Règles de sélection IOS IKEv1/IKEv2 pour des keyrings et des profils - guide de dépannage

Contenu

Introduction

Ce document décrit l'utilisation de plusieurs keyrings pour des plusieurs associations de sécurité Internet et des profils de protocole de gestion de clés (ISAKMP) dans un scénario de l'entre réseaux locaux VPN de logiciel de Cisco IOS®. Lui couvre le comportement de la version du logiciel Cisco IOS 15.3T aussi bien que les problèmes potentiels quand de plusieurs keyrings sont utilisés.

Deux scénarios sont présentés, basé sur un tunnel VPN avec deux profils d'ISAKMP sur chaque routeur. Chaque profil a un keyring différent avec la même adresse IP reliée. Les scénarios expliquent que le tunnel VPN peut être initié seulement d'un côté de la connexion en raison de la sélection et de la vérification de profil.

Les sections suivantes du document récapitulent les critères de sélection pour le profil de keyring pour le demandeur d'Échange de clés Internet (IKE) et le responder d'IKE. Quand différentes adresses IP sont utilisées par le keyring sur le responder d'IKE, la configuration fonctionne correctement, mais l'utilisation de la même adresse IP crée le problème présenté dans le premier scénario.

Les parties suivantes expliquent pourquoi la présence d'un keyring par défaut (configuration

globale) et les keyrings spécifiques pourraient mener aux problèmes et pourquoi l'utilisation du protocole de la version 2 d'échange de clés Internet (IKE) (IKEv2) évite ce problème.

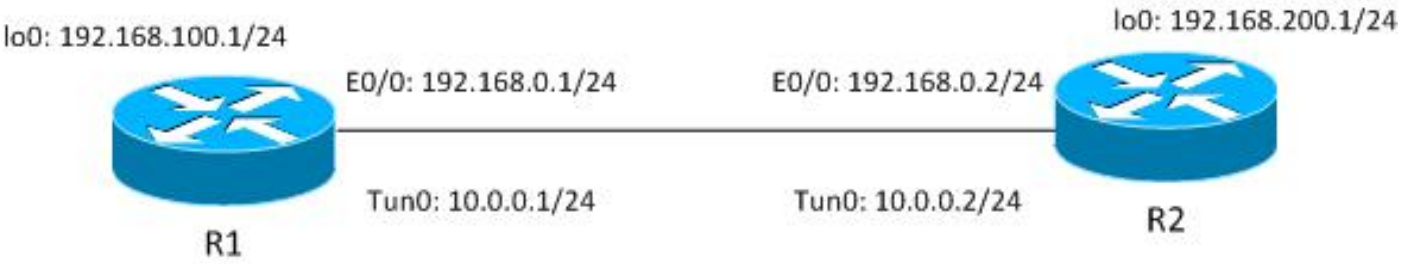
Les sections de finale présentent les critères de sélection pour le profil d'IKE pour chacun des deux pour le demandeur et le responder d'IKE, avec les erreurs typiques qui se produisent quand un profil incorrect est sélectionné.

Configuration

> Remarques :
>
> L'analyseur de Cisco CLI (clients enregistrés seulement) prend en charge certaines **commandes show**. Employez l'analyseur de Cisco CLI afin de visualiser une analyse de sortie de commande show.
>
> Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Topologie

Interfaces virtuelles de l'interface de tunnel d'utilisation Router1 (R1) et de Router2 (R2) (VTI) (Generic Routing Encapsulation [GRE]) afin d'accéder à ses bouclages. Ce VTI est protégé par IPSec (IPSec).



R1 et R2 ont deux profils d'ISAKMP, chacun avec le keyring différent. Tous les keyrings ont le même mot de passe.

Réseau R1 et VPN

La configuration pour le réseau R1 et le VPN est :

```
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 R2 et VPN

La configuration pour le réseau R2 et le VPN est :

```
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
```

Tous les keyrings utilisent la même adresse IP de pair et utilisent le mot de passe « Cisco. »

Sur R1, profile2 est utilisé pour la connexion VPN. Profile2 est le deuxième profil dans la configuration, qui utilise le deuxième keyring dans la configuration. Car vous verrez, la commande de keyring est essentielle.

Exemples de scénarios

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

Le deuxième scénario utilise la même topologie, mais a R2 comme demandeur d'ISAKMP quand la négociation phase1 manque.

La version 1 (IKEv1) d'échange de clés Internet (IKE) a besoin d'une clé pré-partagée pour le calcul de skey, qui est utilisé afin de déchiffrer/chiffre le paquet principal 5 (MM5) de mode et les paquets IKEv1 ultérieurs. Le skey est dérivé du calcul de Protocole DH (Diffie-Hellman) et de la clé pré-partagée. Que la clé pré-partagée doit être déterminée après que MM3 (responder) ou MM4 (demandeur) est reçu, de sorte que le skey, qui est utilisé dans MM5/MM6, peut être calculé.

Pour le responder d'ISAKMP dans MM3, le profil spécifique d'ISAKMP n'est pas encore déterminé parce que cela se produit après que l'IKEID soit reçu dans MM5. Au lieu de cela, tous les keyrings sont recherchés une clé pré-partagée, et le premier ou mieux assorti keyring de la configuration globale est sélectionné. Ce keyring est utilisé afin de calculer le skey qui est utilisé pour le déchiffrement de MM5 et le cryptage de MM6. Après le déchiffrement de MM5 et après le profil et le keyring associé d'ISAKMP sont déterminé, le responder d'ISAKMP exécute la vérification si le même keyring a été sélectionné ; si le même keyring n'est pas sélectionné, la connexion est abandonnée.

Ainsi, pour le responder d'ISAKMP, vous devriez utiliser un keyring simple avec des plusieurs entrées autant que possible.

R1 comme demandeur d'IKE (correct)

Ce scénario décrit ce qui se produit quand R1 est le demandeur d'IKE :

1. Utilisez ces derniers met au point pour R1 et R2 :

```
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
```

2. R1 initie le tunnel, envoie le paquet MM1 avec des propositions de stratégie, et reçoit MM2 dans la réponse. MM3 est alors 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 début, R1 sait que l'ISAKMP profile2 devrait être utilisé parce qu'il est lié sous le profil IPSec utilisé pour celui VTI.

Ainsi, le keyring correct (keyring2) a été sélectionné. La clé pré-partagée de keyring2 est utilisée comme matériel de base pour des calculs CAD quand le paquet MM3 est préparé.

3. Quand R2 reçoit ce paquet MM3, il ne sait toujours pas quel profil d'ISAKMP devrait être utilisé, mais il a besoin d'une clé pré-partagée pour la génération CAD. C'est pourquoi R2 recherche tous les keyrings afin de trouver la clé pré-partagée pour ce pair :

```
*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 pour 192.168.0.1 a été trouvée dans le premier keyring défini (keyring1).

4. R2 prépare alors le paquet MM4 avec des calculs CAD et avec la clé de « 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. Quand R1 reçoit MM4, il prépare le paquet MM5 avec IKEID et avec la clé correcte sélectionnée plus tôt (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 de 192.168.0.1, est reçu par R2. En ce moment, R2 sait à quel profil d'ISAKMP que le trafic devrait être lié (l'**addresscommand de match identity**) :

```
*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 exécute maintenant la vérification si le keyring qui a été aveuglément sélectionné pour le paquet MM4 est identique que le keyring configuré pour le profil d'ISAKMP maintenant choisi. Puisque keyring1 est le premier dans la configuration, il a été sélectionné précédemment, et il est sélectionné maintenant. La validation est réussie, 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'exécuter la vérification du keyring parce qu'on l'a connu du premier paquet ; le demandeur savent toujours quel profil d'ISAKMP à utiliser-et quel keyring est associé avec ce profil. L'authentification est réussie, et Phase1 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. Les débuts Phase2 normalement et est avec succès terminés.

Ce scénario fonctionne correctement seulement en raison de l'ordre approprié de keyrings définis sur R2. Le profil qui devrait être utilisé pour la session VPN utilise le keyring qui était premier dans la configuration.

R2 comme demandeur d'IKE (incorrect)

Ce scénario décrit ce qui se produit quand R2 initie le même tunnel et explique pourquoi le tunnel ne sera pas établi. Quelques logs ont été retirés afin de se concentrer sur les différences entre ceci et l'exemple précédent :

1. R2 initie le tunnel :

```
*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
```

2. Puisque R2 est le demandeur, le profil et le keyring d'ISAKMP sont connus. La clé pré-partagée de keyring1 est utilisée pour des calculs CAD et est introduite MM3. R2 reçoit MM2 et prépare MM3 basé sur 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 d'ISAKMP à l'utiliser, ainsi lui ne connaît pas quel keyring à l'utiliser. R1 utilise ainsi le premier keyring de la configuration globale, qui est keyring1. L'utilisation R1 qui clé pré-partagée pour des calculs CAD 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, emploie la clé pré-partagée de keyring1 afin de calculer le CAD, 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. Puisque l'IKEID égale 192.168.0, profile2 a été sélectionné. Keyring2 a été configuré dans profile2 ainsi keyring2 est sélectionné. Précédemment, pour le calcul CAD dans MM4, R1 a sélectionné le premier keyring configuré, qui était keyring1. Quoique les mots de passe soient exactement identiques, la validation pour le keyring échoue parce que ce sont différents objets de keyring :

```
*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
```

Debugs pour la clé pré-partagée différente

Les scénarios précédents ont utilisé la même clé ("Cisco "). Ainsi, même lorsque le keyring incorrect a été utilisé, le paquet MM5 pourrait être déchiffré correctement et lâché plus tard en raison de la panne de validation de keyring.

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 de keyring

C'est un résumé des critères de sélection de keyring. Voyez les sections suivantes pour des détails supplémentaires.

	Demandeur	Responder
Plusieurs	Configuré. Sinon a explicitement configuré la plupart	La correspondance la plus spécific

keyrings avec différentes adresses IP	de particularité de la configuration	
Plusieurs keyrings avec les mêmes adresses IP	Configuré. Sinon la **configuration** explicitement configurée **devient imprévisible et non prise en charge. On ne devrait pas configurer deux clés pour la même adresse IP.**	**La configuration devient imprévisib non prise en charge. On ne devrait configurer deux clés pour la même adresse IP.**

Cette section également décrit pourquoi la présence d'un keyring par défaut (configuration globale) et les keyrings spécifiques pourrait mener aux problèmes et explique pourquoi l'utilisation du protocole IKEv2 évite de tels problèmes.

Commande de sélection de keyring sur le demandeur d'IKE

Pour la configuration avec un VTI, le demandeur utilise une interface de tunnel spécifique ces points au profil IPSec spécifique. Puisque le profil IPSec utilise un profil spécifique d'IKE avec un keyring spécifique, il n'y a aucune confusion au-dessus dont keyring à l'utiliser.

Le crypto map, qui indique également un profil spécifique d'IKE avec un keyring spécifique, fonctionne de la même manière.

Cependant, il n'est pas toujours possible de déterminer à partir de la configuration qui keyring à l'utiliser. Par exemple, ceci se produit quand il n'y a aucun profil d'IKE configuré - c.-à-d., le profil IPSec n'est pas configuré afin d'utiliser le profil d'IKE :

```
*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
```

Si les essais de ce demandeur d'IKE pour envoyer MM1, il choisiront le keyring le 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
```

Puisque le demandeur n'a aucun profil d'IKE configuré quand il reçoit MM6, il ne frappera pas un profil et se terminera avec l'authentification réussie et le 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
```

Commande de sélection de keyring sur le responder d'IKE - Différentes adresses IP

Le problème avec la sélection de keyring est sur le responder. Quand les keyrings utilisent

différentes adresses IP, la commande de sélection est simple.

Supposez que le responder d'IKE a cette configuration :

```
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
```

Quand ce responder reçoit le paquet MM1 du demandeur d'IKE avec l'adresse IP 192.168.0.2, elle choisira la meilleure correspondance (de la plupart de particularité), même lorsque la commande dans la configuration est différente.

Les critères pour la commande de sélection sont :

1. Seulement des clés avec une adresse IP sont considérées.
2. Le routage et l'expédition virtuels (VRF) du paquet entrant est vérifié (VRF de frontal [fVRF]).
3. Si le paquet est dans le VRF par défaut, le keyring global est vérifié d'abord. La clé la plus précise (longueur de netmask) est sélectionnée.
4. Si aucune clé n'est trouvée dans le keyring par défaut, tous les keyrings qui apparient ce fVRF sont concaténés.
5. La clé la plus précise (le plus long netmask) est appariée. Par exemple, /32 est préféré au-dessus de /24.

Met au point 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
```

Commande de sélection de keyring sur le responder d'IKE - Les mêmes adresses IP

Quand les keyrings utilise les mêmes adresses IP, les problèmes se posent. Supposez que le responder d'IKE a cette configuration :

```
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
```

Cette configuration devient imprévisible et non prise en charge. On ne devrait pas configurer deux clés pour la même adresse IP ou le problème décrit dans R2 que le demandeur d'IKE (incorrect) se produira.

Configuration globale de keyring

Les clés d'ISAKMP définies en configuration globale appartiennent au keyring par défaut :

```
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
```

Quoique la clé d'ISAKMP soit dernière dans la configuration, elle est traitée en tant que premier sur le responder d'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 keyrings de particularité est très risquée et pourrait mener aux problèmes.

Keyring sur IKEv2 - Le problème ne se pose pas

Bien que le protocole IKEv2 utilise les concepts semblables à IKEv1, la sélection de keyring ne pose pas les problèmes semblables.

Dans des cas simples, il y a juste quatre paquets permutés. L'IKEID qui détermine quel profil IKEv2 devrait être sélectionné sur le responder est envoyé par le demandeur dans le troisième paquet. Le troisième paquet est déjà chiffré.

La plus grande différence dans les deux protocoles est qu'IKEv2 utilise seulement le résultat CAD pour le calcul de skey. La clé pré-partagée n'est plus nécessaire afin de calculer le skey utilisé pour le cryptage/déchiffrement.

Le RFC IKEv2 (5996, section 2.14), états :

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

Dans la même section, RFC les notes également :

```
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
```

Toutes les informations nécessaires sont introduites les deux premiers paquets, et il n'y a aucun besoin d'utiliser une clé pré-partagée quand SKEYSEED est calculé.

Comparez ceci au RFC d'IKE (2409, section 3.2), qui énonce :

SKEYID est une chaîne dérivée du contenu secret connu seulement aux lecteurs actifs dans l'échange.

Ce « contenu secret connu seulement aux lecteurs actifs » est la clé pré-partagée. Dans la section 5, RFC les notes également :

Pour des clés pré-partagées : SKEYID = PRF (**pre-shared-key**, Ni_b | Nr_b)

Ceci explique pourquoi la conception IKEv1 pour des clés pré-partagées pose tant de problèmes. Ces problèmes n'existent pas dans IKEv1 quand des Certificats sont utilisés pour l'authentification.

Critères de sélection de profil d'IKE

C'est un résumé des critères de sélection de profil d'IKE. Voyez les sections suivantes pour des détails supplémentaires.

	Demandeur	Responder
Sélection de profil	Il devrait être configuré (placez dans le profil IPSec ou dans le crypto map). Sinon correspondance configurée et première de la configuration. Le pair distant devrait apparier seulement un profil spécifique d'ISAKMP, si l'identité de pair est appariée dans deux profils d'ISAKMP, la configuration est non valide.	Première correspondance de la configuration. Le pair distant devrait apparier seulement profil spécifique d'ISAKMP, si l'identité de pair est appariée dans deux profils d'ISAKMP, la configuration est non valide.

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

Commande de sélection de profil d'IKE sur le demandeur d'IKE

L'interface VTI indique habituellement un profil IPSec spécifique avec un profil spécifique d'IKE. Le routeur sait alors quel profil d'IKE à l'utiliser.

De même, le crypto map indique un profil spécifique d'IKE, et le routeur sait quel profil à l'utiliser en raison de la configuration.

Cependant, il pourrait 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 qui profile pour l'utiliser ; dans cet exemple, aucun profil d'IKE n'est sélectionné dans le profil IPSec :

```
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
```

Quand des essais de ce demandeur pour envoyer un paquet MM1 à 192.168.0.2, le profil le plus spécifique est sélectionnés :

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

Commande de sélection de profil d'IKE sur le responder d'IKE

La commande de sélection de profil sur un responder d'IKE est semblable à la commande de sélection de keyring, où la plupart de particularité a la priorité.

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
```

Quand une connexion de 192.168.0.1 est reçue, profile2 sera sélectionné.

La commande des profils configurés n'importe pas. La commande de runnning-**config d'exposition** place chaque nouveau profil configuré à la fin de la liste.

Parfois le responder pourrait avoir deux profils d'IKE qui utilisent le même keyring. Si un profil incorrect est sélectionné sur le responder mais le keyring sélectionné est correct, l'authentification terminera 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 responder reçoit et reçoit la proposition et des essais QM pour générer les index de paramètre de sécurité IPSec (SPI). Dans cet exemple, une partie met au point a été retirée pour la 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
```

En ce moment, le responder échoue et les états que le profil correct d'ISAKMP n'a pas appariés :

```
 (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 de profil d'IKE, l'erreur 32 est retournée, et le responder envoie le message PROPOSAL_NOT_CHOSEN.

Résumé

Pour IKEv1, une clé pré-partagée est utilisée avec des résultats CAD afin de calculer le skey utilisé pour le cryptage qui commence à MM5. Après qu'il reçoive MM3, le récepteur d'ISAKMP ne peut pas encore déterminer quel profil d'ISAKMP (et keyring associé) devrait être utilisé parce que l'IKEID est introduit MM5 et MM6.

Le résultat est que les essais de responder d'ISAKMP aux rechercher par tous les keyrings globalement définis afin de trouver la clé pour le pair spécifique. Pour différentes adresses IP, le meilleur keyring assorti (la plupart de particularité) est sélectionné ; pour la même adresse IP, la première introduction assortie de la configuration est utilisée. Le keyring est utilisé afin de calculer le skey qui est utilisé pour le déchiffrement de MM5.

Après qu'il reçoive MM5, le demandeur d'ISAKMP détermine le profil d'ISAKMP et le keyring associé. Le demandeur exécute la vérification si c'est le même keyring qui a été sélectionné pour le calcul CAD MM4 ; autrement, la connexion échoue.

La commande des keyrings configurés en configuration globale est essentielle. Ainsi, pour le responder d'ISAKMP, utilisez un keyring simple avec des plusieurs entrées autant que possible.

Les clés pré-partagées qui sont définies en mode de configuration globale appartiennent à un keyring de prédéfinis appelé se transfèrent. Les mêmes règles s'appliquent alors.

Pour la sélection de profil d'IKE pour le responder, le profil le plus spécifique est apparié. Pour le demandeur, le profil de la configuration est utilisé, ou, si ce ne peut pas être déterminée, la meilleure correspondance est utilisée.

Un problème semblable se pose dans les scénarios qui utilisent différents Certificats pour différents profils d'ISAKMP. L'authentification pourrait échouer en raison de la validation de profil de « ca trust-point » quand un certificat différent est choisi. Ce problème sera couvert dans un document distinct.

Les questions décrites en cet article ne sont pas des problèmes de Cisco-particularité, mais sont liées aux limites de conception du protocole IKEv1. IKEv1 utilisé avec des Certificats n'a pas ces limites, et IKEv2 utilisé pour les deux clés et Certificats pré-partagés n'a pas ces limites.

Informations connexes

- Certificat à la section de mappage de profil d'ISAKMP de l'échange de clés Internet (IKE) pour le guide de configuration d'IPsec VPN, version de Cisco IOS 15M&T
- ca trust-point par la section de clear eou de référence de commandes de Cisco IOS Security : Commande A au C
- Support et documentation techniques - Cisco Systems