Debugs ASA IPsec et d'IKE (IKEv1 mode principal) dépannage de TechNote

Contenu

Introduction

Ce document décrit met au point sur l'appliance de sécurité adaptable (ASA) quand le mode principal et la clé pré-partagée (PSK) sont utilisés. La traduction de certaines lignes de débogage dans la configuration est également abordée.

Les thèmes non discutés dans ce document incluent passer le trafic après que le tunnel ait été établi et des concepts de base d'IPsec ou d'Échange de clés Internet (IKE).

Conditions préalables

Exigences

Les lecteurs de ce document devraient avoir la connaissance de ces thèmes.

- PSK
- IKE

Composants utilisés

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 le Cisco IOS® $^{12.4T}$

Principale question

L'IKE et l'IPsec met au point sont parfois cryptiques, mais vous pouvez les employer pour comprendre où un problème d'établissement de tunnel VPN d'IPsec se trouve.

Scénario

Le mode principal est typiquement utilisé entre les tunnels entre réseaux locaux ou, dans le cas de l'Accès à distance (EzVPN), quand des Certificats sont utilisés pour l'authentification.

Met au point sont de deux ASA qui exécutent la version de logiciel 9.3.2. Les deux périphériques formeront un tunnel entre réseaux locaux.

Deux scénarios principaux sont décrits :

- ASA comme demandeur pour l'IKE
- ASA en tant que responder pour l'IKE

Commandes de debug utilisées

debug crypto ikev1 127

debug crypto ipsec 127

Configuration ASA

Configuration d'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 de message de demandeur	Débogages	Description de message de responder
L'échange principal de mode commence ; aucune stratégie n'a été partagée, et les pairs sont toujours dans MM_NO_STATE. Comme demandeur, les débuts ASA pour construire la charge utile.	DEBUG [IKEv1] : Broc : a reçu une clé saisissent le message, le spi 0x0 IPSEC(crypto_map_check)-3 : Recherche du crypto map appariant 5-tuple : Prot=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3 : Vérifier la MAP 10 de crypto map : apparié. [[IKEv1] : IP = 10.0.0.2, demandeur d'IKE : Nouveau Phase 1, Intf à l'intérieur, adresse locale 192.168.1.0 de proxy de 10.0.0.2 de pair d'IKE, adresse distante 192.168.2.0 de proxy, crypto map (MAP)	
Élaboration MM1 Ce processus inclut la proposition initiale pour l'IKE et les constructeurs pris en charge NAT-T.	DEBUG [IKEv1] : IP = 10.0.0.2, construisant le DEBUG de la **charge utile** [IKEv1 de **SA ISAKMP**] : IP = 10.0.0.2, construisant la charge utile du ver 02 du NAT-Traversal VID DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile du ver 03 du NAT-Traversal VID DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile RFC de ver du NAT-Traversal VID DEBUG [IKEv1] : L'IP = le 10.0.0.2, construisant la fragmentation VID + ont étendu la charge utile de capacités	
Envoyez MM1.	[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=0) avec des charges utiles : HDR + SA (1) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + AUCUN (0) longueurs totales : 168 ==========MM1========== ====>	
	[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=0) avec des charges utiles : HDR + SA (1) + CONSTRUCTEUR (13) +VENDOR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + AUCUN (0) longueurs totales : 164	MM1 reçu du demandeur.
	DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile SA	Processus MM1.
	DEBUG [IKEv1] : L'IP = le 10.0.0.2, proposition d'Oakley est acceptable	La comparaison des
	DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID	stratégies
	DEBUG [IKEv1] : IP = 10.0.0.2, RFC reçu VID de NAT-Traversal	ISAKMP/IKE
	DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID	commence.
	DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID	Le pair distant
	DEBUG [IKEv1] : IP = 10.0.0.2, ver reçu 03 VID de NAT-Traversal	annonce qu'il peut
	DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID	utiliser NAT-T.
	DEBUG [IKEv1] : IP = 10.0.0.2, ver reçu 02 VID de NAT-Traversal	Configuration relative
	DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile d'IKE SA	:

crypto isakmp policy 10
authentication pre-share
cryptage 3des
SHA d'informations parasites
groupe 2
vie 86400

DEBUG [IKEv1] : L'IP = le 10.0.0.2, proposition d'IKE SA # 1, transforment # 1 entrée globale d'IKE de correspondances acceptables # 2

Élaboration MM2. Dans ce message le responder sélectionne qui des paramètres de la stratégie d'ISAKMP aux utiliser. Il annonce également les versions NAT-T qu'il peut l'utiliser.

DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile de SA ISAKMP
DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile du ver 02 du NAT-Traversal VID
DEBUG [IKEv1] : L'IP = le 10.0.0.2, construisant la fragmentation VID + ont étendu la charge utile de capacités

[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=0) avec des charges utiles : HDR + SA (1) + CONSTRUCTEUR (13) + longueur totale du CONSTRUCTEUR (13) + NONE(0) : 128

Envoyez MM2.

<==========MM2==========

MM2 reçu du responder.

[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=0) avec des charges utiles : HDR + SA (1) + CONSTRUCTEUR (13) + AUCUN (0) longueurs totales : 104

Processus MM2.

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile SA
DEBUG [IKEv1] : L'IP = le 10.0.0.2, proposition d'Oakley est acceptable
DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID
DEBUG [IKEv1] : IP = 10.0.0.2, RFC reçu VID de NAT-Traversal
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, construisant la charge utile du KE
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, construisant la charge utile de nonce
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, construisant la charge utile du Cisco Unity VID
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, construisant la charge utile du Xauth V6 VID

Élaboration MM3. Charges utiles de cette de processus détection d'includesNAT, charges utiles du Key Exchange de Protocole DH (Diffie-Hellman) (KE) (l'initator inclut g, p, et A au responder), et support DPD.

30 novembre DEBUG [IKEv1 de 10:38:29] : L'IP = le 10.0.0.2, envoient IOS VID
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, construisant l'ASA charriant la charge utile d'ID de constructeur IOS (version : 1.0.0, capacités : 20000001)
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, construisant la charge utile VID
30 novembre DEBUG [IKEv1 de 10:38:29] : L'IP = le 10.0.0.2, envoient Altiga/Cisco VPN3000/Cisco ASA le gw VID
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, construisant la charge utile de Nat-détection
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, calculant les informations parasites NAT de détection
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, construisant la charge utile de Nat-détection
30 novembre DEBUG [IKEv1 de 10:38:29] : IP = 10.0.0.2, calculant les informations parasites NAT de détection

Envoyez MM3.

[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=0) avec des charges utiles : HDR + le KE (4) + NONCE (10) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + NAT-D (20) + NAT-D (20) + AUCUN (0) longueurs totales : 304

==========MM3==========>

MM3 reçu du demandeur.

[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=0) avec des charges utiles : HDR + le KE (4) + NONCE (10) +

CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + NAT-D (130) + NAT-D (130) + AUCUN (0) longueurs totales : 284

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile du KE

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile ISA_KE

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

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID

DEBUG [IKEv1] : IP = 10.0.0.2, DPD reçu VID

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile d'ID de constructeur IOS/PIX (version : 1.0.0, capacités : 00000f6f)

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID

DEBUG [IKEv1] : IP = 10.0.0.2, Xauth reçu V6 VID

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile de Nat-détection

DEBUG [IKEv1] : IP = 10.0.0.2, calculant les informations parasites NAT de détection

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile de Nat-détection

DEBUG [IKEv1] : IP = 10.0.0.2, calculant les informations parasites NAT de détection

DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile du KE

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

DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile du Cisco Unity VID

DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile du Xauth V6 VID

DEBUG [IKEv1] : L'IP = le 10.0.0.2, envoient IOS VID

DEBUG [IKEv1] : IP = 10.0.0.2, construisant l'ASA charriant la charge utile d'ID de constructeur IOS (version : 1.0.0, capacités : 20000001)

DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile VID

DEBUG [IKEv1] : L'IP = le 10.0.0.2, envoient Altiga/Cisco VPN3000/Cisco ASA le gw VID

DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile de Nat-détection

DEBUG [IKEv1] : IP = 10.0.0.2, calculant les informations parasites NAT de détection

DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile de Nat-détection

DEBUG [IKEv1] : IP = 10.0.0.2, calculant les informations parasites NAT de détection

[[IKEv1] : L'IP = le 10.0.0.2, connexion ont débarqué sur le tunnel_group 10.0.0.2

DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, générant des clés pour le responder…

[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=0) avec des charges utiles : HDR + le KE (4) + NONCE (10) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + NAT-D (130) + NAT-D (130) + AUCUN (0) longueurs totales : 304

<==========MM4==========

Processus MM3. Des charges utiles NAT-D le responder peut déterminer si l'initator est derrière NAT et si le responder est derrière NAT. Du CAD KE, le responder de charge utile obtient des valeurs de p, de g et de R.

Élaboration MM4. Ce processus inclut la charge utile NAT de détection, le responder CAD KE génère « B » et « s » (renvoie « B » à l'initator), et DPD VID.

Le pair est associé avec le groupe de tunnel de 10.0.0.2 L2L, et le cryptage et les clés d'informations parasites sont générés du « s » ci-dessus et du pre-shared-key.

Envoyez MM4.

MM4 reçu du responder.

[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=0) avec des charges utiles : HDR + le KE (4) + NONCE (10) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + NAT-D (20) + NAT-D (20) + AUCUN (0) longueurs totales : 304

Processus MM4. Des charges utiles NAT-D, l'initator peut maintenant déterminer si l'iniator est derrière NAT et si le responder

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile d'IKE

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile ISA_KE

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

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID

DEBUG [IKEv1] : IP = 10.0.0.2, client reçu VID de Cisco Unity

DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID

est derrière NAT. Du CAD KE, le demandeur reçoit « B » et peut maintenant générer le « S. »	DEBUG [IKEv1] : IP = 10.0.0.2, DPD reçu VID DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile d'ID de constructeur IOS/PIX (version : 1.0.0, capacités : 00000f7f) DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile VID DEBUG [IKEv1] : IP = 10.0.0.2, Xauth reçu V6 VID DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile de Nat-détection DEBUG [IKEv1] : IP = 10.0.0.2, calculant les informations parasites NAT de détection DEBUG [IKEv1] : IP = 10.0.0.2, traitant la charge utile de Nat-détection DEBUG [IKEv1] : IP = 10.0.0.2, calculant les informations parasites NAT de détection		
Le pair est associé avec le groupe de tunnel de 10.0.0.2 L2L, et l'initator génère des clés de cryptage et d'informations parasites utilisant « s » en haut et le pre-shared-key.	[[IKEv1] : L'IP = le 10.0.0.2, connexion ont débarqué sur le tunnel_group 10.0.0.2 DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, générant des clés pour le demandeur…		
Élaboration MM5. Configuration relative : automatique de crypto isakmp identity	DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile d'ID DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile d'informations parasites DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, calculant des informations parasites pour l'ISAKMP DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile de keepalive IOS : sec proposal=32767/32767. DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile de vid de dpd		
Envoyez MM5.	[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=0) avec des charges utiles : HDR + ID (5) + INFORMATIONS PARASITES (8) + KEEPALIVE IOS (128) +VENDOR (13) + AUCUN (0) longueurs totales : 96 ==========MM5==========>		
Le responder n'est pas derrière NAT. Aucun NAT-T requis.	[[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, état NAT automatique de détection : L'extrémité distante n'est pas derrière un périphérique NAT que cette extrémité n'est pas derrière un périphérique NAT	[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=0) avec des charges utiles : HDR + ID (5) + INFORMATIONS PARASITES (8) + AUCUN (0) longueurs totales : 64	MM5 reçu du demandeur. Ce processus inclut l'identité distante de pair (ID) et le renvoi de connexion sur un groupe particulier de tunnel.
		DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile d'IDENTIFICATEUR DE PROCESSUS [IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID ID_IPV4_ADDR reçu 10.0.0.2 DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile d'informations parasites DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, calculant des informations parasites pour l'ISAKMP DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, traitant informent la charge utile [[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2,Automatic NAT [[IKEv1] : L'IP = le 10.0.0.2, connexion ont débarqué sur le tunnel_group	Processus MM5. L'authentification avec des clés pré-partagées commence maintenant. L'authentification se produit sur les deux pairs ; donc, vous verrez deux ensembles de procédures d'authentification correspondantes. Configuration relative

		10.0.0.2	: type ipsec-l2l de 10.0.0.2 de groupe de tunnel
		État de détection : L'extrémité distante n'est pas derrière un périphérique NAT que cette extrémité n'est pas derrière un périphérique NAT	Aucun NAT-T requis dans ce cas.
		DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile d'ID DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile d'informations parasites DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, calculant des informations parasites pour l'ISAKMP DEBUG [IKEv1] : IP = 10.0.0.2, construisant la charge utile de keepalive IOS : sec proposal=32767/32767. DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile de vid de dpd	Élaboration MM6. Envoyez l'identité inclut des temps de rekey commencés et l'identité envoyée au pair distant.
		[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=0) avec des charges utiles : HDR + ID (5) + INFORMATIONS PARASITES (8) + KEEPALIVE IOS (128) +VENDOR (13) + AUCUN (0) longueurs totales : 96 <==========MM6==========>	Envoyez MM6.
			Phase 1 complet. Temporisateur de rekey d'ISAKMP de début. Configuration relative : crypto isakmp policy 10 authentication pre-share cryptage 3des SHA d'informations parasites groupe 2 vie 86400 le ciscoasa # SH exécutent tout le crypto isakmp automatique de crypto isakmp identity
		[[IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, PHASE 1 SE SONT TERMINÉS [[IKEv1] : IP = 10.0.0.2, type de keep-alive pour cette connexion : DPD DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, démarrant le temporisateur du rekey P1 : 64800 secondes.	
MM6 reçu du responder.	[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=0) avec des charges utiles : HDR + ID (5) + INFORMATIONS PARASITES (8) + AUCUN (0) longueurs totales : 64		
Processus MM6. Ce processus inclut l'identité distante envoyée du pair et de la décision finale concernant le groupe de tunnel de sélectionner.	DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile d'IDENTIFICATEUR DE PROCESSUS [IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID ID_IPV4_ADDR reçu 10.0.0.2 DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile d'informations parasites DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, calculant des informations parasites pour l'ISAKMP [[IKEv1] : L'IP = le 10.0.0.2, connexion ont débarqué sur le tunnel_group 10.0.0.2 DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, Oakley commencent le mode rapide [IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, demandeur d'IKE commençant QM : id de msg = 7b80c2b0		
Phase 1 complet. Temporisateur de rekey d'ISAKMP de début. Configuration relative : type ipsec-l2l de	[[IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, PHASE 1 SE SONT TERMINÉS [[IKEv1] : IP = 10.0.0.2, type de keep-alive pour cette connexion : DPD DPD a l'abeille négociée et le Phase 1 est maintenant complet. DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, démarrant le temporisateur du rekey P1 : 82080 secondes.		

10.0.0.2 de groupe de tunnel
ipsec-attributs de 10.0.0.2 de groupe de tunnel
pre-shared-key Cisco

Le Phase 2 (mode rapide) commence.

IPSEC : Nouveaux @ 0x53FC3C00 créés par SA embryonnaires,
SCB : 0x53F90A00,
Direction : d'arrivée
SPI : 0xFD2D851F
ID de session : 0x00006000
VPIF numérique : 0x00000003
Type de tunnel : l2l
Protocol : l'ESP
Vie : 240 secondes

DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, IKE ont obtenu le SPI de l'engine principale : SPI = 0xfd2d851f

Élaboration QM1. Ce processus inclut des stratégies d'id et d'IPsec de proxy.
Configuration relative :
le crypto ipsec transform-set TRANSFORMENT l'ESP-SHA-hmac du l'ESP-aes
la liste d'accès VPN a étendu l'ICMP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 d'autorisation

DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, oakley constucting le mode rapide
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile vide d'informations parasites
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile d'IPSec SA
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile de nonce d'IPSec
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant l'ID de proxy
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, id de transmission de proxy :
Sous-réseau local : masque 255.255.255.0 Protocol de 192.168.1.0 1 port 0
Sous-réseau distant : Masque 255.255.255.0 Protocol de 192.168.2.0 1 port 0
Le sous-réseau local (192.168.1.0/24) et le sous-réseau distant expcted (192.168.2.0/24) sont envoyés
[IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, demandeur d'IKE envoyant le contact initial
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile d'informations parasites de qm
[IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, demandeur d'IKE envoyant le 1er paquet QM : id de msg = 7b80c2b0

Envoyez QM1.

[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=7b80c2b0) avec des charges utiles : HDR + les INFORMATIONS PARASITES (8) + SA (1) + le NONCE (10) + l'ID (5) + l'ID (5) + ANNONCENT (11) + AUCUN (0) longueurs totales : 200
==========QM1==========>

QM1 reçu du demandeur. Le responder commence la phase 2 (QM).

[IKEv1 DÉCODENT] : IP = 10.0.0.2, responder d'IKE commençant QM : id de msg = 52481cf5
[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=52481cf5) avec des charges utiles : HDR + INFORMATIONS PARASITES (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + AUCUN (0) longueurs totales : 172

Processus QM1. Ce processus compare des proxys distants aux gens du pays et sélectionne la stratégie acceptable d'IPsec. Configuration relative : le crypto ipsec transform-set TRANSFORMENT l'ESP-SHA-hmac du

DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile d'informations parasites
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile SA
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile de nonce
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile d'IDENTIFICATEUR DE PROCESSUS

	l'ESP-aes la liste d'accès VPN a étendu l'ICMP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 d'autorisation adresse VPN de correspondance de la MAP 10 de crypto map
[IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID received--192.168.2.0--255.255.255.0[IKEv1] ID_IPV4_ADDR_SUBNET : Le groupe = le 10.0.0.2, IP = 10.0.0.2, ont reçu des données distantes de sous-réseau de proxy IP en charge utile d'ID : Adressez 192.168.2.0, masque 255.255.255.0, Protocol 1, le port 0 DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile d'IDENTIFICATEUR DE PROCESSUS [IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID received--192.168.1.0--255.255.255.0 ID_IPV4_ADDR_SUBNET [[IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, ont reçu des données locales de sous-réseau de proxy IP en charge utile d'ID : Adressez 192.168.1.0, masque 255.255.255.0, Protocol 1, le 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, vieille SA QM IsRekeyed non trouvée par adr [[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, contrôle statique de crypto map, vérifiant la carte = la MAP, = 10 seq… [[IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, contrôle statique de crypto map, MAP de carte, = 10 seq est une concordance réussie [[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, pair distant d'IKE configuré pour le crypto map : MAP	Une crypto entrée statique assortie est recherchée et trouvée.
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile d'IPSec SA DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, proposition d'IPSec SA # 1, transforment # 1 entrée globale d'IPSec SA de correspondances acceptables # 10 [[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, IKE : demande du SPI ! IPSEC : Nouveaux @ 0x53FC3698 créés par SA embryonnaires, SCB : 0x53FC2998, Direction : d'arrivée SPI : 0x1698CAC7 ID de session : 0x00004000 VPIF numérique : 0x00000003 Type de tunnel : l2l Protocol : l'ESP Vie : 240 secondes DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, IKE ont obtenu le SPI de l'engine principale : 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, construisant la charge utile vide d'informations parasites DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile d'IPSec SA DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile de nonce d'IPSec DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant l'ID de proxy DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, id de transmission de proxy : Sous-réseau distant : Masque 255.255.255.0 Protocol de 192.168.2.0 1 port 0	Élaboration QM2. Ce processus inclut la confirmation des identités de proxy, type de tunnel, et un contrôle est exécuté pour crypto ACLs reflété.

Sous-réseau local : masque 255.255.255.0 Protocol de 192.168.1.0 1 port 0
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, construisant la charge utile d'informations parasites de qm
[IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, responder d'IKE envoyant le 2ème paquet QM : id de msg = 52481cf5
[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=52481cf5) avec des charges utiles : HDR + INFORMATIONS PARASITES (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + AUCUN (0) longueurs totales : 172

Envoyez QM2.

<==========QM2==========

QM2 reçu du responder.

[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=7b80c2b0) avec des charges utiles : HDR + les INFORMATIONS PARASITES (8) + SA (1) + le NONCE (10) + l'ID (5) + l'ID (5) + ANNONCENT (11) + AUCUN (0) longueurs totales : 200

Processus QM2. Dans ce processus, l'extrémité distante envoie des paramètres et les vies de la phase proposées les plus courtes 2 est sélectionnées.

DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile d'informations parasites
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile SA
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile de nonce
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile d'IDENTIFICATEUR DE PROCESSUS
[IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID received--192.168.1.0--255.255.255.0 ID_IPV4_ADDR_SUBNET
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, charge utile d'IDENTIFICATEUR DE PROCESSUS
[IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, ID received--192.168.2.0--255.255.255.0 ID_IPV4_ADDR_SUBNET
DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, traitant informent la charge utile
[IKEv1 DÉCODENT] : Le responder que la vie décodent suit (outb SPI[4]|attributes) :
[IKEv1 DÉCODENT] : 0000 : DDE50931 80010001 00020004 00000E10… 1 .....
[[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, responder forçant la modification d'IPSec réintroduisant la durée de 28800 à 3600 secondes basé sur la réponse du pair, l'ASA change certains attributs IPSEC. Dans ce cas l'intervalle de rekey
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, chargeant tout l'IPSEC SAS
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, générant la clé rapide de mode !

Crypto map assorti trouvé « MAP » et entrée 10 et apparié lui contre la liste d'accès « VPN. »

DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, le NP chiffrent la consultation de règle pour l'ACL assorti VPN de la MAP 10 de crypto map : cs_id=53f11198 retourné ; rule=53f11a90

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

L'appliance a généré le trafic en entrée et en sortie 0xfd2d851f et 0xdde50931for SPI respectivement.

IPSEC : Nouveaux @ 0x53FC3698 créés par SA embryonnaires,
SCB : 0x53F910F0,
Direction : sortant
SPI : 0xDDE50931
ID de session : 0x00006000
VPIF numérique : 0x00000003
Type de tunnel : l2l
Protocol : l'ESP
Vie : 240 secondes
IPSEC : Mise à jour terminée de l'hôte OBSA, SPI 0xDDE50931
IPSEC : Création du contexte sortant VPN, SPI 0xDDE50931
Indicateurs : 0x00000005
SA : 0x53FC3698
SPI : 0xDDE50931

MTU : 1500 bytes
VCID : 0x00000000
Pair : 0x00000000
SCB : 0x01CF218F
La Manche : 0x4C69CB80
IPSEC : Contexte sortant terminé VPN, SPI 0xDDE50931
Traitement VPN : 0x000161A4
IPSEC : Nouveau sortant chiffrent la règle, SPI 0xDDE50931
Adr de Src : 192.168.1.0
Masque de Src : 255.255.255.0
Adr de Dst : 192.168.2.0
Masque de Dst : 255.255.255.0
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 1
Protocole d'utilisation : vrai
SPI : 0x00000000
Utilisation SPI : faux
IPSEC : Sortant terminé chiffrent la règle, SPI 0xDDE50931
ID de règle : 0x53FC3AD8
IPSEC : Nouvelle règle sortante d'autorisation, SPI 0xDDE50931
Adr de Src : **10.0.0.1**
Masque de Src : 255.255.255.255
Adr de Dst : 10.0.0.2
Masque de Dst : 255.255.255.255
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 50
Protocole d'utilisation : vrai
SPI : 0xDDE50931
Utilisation SPI : vrai
IPSEC : Règle sortante terminée d'autorisation, SPI 0xDDE50931
ID de règle : 0x53F91538
DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, le NP chiffrent la consultation de règle pour l'ACL assorti VPN de la MAP 10 de crypto map : cs_id=53f11198 retourné ; rule=53f11a90
[[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, négociation de sécurité complète pour le demandeur de groupe d'entre réseaux locaux (10.0.0.2), SPI en entrée = 0xfd2d851f, sortant SPI = 0xdde50931
IPSEC : Mise à jour terminée de l'hôte IBSA, SPI 0xFD2D851F
IPSEC : Création du contexte d'arrivée VPN, SPI 0xFD2D851F
Indicateurs : 0x00000006
SA : 0x53FC3C00
SPI : 0xFD2D851F
MTU : octets 0
VCID : 0x00000000
Pair : 0x000161A4
SCB : 0x01CEA8EF
La Manche : 0x4C69CB80
IPSEC : Contexte d'arrivée terminé VPN, SPI 0xFD2D851F
Traitement VPN : 0x00018BBC
IPSEC : Mise à jour du contexte sortant 0x000161A4 VPN, SPI

Élaboration QM3. Confirmez tous les SPI créés au pair distant.

0xDDE50931
Indicateurs : 0x00000005
SA : 0x53FC3698
SPI : 0xDDE50931
MTU : 1500 bytes
VCID : 0x00000000
Pair : 0x00018BBC
SCB : 0x01CF218F
La Manche : 0x4C69CB80
IPSEC : Contexte sortant terminé VPN, SPI 0xDDE50931
Traitement VPN : 0x000161A4
IPSEC : Règle intérieure sortante terminée, SPI 0xDDE50931
ID de règle : 0x53FC3AD8
IPSEC : Règle externe sortante terminée SPD, SPI 0xDDE50931
ID de règle : 0x53F91538
IPSEC : Nouvelle règle d'arrivée d'écoulement de tunnel, SPI 0xFD2D851F
Adr de Src : 192.168.2.0
Masque de Src : 255.255.255.0
Adr de Dst : 192.168.1.0
Masque de Dst : 255.255.255.0
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 1
Protocole d'utilisation : vrai
SPI : 0x00000000
Utilisation SPI : faux
IPSEC : Règle d'arrivée terminée d'écoulement de tunnel, SPI 0xFD2D851F
ID de règle : 0x53F91970
IPSEC : Nouvelle règle d'arrivée de déchiffrage, SPI 0xFD2D851F
Adr de Src : 10.0.0.2
Masque de Src : 255.255.255.255
Adr de Dst : **10.0.0.1**
Masque de Dst : 255.255.255.255
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 50
Protocole d'utilisation : vrai
SPI : 0xFD2D851F
Utilisation SPI : vrai
IPSEC : Règle d'arrivée terminée de déchiffrage, SPI 0xFD2D851F
ID de règle : 0x53F91A08
IPSEC : Nouvelle règle d'arrivée d'autorisation, SPI 0xFD2D851F
Adr de Src : 10.0.0.2
Masque de Src : 255.255.255.255
Adr de Dst : **10.0.0.1**
Masque de Dst : 255.255.255.255
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0

Inférieur : 0
Op : ignorez
Protocol : 50
Protocole d'utilisation : vrai
SPI : 0xFD2D851F
Utilisation SPI : vrai
IPSEC : Règle d'arrivée terminée d'autorisation, SPI 0xFD2D851F
ID de règle : 0x53F91AA0

Envoyez QM3.

[IKEv1 DÉCODENT] : Groupe = 10.0.0.2, IP = 10.0.0.2, demandeur d'IKE envoyant le 3ème paquet QM : id de msg = 7b80c2b0

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

[[IKEv1] : IP = 10.0.0.2, IKE_DECODE envoyant message (msgid=7b80c2b0) avec des charges utiles : HDR + INFORMATIONS PARASITES (8) + AUCUN (0) longueurs totales : 76

[[IKEv1] : L'IP = le 10.0.0.2, IKE_DECODE ONT REÇU le message (msgid=52481cf5) avec des charges utiles : HDR + INFORMATIONS PARASITES (8) + AUCUN (0) longueurs totales : 52

Demandeur de fom du receivd QM3.

Phase 2 complet. Le demandeur est maintenant prêt à chiffrer et déchiffrer des paquets utilisant ces valeurs SPI.

DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, IKE ont obtenu un msg KEY_ADD pour SA : SPI = 0xdde50931

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

DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, démarrant le temporisateur du rekey P2 : 3060 secondes.

[[IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, PHASE 2 SE SONT TERMINÉS (msgid=7b80c2b0)

DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, traitant la charge utile d'informations parasites

DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, chargeant tout l'IPSEC SAS

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

DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, le NP chiffrent la consultation de règle pour l'ACL assorti VPN de la MAP 10 de crypto map : cs_id=53f11198 retourné ; rule=53f11a90

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

IPSEC : Nouveaux @ 0x53F18B00 créés par SA embryonnaires, SCB : 0x53F8A1C0,
Direction : sortant
SPI : 0xDB680406
ID de session : 0x00004000
VPIF numérique : 0x00000003
Type de tunnel : l2l
Protocol : l'ESP
Vie : 240 secondes

Processus QM3. Des clés de chiffrement sont générées pour les données SAS. Pendant ce processus, Des SPI sont placés afin de passer le trafic.

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

IPSEC : Création du contexte sortant VPN, SPI 0xDB680406
Indicateurs : 0x00000005
SA : 0x53F18B00
SPI : 0xDB680406
MTU : 1500 bytes
VCID : 0x00000000
Pair : 0x00000000
SCB : 0x005E4849
La Manche : 0x4C69CB80

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

IPSEC : Nouveau sortant chiffrent la règle, SPI 0xDB680406
Adr de Src : 192.168.1.0
Masque de Src : 255.255.255.0
Adr de Dst : 192.168.2.0
Masque de Dst : 255.255.255.0
Ports de Src
Stimulant : 0

Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 1
Protocole d'utilisation : vrai
SPI : 0x00000000
Utilisation SPI : faux
IPSEC : Sortant terminé chiffrent la règle, SPI 0xDB680406
ID de règle : 0x53F89160
IPSEC : Nouvelle règle sortante d'autorisation, SPI 0xDB680406
Adr de Src : **10.0.0.1**
Masque de Src : 255.255.255.255
Adr de Dst : 10.0.0.2
Masque de Dst : 255.255.255.255
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 50
Protocole d'utilisation : vrai
SPI : 0xDB680406
Utilisation SPI : vrai
IPSEC : Règle sortante terminée d'autorisation, SPI 0xDB680406
ID de règle : 0x53E47E88
DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, le NP chiffrent la consultation de règle pour l'ACL assorti VPN de la MAP 10 de crypto map : cs_id=53f11198 retourné ; rule=53f11a90
[[IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, négociation de sécurité complète pour le responder de groupe d'entre réseaux locaux (10.0.0.2), SPI en entrée = 0x1698cac7, sortant SPI = 0xdb680406
DEBUG [IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, IKE ont obtenu un msg KEY_ADD pour SA : SPI = 0xdb680406
IPSEC : Mise à jour terminée de l'hôte IBSA, SPI 0x1698CAC7
IPSEC : Création du contexte d'arrivée VPN, SPI 0x1698CAC7
Indicateurs : 0x00000006
SA : 0x53FC3698
SPI : 0x1698CAC7
MTU : octets 0
VCID : 0x00000000
Pair : 0x0000E9B4
SCB : 0x005DAE51
La Manche : 0x4C69CB80
IPSEC : Contexte d'arrivée terminé VPN, SPI 0x1698CAC7
Traitement VPN : 0x00011A8C
IPSEC : Mise à jour du contexte sortant 0x0000E9B4 VPN, SPI 0xDB680406
Indicateurs : 0x00000005
SA : 0x53F18B00
SPI : 0xDB680406
MTU : 1500 bytes
VCID : 0x00000000
Pair : 0x00011A8C
SCB : 0x005E4849
La Manche : 0x4C69CB80
IPSEC : Contexte sortant terminé VPN, SPI 0xDB680406
Traitement VPN : 0x0000E9B4
IPSEC : Règle intérieure sortante terminée, SPI 0xDB680406

Des SPI sont assignés aux données SAS.

ID de règle : 0x53F89160
IPSEC : Règle externe sortante terminée SPD, SPI 0xDB680406
ID de règle : 0x53E47E88
IPSEC : Nouvelle règle d'arrivée d'écoulement de tunnel, SPI 0x1698CAC7
Adr de Src : 192.168.2.0
Masque de Src : 255.255.255.0
Adr de Dst : 192.168.1.0
Masque de Dst : 255.255.255.0
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 1
Protocole d'utilisation : vrai
SPI : 0x00000000
Utilisation SPI : faux
IPSEC : Règle d'arrivée terminée d'écoulement de tunnel, SPI 0x1698CAC7
ID de règle : 0x53FC3E80
IPSEC : Nouvelle règle d'arrivée de déchiffrage, SPI 0x1698CAC7
Adr de Src : 10.0.0.2
Masque de Src : 255.255.255.255
Adr de Dst : **10.0.0.1**
Masque de Dst : 255.255.255.255
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 50
Protocole d'utilisation : vrai
SPI : 0x1698CAC7
Utilisation SPI : vrai
IPSEC : Règle d'arrivée terminée de déchiffrage, SPI 0x1698CAC7
ID de règle : 0x53FC3F18
IPSEC : Nouvelle règle d'arrivée d'autorisation, SPI 0x1698CAC7
Adr de Src : 10.0.0.2
Masque de Src : 255.255.255.255
Adr de Dst : **10.0.0.1**
Masque de Dst : 255.255.255.255
Ports de Src
Stimulant : 0
Inférieur : 0
Op : ignorez
Ports de Dst
Stimulant : 0
Inférieur : 0
Op : ignorez
Protocol : 50
Protocole d'utilisation : vrai
SPI : 0x1698CAC7
Utilisation SPI : vrai
IPSEC : Règle d'arrivée terminée d'autorisation, SPI 0x1698CAC7
ID de règle : 0x53F8AEA8
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, broc : KEY_UPDATE reçu, spi 0x1698cac7
DEBUG [IKEv1] : Groupe = 10.0.0.2, IP = 10.0.0.2, démarrant le temporisateur du rekey P2 : 3060 secondes.

Temps de rekey d'IPsec de début.

[[IKEv1] : Le groupe = le 10.0.0.2, IP = 10.0.0.2, PHASE 2 SE SONT TERMINÉS (msgid=52481cf5)

Phase 2 complet. Le responder et le demandeur sont le trafic capable de to encrypt/decrypt.

Vérification de tunnel

Note: Puisque l'ICMP est utilisé pour déclencher le tunnel, seulement un IPSec SA est. Protocol 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 emplacement adapté à commencer est article de wikipedia sur IPSec. La norme et les références contient beaucoup d'informations utiles
- Dépannage IPsec : Présentation et utilisation des commandes de débogage
- Support et documentation techniques - Cisco Systems