2 et prépare MM3 en fonction de cette clé :

```
*Jun 19 12:28:44.256: ISAKMP (0): received packet from 192.168.0.1 dport
500 sport 500 Global (I) MM_NO_STATE
*Jun 19 12:28:44.256: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 12:28:44.256: ISAKMP:(0):Old State = IKE_I_MM1  New State =
IKE_I_MM2

*Jun 19 12:28:44.256: ISAKMP:(0): processing SA payload. message ID = 0
*Jun 19 12:28:44.256: ISAKMP:(0): processing vendor id payload
*Jun 19 12:28:44.256: ISAKMP:(0): vendor ID seems Unity/DPD but major
69 mismatch
*Jun 19 12:28:44.256: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 12:28:44.256: ISAKMP:(0):Found ADDRESS key in keyring keyring1
*Jun 19 12:28:44.256: ISAKMP:(0): local preshared key found
*Jun 19 12:28:44.256: ISAKMP : Looking for xauth in profile profile1
*Jun 19 12:28:44.256: ISAKMP:(0):Checking ISAKMP transform 1 against
priority 10 policy
*Jun 19 12:28:44.256: ISAKMP:      encryption 3DES-CBC
*Jun 19 12:28:44.256: ISAKMP:      hash MD5
*Jun 19 12:28:44.256: ISAKMP:      default group 2
*Jun 19 12:28:44.256: ISAKMP:      auth pre-share
*Jun 19 12:28:44.256: ISAKMP:      life type in seconds
*Jun 19 12:28:44.256: ISAKMP:      life duration (VPI) of  0x0 0x1
0x51 0x80
```

```
*Jun 19 12:28:44.256: ISAKMP:(0):atts are acceptable. Next payload is 0
*Jun 19 12:28:44.256: ISAKMP:(0):Acceptable atts:actual life: 0
*Jun 19 12:28:44.257: ISAKMP:(0):Acceptable atts:life: 0
*Jun 19 12:28:44.257: ISAKMP:(0):Fill atts in sa vpi_length:4
*Jun 19 12:28:44.257: ISAKMP:(0):Fill atts in sa life_in_seconds:86400
*Jun 19 12:28:44.257: ISAKMP:(0):Returning Actual lifetime: 86400
*Jun 19 12:28:44.257: ISAKMP:(0)::Started lifetime timer: 86400.

*Jun 19 12:28:44.257: ISAKMP:(0): processing vendor id payload
*Jun 19 12:28:44.257: ISAKMP:(0): vendor ID seems Unity/DPD but major
69 mismatch
*Jun 19 12:28:44.257: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 12:28:44.257: ISAKMP:(0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.257: ISAKMP:(0):Old State = IKE_I_MM2  New State =
IKE_I_MM2

*Jun 19 12:28:44.257: ISAKMP:(0): sending packet to 192.168.0.1 my_port
500 peer_port 500 (I) MM_SA_SETUP
```

3. R1 reçoit MM3 de R2. À ce stade, R1 ne sait pas quel profil ISAKMP utiliser, donc il ne sait pas quel clavier utiliser. R1 utilise donc la première sonnerie de la configuration globale, qui est keyring1. R1 utilise cette clé pré-partagée pour les calculs DH et envoie MM4 :

```
*Jun 19 12:28:44.263: ISAKMP:(0):found peer pre-shared key matching
192.168.0.2
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID is DPD
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.263: ISAKMP:(1012): speaking to another IOS box!
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID seems Unity/DPD but major
151 mismatch
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID is XAUTH
*Jun 19 12:28:44.263: ISAKMP:received payload type 20
*Jun 19 12:28:44.263: ISAKMP (1012): His hash no match - this node
outside NAT
*Jun 19 12:28:44.263: ISAKMP:received payload type 20
*Jun 19 12:28:44.263: ISAKMP (1012): No NAT Found for self or peer
*Jun 19 12:28:44.263: ISAKMP:(1012):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.263: ISAKMP:(1012):Old State = IKE_R_MM3  New State =
IKE_R_MM3
*Jun 19 12:28:44.263: ISAKMP:(1012): sending packet to 192.168.0.2 my_port
500 peer_port 500 (R) MM_KEY_EXC
```

4. R2 reçoit MM4 de R1, utilise la clé pré-partagée de keyring1 afin de calculer DH et prépare le paquet MM5 et l'IKEID :

```
*Jun 19 12:28:44.269: ISAKMP:(0):Found ADDRESS key in keyring keyring1
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): vendor ID is Unity
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): vendor ID is DPD
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): speaking to another IOS box!
*Jun 19 12:28:44.269: ISAKMP:received payload type 20
*Jun 19 12:28:44.269: ISAKMP (1012): His hash no match - this node
outside NAT
*Jun 19 12:28:44.269: ISAKMP:received payload type 20
*Jun 19 12:28:44.269: ISAKMP (1012): No NAT Found for self or peer
```

```
*Jun 19 12:28:44.269: ISAKMP:(1012):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.269: ISAKMP:(1012):Old State = IKE_I_MM4  New State =
IKE_I_MM4

*Jun 19 12:28:44.270: ISAKMP:(1012):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 19 12:28:44.270: ISAKMP (1012): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.2
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 12:28:44.270: ISAKMP:(1012):Total payload length: 12
*Jun 19 12:28:44.270: ISAKMP:(1012): sending packet to 192.168.0.1
my_port 500 peer_port 500 (I) MM_KEY_EXCH
```

5. R1 reçoit MM5 de R1. Étant donné que l'IKEID est égal à 192.168.0, le profil2 a été sélectionné. Keyring2 a été configuré dans profile2 et keyring2 est donc sélectionné. Auparavant, pour le calcul DH dans MM4, R1 sélectionnait le premier trousseau de clés configuré, qui était keyring1. Même si les mots de passe sont exactement identiques, la validation de la sonnerie de clés échoue car il s'agit d'objets de sonnerie différents :

```
*Jun 19 12:28:44.270: ISAKMP (1012): received packet from 192.168.0.2
dport 500 sport 500 Global (R) MM_KEY_EXCH
*Jun 19 12:28:44.270: ISAKMP:(1012):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
*Jun 19 12:28:44.270: ISAKMP:(1012):Old State = IKE_R_MM4  New State =
IKE_R_MM5

*Jun 19 12:28:44.270: ISAKMP:(1012): processing ID payload. message ID = 0
*Jun 19 12:28:44.270: ISAKMP (1012): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.2
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 12:28:44.270: ISAKMP:(0):: peer matches profile2 profile
*Jun 19 12:28:44.270: ISAKMP:(1012):Found ADDRESS key in keyring keyring2
*Jun 19 12:28:44.270: ISAKMP:(1012):Key not found in keyrings of profile ,
aborting exchange
*Jun 19 12:28:44.270: ISAKMP (1012): FSM action returned error: 2
```

Débogues pour différentes clés prépartagées

Les scénarios précédents utilisaient la même clé ('cisco'). Ainsi, même lorsque la sonnerie incorrecte a été utilisée, le paquet MM5 a pu être déchiffré correctement et abandonné ultérieurement en raison d'une défaillance de validation de la sonnerie.

Dans les scénarios où différentes clés sont utilisées, MM5 ne peut pas être déchiffré et ce message d'erreur apparaît :

```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
```

failed its sanity check or is malformed

Critères de sélection du clavier

Voici un résumé des critères de sélection des touches. Reportez-vous aux sections suivantes pour plus de détails.

	Initiateur	Répondeur
Plusieurs clés avec des adresses IP différentes	Configuré. Si ce n'est pas explicitement configuré, le plus spécifique de la configuration	Correspondance la plus spécifique
Sonneries multiples avec les mêmes adresses IP	Configuré. Si elle n'est pas explicitement configurée **configuration devient imprévisible et non prise en charge. Il ne faut pas configurer deux clés pour la même adresse IP.**	**La configuration devient imprévisib n'est plus prise en charge. Il ne fau configurer deux clés pour la même adresse IP.**

Cette section décrit également pourquoi la présence d'une combinaison de touches par défaut (configuration globale) et de touches spécifiques peut entraîner des problèmes et explique pourquoi l'utilisation du protocole IKEv2 évite de tels problèmes.

Ordre de sélection du clavier sur l'initiateur IKE

Pour la configuration avec une VTI, l'initiateur utilise une interface de tunnel spécifique qui pointe vers un profil IPSec spécifique. Comme le profil IPSec utilise un profil IKE spécifique avec une sonnerie spécifique, il n'y a aucune confusion quant à la sonnerie à utiliser.

Crypto-map, qui pointe également vers un profil IKE spécifique avec une clé spécifique, fonctionne de la même manière.

Cependant, il n'est pas toujours possible de déterminer à partir de la configuration quel clavier utiliser. Par exemple, cela se produit lorsqu'aucun profil IKE n'est configuré, c'est-à-dire que le profil IPSec n'est pas configuré pour utiliser le profil IKE :

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.0 255.255.255.0 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel

crypto ipsec profile profile1
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
```

Si cet initiateur IKE tente d'envoyer MM1, il choisira la combinaison de touches la plus spécifique :

```
*Oct  7 08:13:58.413: ISAKMP: Locking peer struct 0xF4803B88, refcount 1 for
```

```
isakmp_initiator
*Oct  7 08:13:58.413: ISAKMP:(0):Can not start Aggressive mode, trying Main mode.
*Oct  7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 not available in default
*Oct  7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 found in keyring1
*Oct  7 08:13:58.413: ISAKMP:(0):ISAKMP: Selecting  192.168.0.0,255.255.255.0
as  key
*Oct  7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 found in keyring2
*Oct  7 08:13:58.413: ISAKMP:(0):ISAKMP: Selecting  192.168.0.2,255.255.255.255
as final key
*Oct  7 08:13:58.413: ISAKMP:(0):found peer pre-shared key matching 192.168.0.2
```

Comme aucun profil IKE n'est configuré pour l'initiateur lorsqu'il reçoit MM6, il ne touche pas un profil et se termine avec une authentification réussie et un mode rapide (QM) :

```
Oct  7 08:13:58.428: ISAKMP:(0):: peer matches *none* of the profiles
*Oct  7 08:13:58.428: ISAKMP:(1005): processing HASH payload. message ID = 0
*Oct  7 08:13:58.428: ISAKMP:(1005):SA authentication status:
        authenticated
*Oct  7 08:13:58.432: ISAKMP:(1005):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
```

Ordre de sélection du clavier sur le répondeur IKE - Différentes adresses IP

Le problème avec la sélection de la sonnerie se trouve sur le répondeur. Lorsque les sonneries utilisent des adresses IP différentes, l'ordre de sélection est simple.

Supposez que le répondeur IKE a cette configuration :

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.0 255.255.0.0 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco2
```

Lorsque ce répondeur reçoit le paquet MM1 de l'initiateur IKE avec l'adresse IP 192.168.0.2, il choisit la meilleure correspondance (la plus spécifique), même si l'ordre dans la configuration est différent.

Les critères d'ordre de sélection sont les suivants :

1. Seules les clés avec une adresse IP sont prises en compte.
2. Le routage et le transfert virtuels (VRF) du paquet entrant est vérifié (VRF frontal [fVRF]).
3. Si le paquet se trouve dans le VRF par défaut, la sonnerie globale est d'abord vérifiée. La clé la plus précise (longueur du masque de réseau) est sélectionnée.
4. Si aucune clé n'est trouvée dans la sonnerie par défaut, toutes les sonneries correspondant à ce fVRF sont concaténées.
5. La clé la plus précise (masque de réseau le plus long) correspond. Par exemple, un /32 est préféré à un /24.

Les débogages confirment la sélection :

```
R1#debug crypto isakmp detail
Crypto ISAKMP internals debugging is on

*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 not available in default
*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 found in keyring1
*Oct  2 11:57:13.301: ISAKMP:(0):ISAKMP: Selecting  192.168.0.0,255.255.255.0
as  key
```

```
*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 found in keyring2
*Oct  2 11:57:13.301: ISAKMP:(0):ISAKMP: Selecting  192.168.0.2,255.255.255.255
as final key
```

Ordre de sélection du clavier sur le répondeur IKE - Mêmes adresses IP

Lorsque les sonneries utilisent les mêmes adresses IP, des problèmes se produisent. Supposez que le répondeur IKE a cette configuration :

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.2 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco
```

Cette configuration devient imprévisible et n'est plus prise en charge. Il ne faut pas configurer deux clés pour la même adresse IP ou le problème décrit dans R2 As IKE Initiator (Incorrect) se produira.

Configuration globale du clavier

Les clés ISAKMP définies dans la configuration globale appartiennent à la clé par défaut :

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.0 255.255.0.0 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco2
crypto isakmp key cisco3 address 0.0.0.0
```

Bien que la clé ISAKMP soit la dernière dans la configuration, elle est traitée comme la première sur le répondeur IKE :

```
R1#show crypto isakmp key
Keyring      Hostname/Address                            Preshared Key

default      0.0.0.0        [0.0.0.0]                    cisco3

keyring1     192.168.0.0    [255.255.0.0]                cisco

keyring2     192.168.0.2                                 cisco2
```

Ainsi, l'utilisation de la configuration globale et des trousseaux de clés spécifiques est très risquée et pourrait conduire à des problèmes.

Clavier sur IKEv2 - Problème non survenu

Bien que le protocole IKEv2 utilise des concepts similaires à IKEv1, la sélection de la sonnerie ne provoque pas de problèmes similaires.

Dans des cas simples, il n'y a que quatre paquets échangés. L'IKEID qui détermine quel profil IKEv2 doit être sélectionné sur le répondeur est envoyé par l'initiateur dans le troisième paquet. Le troisième paquet est déjà chiffré.

La plus grande différence dans les deux protocoles est que IKEv2 utilise uniquement le résultat DH pour le calcul de clé. La clé pré-partagée n'est plus nécessaire pour calculer la clé utilisée pour le chiffrement/déchiffrement.

La RFC IKEv2 (5996, section 2.14), stipule :

Les clés partagées sont calculées comme suit. Une quantité appelée SKEYSEED est calculée à partir des nonces échangées pendant l'échange IKE_SA_INIT et du secret partagé Diffie-Hellman établi pendant cet échange.

Dans la même section, la RFC note également :

```
SKEYSEED = prf(Ni | Nr, g^ir)
```

Toutes les informations nécessaires sont envoyées dans les deux premiers paquets, et il n'est pas nécessaire d'utiliser une clé pré-partagée lors du calcul de SKEYSEED.

Comparez ceci avec la RFC IKE (2409, section 3.2), qui stipule :

SKEYID est une chaîne dérivée de matériel secret connu uniquement des joueurs actifs dans l'échange.

Ce « matériel secret connu seulement des joueurs actifs » est la clé pré-partagée. Dans la section 5, la RFC note également :

Pour les clés pré-partagées : SKEYID = prf(**clé pré-partagée**, Ni_b | Nr_b)

Ceci explique pourquoi la conception IKEv1 pour les clés pré-partagées entraîne tant de problèmes. Ces problèmes n'existent pas dans IKEv1 lorsque des certificats sont utilisés pour l'authentification.

Critères de sélection du profil IKE

Voici un résumé des critères de sélection de profil IKE. Reportez-vous aux sections suivantes pour plus de détails.

	Initiateur	Répondeur
Sélection du profil	Il doit être configuré (défini dans le profil IPSec ou dans la crypto-carte). Si ce n'est pas le cas, faites d'abord correspondre à partir de la configuration. L'homologue distant ne doit correspondre qu'à un profil ISAKMP spécifique, si l'identité de l'homologue est appariée dans deux profils ISAKMP, la configuration n'est pas valide.	Première correspondance de la configuration. L'homologue distant ne doit correspondre qu'à un profil ISAKMP spécifique, si l'ident de l'homologue est appariée dans deux profils ISAKMP, la configuration n'est pas valide.

Cette section décrit également les erreurs typiques qui se produisent lorsqu'un profil incorrect a été sélectionné.

Ordre de sélection de profil IKE sur l'initiateur IKE

L'interface VTI pointe généralement vers un profil IPSec spécifique avec un profil IKE spécifique. Le routeur sait alors quel profil IKE utiliser.

De même, la crypto-carte pointe vers un profil IKE spécifique, et le routeur sait quel profil utiliser en raison de la configuration.

Toutefois, il peut y avoir des scénarios où le profil n'est pas spécifié et où il n'est pas possible de déterminer directement à partir de la configuration quel profil utiliser ; dans cet exemple, aucun profil IKE n'est sélectionné dans le profil IPSec :

```
crypto isakmp profile profile1
  keyring keyring
  match identity address 192.168.0.0 255.255.255.0
crypto isakmp profile profile2
  keyring keyring
  match identity address 192.168.0.2 255.255.255.255

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel

crypto ipsec profile profile1
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
```

Lorsque cet initiateur tente d'envoyer un paquet MM1 à 192.168.0.2, le profil le plus spécifique est sélectionné :

```
*Oct  7 07:53:46.474: ISAKMP:(0): SA request profile is profile2
```

Ordre de sélection de profil IKE sur le répondeur IKE

L'ordre de sélection de profil d'un répondeur IKE est similaire à l'ordre de sélection de la sonnerie, où la priorité est la plus spécifique.

Assumez cette configuration :

```
crypto isakmp profile profile1
  keyring keyring
  match identity address 192.168.0.0 255.255.255.0
crypto isakmp profile profile2
  keyring keyring
  match identity address 192.168.0.1 255.255.255.255
```

Lorsqu'une connexion à partir de 192.168.0.1 est reçue, le profil2 est sélectionné.

L'ordre des profils configurés n'a pas d'importance. La commande **show running-config** place chaque nouveau profil configuré à la fin de la liste.

Parfois, le répondeur peut avoir deux profils IKE qui utilisent la même sonnerie. Si un profil incorrect est sélectionné sur le répondeur mais que la sonnerie sélectionnée est correcte, l'authentification se termine correctement :

```
*Oct  7 06:46:39.893: ISAKMP:(1003): processing ID payload. message ID = 0
*Oct  7 06:46:39.893: ISAKMP (1003): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.1
```

```
       protocol     : 17
       port         : 500
       length       : 12
*Oct  7 06:46:39.893: ISAKMP:(0):: peer matches profile2 profile
*Oct  7 06:46:39.893: ISAKMP:(0):key for 192.168.0.1 not available in default
*Oct  7 06:46:39.893: ISAKMP:(0):key for 192.168.0.1 found in keyring
*Oct  7 06:46:39.893: ISAKMP:(0):ISAKMP: Selecting  192.168.0.1,255.255.255.255
as final key

*Oct  7 06:46:39.893: ISAKMP:(1003):SA authentication status:
       authenticated
*Oct  7 06:46:39.893: ISAKMP:(1003):SA has been authenticated with 192.168.0.1
*Oct  7 06:46:39.893: ISAKMP:(1003):SA authentication status:
       authenticated

*Oct  7 06:46:39.893: ISAKMP:(1003):Old State = IKE_R_MM5  New State =
IKE_P1_COMPLETE
```

Le répondeur reçoit et accepte la proposition QM et tente de générer les index de paramètres de sécurité IPSec (SPI). Dans cet exemple, certains débogages ont été supprimés pour plus de clarté :

```
*Oct  7 06:46:39.898: ISAKMP:(1003):Checking IPSec proposal 1
*Oct  7 06:46:39.898: ISAKMP:(1003):atts are acceptable.
*Oct  7 06:46:39.898: IPSEC(validate_proposal_request): proposal part #1
```

Àce stade, le répondeur échoue et signale que le profil ISAKMP correct ne correspond pas :

```
 (key eng. msg.) INBOUND local= 192.168.0.2:0, remote= 192.168.0.1:0,
   local_proxy= 192.168.0.2/255.255.255.255/47/0,
   remote_proxy= 192.168.0.1/255.255.255.255/47/0,
   protocol= ESP, transform= NONE  (Tunnel),
   lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Oct  7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct  7 06:46:39.898: Crypto mapdb : proxy_match
       src addr     : 192.168.0.2
       dst addr     : 192.168.0.1
       protocol     : 47
       src port     : 0
       dst port     : 0
*Oct  7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct  7 06:46:39.898: Crypto mapdb : proxy_match
       src addr     : 192.168.0.2
       dst addr     : 192.168.0.1
       protocol     : 47
       src port     : 0
       dst port     : 0
*Oct  7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct  7 06:46:39.898: map_db_find_best did not find matching map
*Oct  7 06:46:39.898: IPSEC(ipsec_process_proposal): proxy identities not
supported
*Oct  7 06:46:39.898: ISAKMP:(1003): IPSec policy invalidated proposal with
error 32
*Oct  7 06:46:39.898: ISAKMP:(1003): phase 2 SA policy not acceptable!
(local 192.168.0.2 remote 192.168.0.1)
*Oct  7 06:46:39.898: ISAKMP: set new node 1993778370 to QM_IDLE
R2#
*Oct  7 06:46:39.898: ISAKMP:(1003):Sending NOTIFY PROPOSAL_NOT_CHOSEN
protocol 3
```

En raison de la sélection incorrecte du profil IKE, l'erreur 32 est renvoyée et le répondeur envoie le

message PROPOSAL_NOT_CHOSEN.

Résumé

Pour IKEv1, une clé pré-partagée est utilisée avec les résultats DH afin de calculer la clé utilisée pour le chiffrement qui commence à MM5. Après avoir reçu MM3, le récepteur ISAKMP n'est pas encore en mesure de déterminer quel profil ISAKMP (et la clé associée) doit être utilisé car l'IKEID est envoyé dans MM5 et MM6.

Le résultat est que le répondeur ISAKMP essaie de rechercher dans toutes les clés définies globalement afin de trouver la clé pour un homologue spécifique. Pour différentes adresses IP, la meilleure combinaison de touches (la plus spécifique) est sélectionnée ; pour la même adresse IP, la première clé correspondante de la configuration est utilisée. La clé est utilisée afin de calculer la clé qui est utilisée pour le déchiffrement de MM5.

Après avoir reçu MM5, l'initiateur ISAKMP détermine le profil ISAKMP et la sonnerie associée. L'initiateur effectue une vérification s'il s'agit du même trousseau de clés sélectionné pour le calcul DH MM4 ; sinon, la connexion échoue.

L'ordre des sonneries configurées dans la configuration globale est critique. Ainsi, pour le répondeur ISAKMP, utilisez une seule clé avec plusieurs entrées chaque fois que possible.

Les clés pré-partagées définies en mode de configuration globale appartiennent à une clé prédéfinie appelée default. Les mêmes règles s'appliquent alors.

Pour la sélection du profil IKE pour le répondeur, le profil le plus spécifique est mis en correspondance. Pour l'initiateur, le profil de la configuration est utilisé ou, si cela ne peut pas être déterminé, la meilleure correspondance est utilisée.

Un problème similaire se produit dans les scénarios qui utilisent différents certificats pour différents profils ISAKMP. L'authentification peut échouer en raison de la validation du profil 'ca trust-point' lorsqu'un autre certificat est choisi. Ce problème sera traité dans un document distinct.

Les problèmes décrits dans cet article ne sont pas spécifiques à Cisco, mais sont liés aux limites de la conception de protocole IKEv1. IKEv1 utilisé avec les certificats ne possède pas ces limitations, et IKEv2 utilisé pour les clés prépartagées et les certificats n'a pas ces limitations.

Informations connexes

- Section Certificate to ISAKMP Profile Mapping du Guide de configuration d'Internet Key Exchange pour VPN IPsec, Cisco IOS version 15M&T
- ca trust-point via clear eou section de référence des commandes de sécurité Cisco IOS : Commandes A à C
- Support et documentation techniques - Cisco Systems