Dépannage des débogages ASA IPsec et IKE (mode principal IKEv1)

Contenu

Introduction

Ce document décrit les débogages sur l'ASA (Adaptive Security Appliance) lorsque le mode principal et la clé prépartagée (PSK) sont utilisés. La traduction de certaines lignes de débogage dans la configuration est également abordée.

Les sujets non abordés dans ce document incluent le passage du trafic après l'établissement du tunnel et les concepts de base d'IPsec ou d'Internet Key Exchange (IKE).

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants .

- PSK
- IKE

Components Used

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

- Cisco ASA 9.3.2
- Routeurs qui exécutent Cisco IOS® 12.4T

Problème principal

Les débogages IKE et IPsec sont parfois cryptiques, mais vous pouvez les utiliser pour comprendre où se trouve un problème d'établissement de tunnel VPN IPsec.

Scénario

Le mode principal est généralement utilisé entre des tunnels LAN à LAN ou, dans le cas d'un accès distant (EzVPN), lorsque des certificats sont utilisés pour l'authentification.

Les débogages proviennent de deux ASA qui exécutent le logiciel version 9.3.2. Les deux périphériques forment un tunnel LAN à LAN.

Deux scénarios principaux sont décrits :

- ASA comme initiateur pour IKE
- ASA comme répondeur pour IKE

Commandes de débogage utilisées

debug crypto ikev1 127

debug crypto ipsec 127

Configuration ASA

Configuration IPsec :

```
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
crypto map MAP 10 match address VPN
crypto map MAP 10 set peer 10.0.0.2
crypto map MAP 10 set transform-set TRANSFORM
crypto map MAP 10 set reverse-route
crypto map MAP interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
 pre-shared-key cisco
access-list VPN extended permit tcp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
```

Configuration IP :

```
ciscoasa#

show ip
```

```
System IP Addresses:
Interface                  Name      IP address      Subnet mask      Method
GigabitEthernet0/0       inside     192.168.1.1     255.255.255.0   manual
GigabitEthernet0/1       outside   10.0.0.1          255.255.255.0   manual
Current IP Addresses:
Interface                  Name       IP address      Subnet mask      Method
GigabitEthernet0/0       inside     192.168.1.1    255.255.255.0   manual
GigabitEthernet0/1       outside   10.0.0.1          255.255.255.0   manual
```

Configuration NAT :

```
object network INSIDE-RANGE
 subnet 192.168.1.0 255.255.255.0 object network FOREIGN_NETWORK
 subnet 192.168.2.0 255.255.255
nat (inside,outside) source static INSIDE-RANGE INSIDE-RANGE destination static
FOREIGN_NETWORK FOREIGN_NETWORK no-proxy-arp route-lookup
```

Débogage

Description du message de l'initiateur	Déboguages	Description du message du répondeur
L'échange en mode principal commence ; aucune stratégie n'a été partagée et les homologues sont toujours dans MM_NO_STATE.	[DEBUG IKEv1] : Pitcher : reçu un message d'acquisition de clé, spi 0x0 IPSEC(crypto_map_check)-3 : Recherche de crypto-carte correspondant à 5-tuple : Port=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, port=2816 IPSEC(crypto_map_check)-3 : Vérification de la carte de chiffrement MAP 10 : correspondant.	
En tant qu'initiateur, l'ASA commence à construire la charge utile.	[IKEv1] : IP = 10.0.0.2, initiateur IKE : Nouvelle phase 1, Intf inside, homologue IKE 10.0.0.2 adresse de proxy locale 192.168.1.0, adresse de proxy distante 192.168.2.0, carte de chiffrement (MAP)	
Construire MM1 Ce processus estcomprend iProposition initiale pour IKE et sFournisseurs NAT-T pris en charge.	[DEBUG IKEv1] : IP = 10.0.0.2, construction de la **charge utile ISAKMP SA** [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile NAT-Traversal VID ver 02 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile NAT-Traversal VID ver 03 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile NAT-Traversal VID ver RFC [DEBUG IKEv1] : IP = 10.0.0.2, construction de la trame VID + charge utile de fonctionnalités étendues	
Envoyez MM1.	[IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=0) avec charges utiles : HDR + SA (1) + VENDEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) + AUCUNE (0) longueur totale : 168	
	==========> ==========> ==========> ==========> ==========	
	[IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=0) avec charges utiles : HDR + SA (1) + VENDEUR (13) + VENDEUR (13) + VENDEUR (13) + VENDEUR (13) + AUCUNE (0) longueur totale : 164	MM1 reçu de l'initiateur.
	[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile SA	Processus MM1.
	[DEBUG IKEv1] : IP = 10.0.0.2, proposition Oakley acceptable	La comparaison des
	[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID	politiques
	[DEBUG IKEv1] : IP = 10.0.0.2, VID RFC NAT-Traversal reçu	ISAKMP/IKE
	[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID	commence.
	[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID	L'homologue distant
	[DEBUG IKEv1] : IP = 10.0.0.2, NAT-Traversal reçu ver 03 VID	annonce qu'il peut
	[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID	utiliser NAT-T.
	[DEBUG IKEv1] : IP = 10.0.0.2, NAT-Traversal reçu ver 02 VID	Configuration associée

:
crypto isakmp policy 10
authentication pre-share
cryptage 3des
hash sha
groupe 2
86400 à vie

[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile IKE SA

[DEBUG IKEv1] : IP = 10.0.0.2, proposition de SA IKE n° 1, transformation n° 1 correspondance acceptable entrée IKE n° 2 globale

Construire MM2. Dans ce message, le répondeur sélectionne les paramètres de stratégie isakmp à utiliser. Il annonce également les versions NAT-T qu'il peut utiliser.

[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile ISAKMP SA

[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile NAT-Traversal VID ver 02

[DEBUG IKEv1] : IP = 10.0.0.2, construction de la trame VID + charge utile de fonctionnalités étendues

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=0) avec charges utiles : HDR + SA (1) + VENDEUR (13) + VENDEUR (13) + AUCUNE (0) longueur totale : 128

Envoyez MM2.

<==========
==========
==========
==========
==========

MM2 reçu du répondeur.

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=0) avec charges utiles : HDR + SA (1) + VENDEUR (13) + AUCUNE (0) longueur totale : 104

Processus MM2.

[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile SA
[DEBUG IKEv1] : IP = 10.0.0.2, proposition Oakley acceptable
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID
[DEBUG IKEv1] : IP = 10.0.0.2, VID RFC NAT-Traversal reçu
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile clé
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile nonce
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile VID Cisco Unity
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile VID xauth V6
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, envoyer IOS VID
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, Constructing ASA spoofing IOS Vendor ID utiles (version : 1.0.0, fonctionnalités : 20000001)
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile VID
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, Envoyer Altiga/Cisco VPN3000/Cisco ASA GW VID
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile NAT-Discovery
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, calcul du hachage de découverte NAT
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile NAT-Discovery
30 nov 10:38:29 [DEBUG IKEv1] : IP = 10.0.0.2, calcul du hachage de découverte NAT

Construisez MM3. Ce processus estinclutles charges utiles de découverte NAT, Différer-Charges utiles d'échange de clés Hellman (DH) (i)l'initiateur inclut g, p et A au répondeur), et Prise en charge DPD.

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=0) avec charges utiles : HDR + KE (4) + NONCE (10) + VENDEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) + NAT-D (20) + NAT-D (20) + AUCUNE (0) longueur totale : 304

Envoyez MM3.

==========
==========>==========>==========>==========
==========>==========>==========>=
==========>==========>==========

```
================>================
[IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=0) avec
charges utiles : HDR + KE (4) + NONCE (10) + VENDEUR (13) +
VENDEUR (13) + VENDEUR (13) + NAT-D (130) + NAT-D (130) +
AUCUNE (0) longueur totale : 284
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile clé
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile ISA_KE
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile nonce
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID
[DEBUG IKEv1] : IP = 10.0.0.2, VID DPD reçu
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile IOS/PIX ID
fournisseur (version : 1.0.0, fonctionnalités : 00000f6f)
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID
[DEBUG IKEv1] : IP = 10.0.0.2, reçu xauth V6 VID
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile NAT-
Discovery
[DEBUG IKEv1] : IP = 10.0.0.2, calcul du hachage de découverte NAT
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile NAT-
Discovery
[DEBUG IKEv1] : IP = 10.0.0.2, calcul du hachage de découverte NAT
[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile clé
[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile nonce
[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile VID Cisco
Unity
[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile VID xauth
V6
[DEBUG IKEv1] : IP = 10.0.0.2, envoyer IOS VID
[DEBUG IKEv1] : IP = 10.0.0.2, Constructing ASA spoofing IOS Vendor
ID utiles (version : 1.0.0, fonctionnalités : 20000001)
[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile VID
[DEBUG IKEv1] : IP = 10.0.0.2, Send Altiga/Cisco VPN3000/Cisco ASA
GW VID
[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile NAT-
Discovery
[DEBUG IKEv1] : IP = 10.0.0.2, calcul du hachage de découverte NAT
[DEBUG IKEv1] : IP = 10.0.0.2, construction de la charge utile NAT-
Discovery
[DEBUG IKEv1] : IP = 10.0.0.2, calcul du hachage de découverte NAT
[IKEv1] : IP = 10.0.0.2, Connexion échouée sur tunnel_group 10.0.0.2
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Génération de clés pour
le répondeur...
[IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=0) avec
charges utiles : HDR + KE (4) + NONCE (10) + VENDEUR (13) +
FOURNISSEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) +
NAT-D (130) + NAT-D (130) + AUCUNE (0) longueur totale : 304
<================================================
================================================
================================================
================================================
=================================
[IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=0) avec
charges utiles : HDR + KE (4) + NONCE (10) + VENDEUR (13) +
FOURNISSEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) +
NAT-D (20) + NAT-D (20) + AUCUNE (0) longueur totale : 304
[DEBUG IKEv1] : IP = 10.0.0.2, traitement comme charge utile
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile ISA_KE
[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile nonce
```

MM3 reçu de l'initiateur.

Processus MM3. À partir des charges utiles NAT-D, le répondeur est en mesure de déterminer si le L'initiateur est derrière NAT et si le répondeur est derrière NAT.

À partir du DH KE, le répondeur de charge utile obtient les valeurs p, g et A.

Construisez MM4. Ce processus estinclut charge utile de découverte NAT, DH Rle répondeur génère « B » et « s » (renvoie « B » à l'initiateur), et VID DPD.

L'homologue est associé au groupe de tunnels L2L 10.0.0.2, et les clés de chiffrement et de hachage sont générées à partir des « s » ci-dessus et de la clé pré-partagée.

Envoyez MM4.

MM4 reçu du répondeur.

Processus MM4. À partir des charges utiles NAT-D,

l'initiateur est désormais en mesure de déterminer si L'initiateur est derrière NAT et si le répondeur est derrière NAT. De DH KE, iL'initiateur reçoit « B » et peut maintenant générer « s. » L'homologue est associé au groupe de tunnels L2L 10.0.0.2, et l'initiateur génère des clés de chiffrement et de hachage en utilisant « s » ci-dessus et la clé pré-partagée. Construisez MM5. Configuration associée : crypto isakmp identity auto Envoyer MM5. Le répondeur n'est derrière aucune NAT. Aucune NAT-T requise.	[DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID [DEBUG IKEv1] : IP = 10.0.0.2, VID du client Cisco Unity reçu [DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID [DEBUG IKEv1] : IP = 10.0.0.2, VID DPD reçu [DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID [DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile IOS/PIX ID fournisseur (version : 1.0.0, fonctionnalités : 00000f7f) [DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile VID [DEBUG IKEv1] : IP = 10.0.0.2, reçu xauth V6 VID [DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile NAT-Discovery [DEBUG IKEv1] : IP = 10.0.0.2, calcul du hachage de découverte NAT [DEBUG IKEv1] : IP = 10.0.0.2, traitement de la charge utile NAT-Discovery [DEBUG IKEv1] : IP = 10.0.0.2, calcul du hachage de découverte NAT [IKEv1] : IP = 10.0.0.2, Connexion échouée sur tunnel_group 10.0.0.2 [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Génération de clés pour l'initiateur... [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile d'ID [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile de hachage [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Hachage de calcul pour ISAKMP [DEBUG IKEv1] : IP = 10.0.0.2, Constructing IOS keep alive utiles : proposition=32767/32767 sec. [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile dpd vid [IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=0) avec charges utiles : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDEUR (13) + AUCUNE (0) longueur totale : 96 ==========>==========>==========>==========>==========>==========>==========>==========>==========>========== [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, État de détection NAT automatique : L'extrémité distante n'est PAS derrière un périphérique NAT Cette extrémité n'est PAS derrière un périphérique NAT [IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=0) avec charges utiles : HDR + ID (5) + HASH (8) + AUCUNE (0) longueur totale : 64 [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile de l'ID de traitement [DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID reçu 10.0.0.2 [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile de hachage [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Hachage de calcul pour ISAKMP	MM5 reçu de l'initiateur. Ce processus estcomprend remote peer identity (ID) et cAtterrissage de la connexion sur un groupe de tunnels particulier. Processus MM5. L'authentification avec les clés pré-partagées commence maintenant. L'authentification se produit sur les deux homologues ; par conséquent, vous

verrez deux jeux de processus d'authentification correspondants.

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile de notification
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, NAT automatique
[IKEv1] : IP = 10.0.0.2, Connexion échouée sur tunnel_group 10.0.0.2

Configuration associée :
tunnel group 10.0.0.2 type ipsec-l2l

État de la détection : L'extrémité distante n'est PAS derrière un périphérique NAT Cette extrémité n'est PAS derrière un périphérique NAT

Non NAT-T requis dans ce cas.

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile d'ID
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile de hachage
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Hachage de calcul pour ISAKMP
[DEBUG IKEv1] : IP = 10.0.0.2, Constructing IOS keep alive utiles : proposition=32767/32767 sec.
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile dpd vid
[IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=0) avec charges utiles : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDEUR (13) + AUCUNE (0) longueur totale : 96

Construisez MM6. Envoyer l'identité inclut les heures de démarrage de la clé et l'identité envoyée à l'homologue distant.

Envoyez MM6.

<==========
==========
==========
==========
==========

MM6 reçu du répondeur.

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=0) avec charges utiles : HDR + ID (5) + HASH (8) + AUCUNE (0) longueur totale : 64

[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, PHASE 1 TERMINÉE
[IKEv1] : IP = 10.0.0.2, type Keep-alive pour cette connexion : DPD
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Démarrage du minuteur de clé P1 : 64800 secondes.

Phase 1 terminée. Démarrez le minuteur isakmp rekey.
Configuration associée :
crypto isakmp policy 10
authentication pre-share
cryptage 3des
hash sha
groupe 2
86400 à vie
ciscoasa# sh run all crypto isakmp
crypto isakmp identity auto

Processus MM6. Ce processus estcomprend ridentité distante envoyée par peer et fdécision finale concernant le groupe de tunnels à choisir.

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile de l'ID de traitement
[DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID reçu
10.0.0.2
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile de hachage
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Hachage de calcul pour ISAKMP
[IKEv1] : IP = 10.0.0.2, Connexion échouée sur tunnel_group 10.0.0.2
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, mode rapide de démarrage d'Oakley
[DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE Initiator start QM : msg id = 7b80c2b0

Phase 1 terminée. Démarrez le minuteur ISAKMP Rekey. Connexe cconfiguration :

[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, PHASE 1 TERMINÉE
[IKEv1] : IP = 10.0.0.2, type Keep-alive pour cette connexion : DPD
La DPD a été négociée et la phase 1 est maintenant terminée.
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Démarrage du minuteur de clé P1 : 82080 secondes.

tunnel group 10.0.0.2 type ipsec-l2l
groupe de tunnels 10.0.0.2 ipsec-attributs
cisco à clé prépartagée

La phase 2 (mode rapide) commence.

IPSEC : Nouvelle SA embryonnaire créée @ 0x53FC3C00,
SCB : 0x53F90A00,
Direction : entrant
SPI : 0xFD2D851F
ID de session : 0x00006000
Numéro VPIF : 0x0000003
Type de tunnel : l2l
Protocole : esp
Durée de vie : 240 secondes

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE a obtenu SPI du moteur de clé : SPI = 0xfd2d851f

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, oakley en mode rapide

Construisez QM1. Ce processus comprend : ID proxy et IPsec politiques. Configuration associée :
jeu de transformation crypto ipsec TRANSFORM esp-aes esp-sha-hmac
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction d'une charge utile de hachage vide

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile IPSec SA

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de données utiles IPSec nonce

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de l'ID proxy

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID du proxy émetteur : Sous-réseau local : 192.168.1.0 masque 255.255.255.0 protocole 1 port 0
Sous-réseau distant : 192.168.2.0 Masque 255.255.255.0 Protocole 1 port 0
Le sous-réseau local (192.168.1.0/24) et le sous-réseau distant attendu (192.168.2.0/24) sont envoyés

[DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, initiateur IKE envoyant le contact initial

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile de hachage qm

[DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE Initiator envoyant 1er pkt QM : msg id = 7b80c2b0

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=7b80c2b0) avec charges utiles : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) longueur totale : 200

Envoyer QM1.

==========QM1==========>

[DÉCODE IKEv1] : IP = 10.0.0.2, IKE Responder démarrant QM : msg id = 52481cf5

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=52481cf5) avec charges utiles : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + AUCUNE (0) longueur totale : 172

QM1 reçu de l'initiateur.
Le répondeur démarre la phase 2 (QM).

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile de hachage

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile SA

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile nonce

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile de l'ID de traitement

Traiter QM1.
Ce processus compare les serveurs proxy distants aux serveurs locaux et sélectionne une adresse IP acceptablesec politique.
Configuration associée : crypto ipsec transformation-set TRANSFORM esp-aes esp-sha-hmac
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0

192.168.2.0
255.255.255.0
crypto map MAP 10
match address VPN

[DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID reçu—192.168.2.0—255.255.255.0[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Données de sous-réseau du proxy IP distant reçues dans ID Payload : Adresse 192.168.2.0, Masque 255.255.255.0, Protocole 1, Port 0
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile de l'ID de traitement
[DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID reçu—192.168.1.0—255.255.255.0
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Données de sous-réseau du proxy IP local reçues dans ID Payload : Adresse 192.168.1.0, Masque 255.255.255.0, Protocole 1, Port 0

Les sous-réseaux distants et locaux (192.168.2.0/24 et 192.168.1.0/24) sont reçus.

[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed old sa introuvable par addr
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, vérification de la carte de chiffrement statique, vérification de la carte = MAP, seq = 10...
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, vérification de la carte de chiffrement statique, carte MAP, seq = 10 est une correspondance réussie
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, homologue distant IKE configuré pour la carte de chiffrement : CARTE

Une entrée de chiffrement statique correspondante est recherchée et trouvée.

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile IPSec SA
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IPSec SA Proposition n° 1, Transformation n° 1 Correspondances acceptables IPSec SA n° 10 globale
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE : demande SPI
IPSEC : Nouvelle SA embryonnaire créée @ 0x53FC3698,
SCB : 0x53FC2998,
Direction : entrant
SPI : 0x1698CAC7
ID de session : 0x00004000
Numéro VPIF : 0x0000003
Type de tunnel : l2l
Protocole : esp
Durée de vie : 240 secondes
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE a obtenu SPI du moteur de clé : SPI = 0x1698cac7
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, oakley construisant le mode rapide
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction d'une charge utile de hachage vide
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile IPSec SA
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de données utiles IPSec nonce
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de l'ID proxy
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID du proxy émetteur : Sous-réseau distant : 192.168.2.0 Masque 255.255.255.0 Protocole 1 port 0 Sous-réseau local : 192.168.1.0 masque 255.255.255.0 protocole 1 port 0
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construction de la charge utile de hachage qm
[DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, répondeur IKE envoyant 2e paquet QM : msg id = 52481cf5

Construisez QM2. Ce processus estcomprend cConfirmation des identités proxy, du type de tunnel et d'une vérifie les listes de contrôle d'accès crypto mises en miroir.

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=52481cf5) avec charges utiles : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + AUCUNE (0) longueur totale : 172

Envoyez QM2.

<==========
==========

QM2 reçu du

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=7b80c2b0)

répondeur.	avec charges utiles : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) longueur totale : 200 [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile de hachage [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile SA [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile nonce [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile de l'ID de traitement [DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID reçu—192.168.1.0—255.255.255.0
Traiter QM2. Dans ce processus, remote end envoie les paramètres et les durées de vie de phase 2 les plus courtes sont choisies.	[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile de l'ID de traitement [DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID reçu—192.168.2.0—255.255.255.0 [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile de notification [DÉCODE IKEv1] : Le décodage de durée de vie du répondeur suit (hors SPI[4]|attributs) : [DÉCODE IKEv1] : 0000: DDE50931 80010001 00020004 00000E10 ...1..... [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, réponse forçant le changement de durée de reprise IPSec de 28 800 à 3 600 secondes en fonction de la réponse de l'homologue, l'ASA modifie certains attributs IPSEC. Dans ce cas, l'intervalle de retouche [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, chargement de toutes les SA IPSEC [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Génération de la clé de mode rapide !
La carte de chiffrement « MAP » et l'entrée 10 correspondant ont été trouvées et comparées à la liste d'accès « VPN ».	[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, règle de cryptage NP recherche la crypto map MAP 10 correspondant à ACL VPN : retourné cs_id=53f11198 ; règle=53f11a90
L'appliance a généré les SPI 0xfd2d851f et 0xdde50931pour le trafic entrant et sortant, respectivement.	[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Génération de la clé de mode rapide ! IPSEC : Nouvelle SA embryonnaire créée @ 0x53FC3698, SCB : 0x53F910F0, Direction : sortant SPI : 0xDDE50931 ID de session : 0x00006000 Numéro VPIF : 0x0000003 Type de tunnel : l2l Protocole : esp Durée de vie : 240 secondes IPSEC : Mise à jour OBSA de l'hôte terminée, SPI 0xDDE50931 IPSEC : Création du contexte VPN sortant, SPI 0xDDE50931 Indicatifs: 0x00000005 SA : 0x53FC3698 SPI : 0xDDE50931 MTU : 1500 bytes VCID : 0x00000000 Homologue : 0x00000000 SCB : 0x01CF218F Canal: 0x4C69CB80 IPSEC : Contexte VPN sortant terminé, SPI 0xDDE50931 Handle VPN : 0x000161A4 IPSEC : Nouvelle règle de chiffrement sortant, SPI 0xDDE50931 Adresse Src : 192.168.1.0 Masque Src : 255.255.255.0 Adresse Dst : 192.168.2.0

Masque Dst : 255.255.255.0
Ports Src
Supérieur : 0
Inférieur : 0
Op: ignorer
Ports Dst
Supérieur : 0
Inférieur : 0
Op: ignorer
Protocole : 1
Utiliser le protocole : vrai
SPI : 0x00000000
Utiliser SPI : faux
IPSEC : Règle de chiffrement sortant terminée, SPI 0xDDE50931
ID de règle : 0x53FC3AD8
IPSEC : Nouvelle règle d'autorisation de sortie, SPI 0xDDE50931
Adresse Src : 10.0.0.1
Masque Src : 255.255.255.255
Adresse Dst : 10.0.0.2
Masque Dst : 255.255.255.255
Ports Src
Supérieur : 0
Inférieur : 0
Op: ignorer
Ports Dst
Supérieur : 0
Inférieur : 0
Op: ignorer
Protocole : 50
Utiliser le protocole : vrai
SPI : 0xDDE50931
Utiliser SPI : vrai
IPSEC : Règle d'autorisation sortante terminée, SPI 0xDDE50931
ID de règle : 0x53F91538
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, règle de cryptage NP recherche la crypto map MAP 10 correspondant à ACL VPN : retourné cs_id=53f11198 ; règle=53f11a90
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, négociation de sécurité terminée pour le groupe LAN à LAN (10.0.0.2) Initiateur, SPI entrant = 0xfd2d851f, SPI sortant = 0xdde50931
IPSEC : Mise à jour IBSA de l'hôte terminée, SPI 0xFD2D851F
IPSEC : Création d'un contexte VPN entrant, SPI 0xFD2D851F
Indicatifs: 0x00000006
SA : 0x53FC3C00
SPI : 0xFD2D851F
MTU : 0 bytes
VCID : 0x00000000
Homologue : 0x000161A4
SCB : 0x01CEA8EF
Canal: 0x4C69CB80

Construisez QM3. Confirmer tous les SPI créés pour l'homologue distant.

IPSEC : Contexte VPN entrant terminé, SPI 0xFD2D851F
Handle VPN : 0x00018BBC
IPSEC : Mise à jour du contexte VPN sortant 0x000161A4, SPI 0xDDE50931
Indicatifs: 0x00000005
SA : 0x53FC3698
SPI : 0xDDE50931
MTU : 1500 bytes
VCID : 0x00000000
Homologue : 0x00018BBC
SCB : 0x01CF218F
Canal: 0x4C69CB80
IPSEC : Contexte VPN sortant terminé, SPI 0xDDE50931
Handle VPN : 0x000161A4

IPSEC : Règle interne sortante terminée, SPI 0xDDE50931
ID de règle : 0x53FC3AD8
IPSEC : Règle SPD externe sortante terminée, SPI 0xDDE50931
ID de règle : 0x53F91538
IPSEC : Nouvelle règle de flux de tunnel entrant, SPI 0xFD2D851F
Adresse Src : 192.168.2.0
Masque Src : 255.255.255.0
Adresse Dst : 192.168.1.0
Masque Dst : 255.255.255.0
Ports Src
Supérieur : 0
Inférieur : 0
Op: ignorer
Ports Dst
Supérieur : 0
Inférieur : 0
Op: ignorer
Protocole : 1
Utiliser le protocole : vrai
SPI : 0x00000000
Utiliser SPI : faux
IPSEC : Règle de flux de tunnel entrant terminée, SPI 0xFD2D851F
ID de règle : 0x53F91970
IPSEC : Nouvelle règle de déchiffrement entrant, SPI 0xFD2D851F
Adresse Src : 10.0.0.2
Masque Src : 255.255.255.255
Adresse Dst : 10.0.0.1
Masque Dst : 255.255.255.255
Ports Src
Supérieur : 0
Inférieur : 0
Op: ignorer
Ports Dst
Supérieur : 0
Inférieur : 0
Op: ignorer
Protocole : 50
Utiliser le protocole : vrai
SPI : 0xFD2D851F
Utiliser SPI : vrai
IPSEC : Règle de déchiffrement entrant terminée, SPI 0xFD2D851F
ID de règle : 0x53F91A08
IPSEC : Nouvelle règle d'autorisation entrante, SPI 0xFD2D851F
Adresse Src : 10.0.0.2
Masque Src : 255.255.255.255
Adresse Dst : 10.0.0.1
Masque Dst : 255.255.255.255
Ports Src
Supérieur : 0
Inférieur : 0
Op: ignorer
Ports Dst
Supérieur : 0
Inférieur : 0
Op: ignorer
Protocole : 50
Utiliser le protocole : vrai
SPI : 0xFD2D851F
Utiliser SPI : vrai
IPSEC : Règle d'autorisation entrante terminée, SPI 0xFD2D851F
ID de règle : 0x53F91AA0

Envoyez QM3.

[DÉCODE IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE Initiator envoyant 3ème pkt QM : msg id = 7b80c2b0

==========QM3==========
==========>

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE ENVOI (msgid=7b80c2b0) avec charges utiles : HDR + HASH (8) + AUCUN (0) longueur totale : 76

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE a obtenu un message KEY_ADD pour SA : SPI = 0xdde50931

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Pitcher : reçu KEY_UPDATE, spi 0xfd2d851f

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Démarrage du minuteur de clé P2 : 3060 secondes.

[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, PHASE 2 TERMINÉE (msgid=7b80c2b0)

Phase 2 terminée. L'initiateur est maintenant prêt à chiffrer et déchiffrer les paquets à l'aide de ces valeurs SPI.

[IKEv1] : IP = 10.0.0.2, message IKE_DECODE REÇU (msgid=52481cf5) avec charges utiles : HDR + HASH (8) + AUCUNE (0) longueur totale : 52

QM3 reçu de l'initiateur.

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitement de la charge utile de hachage

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, chargement de toutes les SA IPSEC

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Génération de la clé de mode rapide !

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, règle de cryptage NP recherche la crypto map MAP 10 correspondant à ACL VPN : retourné cs_id=53f11198 ; règle=53f11a90

[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Génération de la clé de mode rapide !

IPSEC : Nouvelle SA embryonnaire créée @ 0x53F18B00,
SCB : 0x53F8A1C0,
Direction : sortant
SPI : 0xDB680406
ID de session : 0x00004000
Numéro VPIF : 0x0000003
Type de tunnel : l2l
Protocole : esp
Durée de vie : 240 secondes

IPSEC : Mise à jour OBSA de l'hôte terminée, SPI 0xDB680406

IPSEC : Création du contexte VPN sortant, SPI 0xDB680406
Indicatifs: 0x00000005
SA : 0x53F18B00
SPI : 0xDB680406
MTU : 1500 bytes
VCID : 0x00000000
Homologue : 0x00000000
SCB : 0x005E4849
Canal: 0x4C69CB80

Traiter QM3. Les clés de chiffrement sont générées pour les SA de données. Au cours de ce processus, Les SPI sont définis pour transmettre le trafic.

IPSEC : Contexte VPN sortant terminé, SPI 0xDB680406
Handle VPN : 0x0000E9B4

IPSEC : Nouvelle règle de chiffrement sortant, SPI 0xDB680406
Adresse Src : 192.168.1.0
Masque Src : 255.255.255.0
Adresse Dst : 192.168.2.0
Masque Dst : 255.255.255.0
Ports Src
Supérieur : 0
Inférieur : 0
Op: ignorer
Ports Dst
Supérieur : 0
Inférieur : 0
Op: ignorer
Protocole : 1
Utiliser le protocole : vrai
SPI : 0x00000000
Utiliser SPI : faux

IPSEC : Règle de chiffrement sortant terminée, SPI 0xDB680406

ID de règle : 0x53F89160
IPSEC : Nouvelle règle d'autorisation sortante, SPI 0xDB680406
Adresse Src : 10.0.0.1
Masque Src : 255.255.255.255
Adresse Dst : 10.0.0.2
Masque Dst : 255.255.255.255
Ports Src
Supérieur : 0
Inférieur : 0
Op: ignorer
Ports Dst
Supérieur : 0
Inférieur : 0
Op: ignorer
Protocole : 50
Utiliser le protocole : vrai
SPI : 0xDB680406
Utiliser SPI : vrai
IPSEC : Règle d'autorisation sortante terminée, SPI 0xDB680406
ID de règle : 0x53E47E88
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, règle de cryptage NP recherche la crypto map MAP 10 correspondant à ACL VPN : retourné cs_id=53f11198 ; règle=53f11a90
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, négociation de sécurité terminée pour le groupe LAN-LAN (10.0.0.2) Répondeur, SPI entrant = 0x1698cac7, SPI sortant = 0xdb680406
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE a obtenu un message KEY_ADD pour SA : SPI = 0xdb680406
IPSEC : Mise à jour IBSA de l'hôte terminée, SPI 0x1698CAC7
IPSEC : Création du contexte VPN entrant, SPI 0x1698CAC7
Indicatifs: 0x00000006
SA : 0x53FC3698
SPI : 0x1698CAC7
MTU : 0 bytes
VCID : 0x00000000
Homologue : 0x0000E9B4
SCB : 0x005DAE51
Canal: 0x4C69CB80
IPSEC : Contexte VPN entrant terminé, SPI 0x1698CAC7
Handle VPN : 0x00011A8C
IPSEC : Mise à jour du contexte VPN sortant 0x0000E9B4, SPI 0xDB680406
Indicatifs: 0x00000005
SA : 0x53F18B00
SPI : 0xDB680406
MTU : 1500 bytes
VCID : 0x00000000
Homologue : 0x00011A8C
SCB : 0x005E4849
Canal: 0x4C69CB80
IPSEC : Contexte VPN sortant terminé, SPI 0xDB680406
Handle VPN : 0x0000E9B4
IPSEC : Règle interne sortante terminée, SPI 0xDB680406
ID de règle : 0x53F89160
IPSEC : Règle SPD externe sortante terminée, SPI 0xDB680406
ID de règle : 0x53E47E88
IPSEC : Nouvelle règle de flux de tunnel entrant, SPI 0x1698CAC7
Adresse Src : 192.168.2.0
Masque Src : 255.255.255.0
Adresse Dst : 192.168.1.0
Masque Dst : 255.255.255.0
Ports Src
Supérieur : 0
Inférieur : 0

Les SPI sont affectés aux SA de données.

Op: ignorer Ports Dst Supérieur : 0 Inférieur : 0 Op: ignorer Protocole : 1 Utiliser le protocole : vrai SPI : 0x00000000 Utiliser SPI : faux IPSEC : Règle de flux de tunnel entrant terminée, SPI 0x1698CAC7 ID de règle : 0x53FC3E80 IPSEC : Nouvelle règle de décryptage entrant, SPI 0x1698CAC7 Adresse Src : 10.0.0.2 Masque Src : 255.255.255.255 Adresse Dst : 10.0.0.1 Masque Dst : 255.255.255.255 Ports Src Supérieur : 0 Inférieur : 0 Op: ignorer Ports Dst Supérieur : 0 Inférieur : 0 Op: ignorer Protocole : 50 Utiliser le protocole : vrai SPI : 0x1698CAC7 Utiliser SPI : vrai IPSEC : Règle de déchiffrement entrant terminée, SPI 0x1698CAC7 ID de règle : 0x53FC3F18 IPSEC : Nouvelle règle d'autorisation entrante, SPI 0x1698CAC7 Adresse Src : 10.0.0.2 Masque Src : 255.255.255.255 Adresse Dst : 10.0.0.1 Masque Dst : 255.255.255.255 Ports Src Supérieur : 0 Inférieur : 0 Op: ignorer Ports Dst Supérieur : 0 Inférieur : 0 Op: ignorer Protocole : 50 Utiliser le protocole : vrai SPI : 0x1698CAC7 Utiliser SPI : vrai IPSEC : Règle d'autorisation entrante terminée, SPI 0x1698CAC7 ID de règle : 0x53F8AEA8 [DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Pitcher : reçu KEY_UPDATE, spi 0x1698cac7	
[DEBUG IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, Démarrage du minuteur de clé P2 : 3060 secondes.	Démarrer les heures de retouche IPsec.
[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, PHASE 2 TERMINÉE (msgid =52481cf5)	Phase 2 terminée. Le répondeur et l'initiateur sont capables de chiffrer/déchiffrer le trafic.

Vérification du tunnel

Note: Puisque le protocole ICMP est utilisé pour déclencher le tunnel, une seule SA IPSec est activée. Protocole 1 = ICMP.

show crypto ipsec sa

```
interface: outside
  Crypto map tag: MAP, seq num: 10, local addr: 10.0.0.1
   access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
   local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/
```

1

```
/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/
```

1

```
/0)
   current_peer: 10.0.0.2
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
   #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
   #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0
   local crypto endpt.: 10.0.0.1/0, remote crypto endpt.: 10.0.0.2/0
   path mtu 1500, ipsec overhead 74, media mtu 1500
   current outbound spi: DB680406
   current inbound spi : 1698CAC7
  inbound esp sas:
   spi: 0x
```

1698CAC7

```
 (379112135)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x0000001F
  outbound esp sas:
   spi: 0xDB680406 (3681027078)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
      0x00000000 0x00000001
```

show crypto isakmp sa

```
  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.0.0.2
   Type    :
```

L2L

```
             Role    :
```

responder

```
   Rekey   : no              State   :
```

MM_ACTIVE

Informations connexes

- Un bon point de départ : article de wikipedia sur IPSec. Standard et références contiennent beaucoup d'informations utiles
- Dépannage IPsec : Présentation et utilisation des commandes de débogage
- Support et documentation techniques - Cisco Systems