ASA IPsec- en IKE-debugs (IKEv1 hoofdmodus) voor probleemoplossing bij technische opmerking

Inhoud

Inleiding

In dit document worden de tekortkomingen van de adaptieve security applicatie (ASA) beschreven, wanneer zowel de hoofdmodus als de vooraf gedeelde sleutel (PSK) wordt gebruikt. De vertaling van bepaalde debug-lijnen in de configuratie wordt ook besproken.

De onderwerpen die niet in dit document worden besproken omvatten het doorgeven van verkeer nadat de tunnel is opgericht en basisconcepten van IPsec of Internet Key Exchange (IKE).

Voorwaarden

Vereisten

Lezers van dit document zouden kennis van deze onderwerpen moeten hebben.

- PSK
- IKE

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- Cisco ASA 9.3.2
- Routers die Cisco IOS® 12.4T uitvoeren

kernvraagstuk

IKE en IPsec debugs zijn soms cryptisch, maar u kunt ze gebruiken om te begrijpen waar een probleem van de IPsec VPN-tunnelvestiging zich bevindt.

Scenario

De hoofdmodus wordt doorgaans gebruikt tussen LAN-to-LAN tunnels of, in het geval van externe toegang (EzVPN) wanneer certificaten worden gebruikt voor verificatie.

Deze apparaten komen van twee ASA's die softwareversie 9.3.2 uitvoeren. De twee apparaten zullen een LAN-to-LAN tunnel vormen.

Er worden twee hoofdscenario's beschreven:

- ASA als initiator voor IKE
- ASA als responder voor IKE

Gebruikte debug-opdrachten

debug van crypto ikev1 127

debug van crypto ipsec 127

ASA-configuratie

IPsec-configuratie:

```
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
```

IP-configuratie:

```
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
```

NAT-configuratie:

```
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
```

Ontbreken

Beschrijving van initiator-bericht	Debugs	Beschrijving van bericht weergeven
De omwisseling van de hoofdmodus begint; Er is geen beleid gedeeld en de peers zijn nog steeds in MM_NO_STATE. Als initiator begint de ASA de lading te construeren.	[IKEv1 DEBUG]: Steek: kreeg een sleutel, spi 0x0 IPSEC (crypto_map_check)-3: Op zoek naar crypto-kaart die overeenkomt met 5-tuple: Prot=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC (crypto_map_check)-3: Crypto-kaart MAP 10 controleren: gelijk. [IKEv1]: IP = 10.0.0.2, IKE-initiator: Nieuwe fase 1, Intf binnenin, IKE peer 10.0.2 lokale proxy-Address 192.168.1.0, Remote Proxy Address 192.168.2.0, Crypto Map (MAP)	
Fabric M1 Dit proces isOmvat iOorspronkelijk voorstel voor IKE en sOndersteunde NAT-T verkopers.	[IKEv1 DEBUG]: IP = 10.0.0.2, **waarbij ISAKMP SA-lading wordt** geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij NAT-traversal VID wordt geconstrueerd voor een lading van meer dan 200 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij NAT-traversal VID wordt geconstrueerd voor een nuttige lading van meer dan 03 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij NAT-traversal VID via RFC-lading wordt geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de fragmentatie VID + uitgebreide mogelijkheden worden geconstrueerd	
Stuur MM1.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) met payload: HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) totale lengte : 168	
	= ========== ========== ========== ========== ==========	
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=0) met payload: HDR + SA (1) + VENDOR (13) +VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) totale lengte : 164	MM1 ontvangen van de initiatiefnemer.
	[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van SA-lading	Verwerking M1.
	[IKEv1 DEBUG]: IP = 10.0.0.2, het voorstel van Oakley is aanvaardbaar	De vergelijking van
	[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading	het ISAKMP/IKE-
	[IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen NAT-traversal RFC VID	beleid begint.
	[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading	De externe peer
	[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading	advertenties die het
	[IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen NAT-traversal ver 03 VID	NAT-T kan gebruiken.
	[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading	Gerelateerde
	[IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen NAT-traversal ver 02 VID	configuratie:
	[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van IKE SA-lading	*crypto isakmp - beleid*
	[IKEv1 DEBUG]: IP = 10.0.0.2, IKE SA-voorstel # 1, Transformeer # 1	*10*

acceptabele matches wereldwijde IKE-vermelding # 2

controle vooraf
encryptie 3DES
hash sha
groep 2
levensduur: 8640

[IKEv1 DEBUG]: IP = 10.0.0.2, waarbij ISAKMP SA-lading wordt geconstrueerd
[IKEv1 DEBUG]: IP = 10.0.0.2, waarbij NAT-traversal VID wordt geconstrueerd voor een lading van meer dan 200
[IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de fragmentatie VID + uitgebreide mogelijkheden worden geconstrueerd

bouwen M2.
In dit bericht selecteert de responder welke beleidsinstellingen u wilt gebruiken. Ook worden de NAT-versies die het kan gebruiken geadverteerd.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) met payload: HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE(0) totale lengte : 128

Stuur MM2.

<================================"======"==========="===
==================="="="="="="<="="="="="="="="="="="="
="="<="
="="="<="<="=
"="="="="

MM2 ontvangen van de responder.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=0) met payload: HDR + SA (1) + VENDOR (13) + NONE (0) totale lengte: 104

Procesmodule M2.

[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van SA-lading
[IKEv1 DEBUG]: IP = 10.0.0.2, het voorstel van Oakley is aanvaardbaar
[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading
[IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen NAT-traversal RFC VID
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de nuttige lading wordt geconstrueerd
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de lading eenmaal wordt geconstrueerd
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij Cisco Unity VID-payload wordt geconstrueerd

Fabric MM3.
Dit proces isOmvatNAT ontdekkingsnuttige ladingen, Diffie-Hellman (DH) Key Exchange (KE) - nuttige ladingen (i)nitator bevat g, p en A voor de respons), en DPD ondersteuning.

30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de maximale V6 VID-lading wordt geconstrueerd
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, Verzend IOS VID
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, voor het construeren van ASA-spoofing van IOS-verkoper ID payload (versie: 1.0.0. capaciteiten: 20000001)
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de VID-lading wordt geconstrueerd
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, Verzend Altiga/Cisco VPN300/Cisco ASA GW VID
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de payload met NAT-ontdekking wordt geconstrueerd
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, NAT-detectieshash voor computers
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de payload met NAT-ontdekking wordt geconstrueerd
30 nov. 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, NAT-detectieshash voor computers

Stuur MM3.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) met payload: HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) totale lengte : 304

=
===
===
===
===
======================================

[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=0)

MM3 ontvangen van

met payload: HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) totale lengte : 284	de initiatiefnemer.
[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking bij nuttige lading [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van ISA_KE-lading [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking eenmaal payload [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading [IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen DPD VID [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van IOS/PIX-verkoper ID payload (versie: 1.0.0. capaciteiten: 00000f6f) [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading [IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen xauth V6 VID [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van de lading met NAT-ontdekking [IKEv1 DEBUG]: IP = 10.0.0.2, NAT-detectieshash voor computers [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van de lading met NAT-ontdekking [IKEv1 DEBUG]: IP = 10.0.0.2, NAT-detectieshash voor computers	Procesmodule M3. Van NAT-D payload-responder kan bepalen of indicatielampje zit achter NAT en als Achter NAT zit een antwoordapparaat. Van de DH KE krijgt de payload-responder waarden van p, g en A.
[IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de nuttige last wordt geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de lading eenmaal wordt geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij Cisco Unity VID-payload wordt geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de belasting met V6 VID wordt geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, Verzend IOS VID [IKEv1 DEBUG]: IP = 10.0.0.2, voor het construeren van ASA-spoofing van IOS-verkoper ID payload (versie: 1.0.0. capaciteiten: 20000001) [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de VID-lading wordt geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, Verzend Altiga/Cisco VPN3000/Cisco ASA GW VID [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de payload met NAT-ontdekking wordt geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, NAT-detectieshash voor computers [IKEv1 DEBUG]: IP = 10.0.0.2, waarbij de payload met NAT-ontdekking wordt geconstrueerd [IKEv1 DEBUG]: IP = 10.0.0.2, NAT-detectieshash voor computers	BOUW M4. Dit proces isOmvat NAT ontdekkingslading, D H KEesponder genereert "B" en "s" (stuurt "B" terug naar initator), en DPD VID.
[IKEv1]: IP = 10.0.0.2, verbinding geland op tunnel_group 10.0.0.2 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, genererende toetsen voor Responder...	De peer wordt geassocieerd met de 10.0.0.2 L2L tunnelgroep en de encryptie en de haktoetsen worden gegenereerd van de "s" hierboven en de pre-gedeeld-sleutel.
[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) met payload: HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) totale lengte : 304	Stuur MM4.
<===================================="===="=========="==================="="="="="="="="="="="="="="<="<="<="<="	
MM4 ontvangen van een responder.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=0) met payload: HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) totale lengte : 304
PROCES M4. Vanuit de NAT-D-lading kan de initiatiefnemer nu	[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking zoals lading [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van ISA_KE-lading [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking eenmaal payload [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading

bepalen of De beheerder zit achter NAT en of Achter NAT zit een antwoordapparaat.	[IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen Cisco Unity client-VID [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading [IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen DPD VID [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van IOS/PIX-verkoper ID payload (versie: 1.0.0. capaciteiten: 00000f (7) [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van VID-lading [IKEv1 DEBUG]: IP = 10.0.0.2, ontvangen xauth V6 VID	
Van DH KE, iDe initiator ontvangt "B" en kan nu "s" genereren.	[IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van de lading met NAT-ontdekking [IKEv1 DEBUG]: IP = 10.0.0.2, NAT-detectieshash voor computers [IKEv1 DEBUG]: IP = 10.0.0.2, verwerking van de lading met NAT-ontdekking [IKEv1 DEBUG]: IP = 10.0.0.2, NAT-detectieshash voor computers	
De peer wordt geassocieerd met de 10.0.0.2 L2L tunnelgroep en de initator genereert encryptie en haktoetsen met behulp van "s" hierboven en de pre-Shared key.	[IKEv1]: IP = 10.0.0.2, verbinding geland op tunnel_group 10.0.0.2 [IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, genererende toetsen voor Initiator...	
Opstellen M5. Gerelateerde configuratie: auto met encryptie - identiteit	[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij de ID-lading wordt geconstrueerd [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij de lading wordt geconstrueerd [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Computing hash voor ISAKMP [IKEv1 DEBUG]: IP = 10.0.0.2, bouw IOS houdt lading in leven: voorstel=32767/32767 sec. [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij dpd vaste lading wordt geconstrueerd	
Verzenden MM5.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) met payload: HDR + ID (5) + HASH (8) + IOS-BEHOUD (128) +VENDOR (13) + NIET (0) totale lengte: 96	
	= ========== ========== ========== ========== ==========	
Responder ligt niet achter een NAT. Geen NAT-T vereist.	[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, automatische NAT-detectiestatus: Afstandseinde zit NIET achter een NAT-apparaat Dit uiteinde zit NIET achter een NAT-apparaat	[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=0) met payload: HDR + ID (5) + HASH (8) + NONE (0) totale lengte: 64
	[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkings-ID-lading	MM5 ontvangen van initiatiefnemer. Dit proces isOmvat rd e oto peer Identity (ID) en ceen verbindingslanding op een bepaalde tunnelgroep.
	[IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ontvangen ID 10.0.0.2	PROCES M5. Verificatie met vooraf gedeelde toetsen begint nu.
	[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkingslading	Verificatie vindt plaats
	[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Computing hash voor ISAKMP	op beide peers; daarom ziet u twee
	[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerking melden de lading	reeksen corresponderende
	[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, automatisch NAT	echtheidsprocessen.

		[IKEv1]: IP = 10.0.0.2, verbinding geland op tunnel_group 10.0.0.2	Gerelateerde configuratie: tunnelgroep 10.0.0.2 type ipsec-l2l
		Detectiestatus: Afstandseinde zit NIET achter een NAT-apparaat Dit uiteinde zit NIET achter een NAT-apparaat	Nee NAT-T vereist in dit geval.
		[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij de ID-lading wordt geconstrueerd [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij de lading wordt geconstrueerd [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Computing hash voor ISAKMP [IKEv1 DEBUG]: IP = 10.0.0.2, bouw IOS houdt lading in leven: voorstel=32767/32767 sec. [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij dpd vaste lading wordt geconstrueerd	BOUW M6. Verzenden van identiteit omvat rekey times die zijn gestart en identiteit die naar een externe peer wordt verstuurd.
		[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) met payload: HDR + ID (5) + HASH (8) + IOS-BEHOUD (128) +VENDOR (13) + NIET (0) totale lengte: 96 <======================================"===="=========== ==============="="===="="<="=="<==="="="="="="="="="="="=" ="< ="="="="<="<= "="="="="	Stuur MM6.
MM6 ontvangen van een responder.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=0) met payload: HDR + ID (5) + HASH (8) + NONE (0) totale lengte: 64	[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, FASE 1 VOLTOOID [IKEv1]: IP = 10.0.0.2, type houd-levend voor deze verbinding: DPD [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Starttimer P1: 64800 seconden.	Fase 1 voltooid. Start de uitzettimer. Gerelateerde configuratie: crypto isakmp - beleid 10 controle vooraf encryptie 3DES hash sha groep 2 levensduur: 8640 ciscoasa# sh runt alle crypto isakmp auto met encryptie - identiteit
PROCES M6. Dit proces isOmvat remotionele identiteit verzonden van peer en feindbeslissing over te kiezen tunnelgroep .	[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkings-ID-lading [IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ontvangen ID 10.0.0.2 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkingslading [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Computing hash voor ISAKMP [IKEv1]: IP = 10.0.0.2, verbinding geland op tunnel_group 10.0.0.2 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Oakley start snelle modus [IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE-initiator met QM: msg id = 7b80c2b0		
Fase 1 voltooid. Start ISAKMP-uitzettimer. Verwante cconfiguratie: tunnelgroep 10.0.0.2 type ipsec-l2l tunnelgroep 10.0.0.2 ipsec-eigenschappen cisco met voorgedeelde toets	[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, FASE 1 VOLTOOID [IKEv1]: IP = 10.0.0.2, type houd-levend voor deze verbinding: DPD DPD is onderhandeld en fase 1 is nu voltooid. [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Starttimer P1: 82080 seconden.		

Fase 2 (snelle modus) begint.

IPSEC: Nieuwe embryonaal-SA gemaakt bij 0x53FC3C00,
SCB: 0x53F90A00,
Richting: binnenkomend
SPI : 0xFD2D851F
Session-id: 0x00006000
VPIF num : 0x0000003
Tunneltype: l2l
Protocol: esp
Lifetime: 240 seconden

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE kreeg SPI van de sleutelmotor: SPI = 0xfd2d851f

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, oakley bouwt snelle modus

Bevestig QM1. Dit proces omvat: proxy-ID's en IPsec beleid. Gerelateerde configuratie: crypto ipsec transformatie-set TRANSFORM esp-aes esp-sha-hmac Toegang tot VPN-lijst uitgebreide vergunning ICMP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.0

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, het construeren van de lading van de lege hash

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij IPSec SA-lading wordt geconstrueerd

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij IPSec eenmaal wordt geconstrueerd

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij proxy-ID wordt geconstrueerd

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, transmissieproxy-ID:
Plaatselijk subnet: 192.168.1.0-masker, 25.25.255.0 Protocol, 1 poort 0
Remote-weg: 192.168.2.0-masker, 25.25.255.0 Protocol, 1 poort 0
Plaatselijke behalve (192.168.1.0/24) en verwachte, afstandsbediening (192.168.2.0/24) worden verzonden

[IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE-initiator die eerste contactgegevens stuurt

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij qm hash payload wordt geconstrueerd

[IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE-initiator die 1ste QM-pakket verstuurt: msg id = 7b80c2b0

Verzenden QM1.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=7b80c2b0) met payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + MEDEDELING (11) + GEEN (0) totale lengte : 200

==========

[IKEv1-DECODE]: IP = 10.0.0.2, IKE Responder vanaf QM: msg steun = 52481cf5

[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=52481cf5) met payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) totale lengte: 172

QM1 ontvangen van initiatiefnemer. Responder start fase 2 (QM).

Verwerking van QM1. Dit proces vergelijkt afgelegen proxy met lokaal en selecteert aanvaardbare IPsec beleid. Verwante configuratie: crypto ipsec transformatie-set TRANSFORM esp-aes esp-sha-hmac Toegang tot VPN-lijst uitgebreide vergunning ICMP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.0 crypto kaart MAP 10 matchadres van VPN

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkingslading

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerking SA lading

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerking eenmaal lading

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkings-ID-lading

[IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID ontvangen—192.168.2.0—255.255.255.0[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, ontvangen externe IP Proxy Subnet-gegevens in ID-payload: Adres 192.168.2.0, masker 255.255.255.0, protocol 1, poort 0
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkings-ID-lading
[IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID ontvangen—192.168.1.0—255.255.255.0
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, ontvangen lokale IP Proxy Subnet-gegevens in ID-payload: Adres 192.168.1.0, masker 255.255.255.0, protocol 1, poort 0

Afgelegen en lokale subnetten (192.168.2.0/24 en 192.168.1.0/24) worden ontvangen.

[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed old als niet gevonden door addr
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, Static Crypto Map check, check map = MAP, seq = 10...
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, Static Crypto Map check, map MAP, seq = 10 is een geslaagde match
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE Remote Peer ingesteld voor crypto-kaart: MAP

Er wordt gezocht naar een bijpassend statische cryptoingang.

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerking van IPSec SA-lading
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, IPSec SA Voorstel # 1, Transformeer # 1 aanvaardbare overeenkomsten wereldwijde IPSec SA-ingang # 10
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE: SPI eisen!
IPSEC: Nieuwe embryonaal SA gemaakt bij 0x53FC3698,
SCB: 0x53FC2998,
Richting: binnenkomend
SPI : 0x1698CAC7
Session-id: 0x00004000
VPIF num : 0x0000003
Tunneltype: l2l
Protocol: esp
Lifetime: 240 seconden
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE kreeg SPI van de sleutelmotor: SPI = 0x1698cac7
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, oakley die snelle modus bouwt
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, het construeren van de lading van de lege hash
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij IPSec SA-lading wordt geconstrueerd
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij IPSec eenmaal wordt geconstrueerd
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij proxy-ID wordt geconstrueerd
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, transmissieproxy-ID:
Remote-weg: 192.168.2.0-masker, 25.25.255.0 Protocol, 1 poort 0
Plaatselijk subnet: 192.168.1.0-masker, 25.25.255.0 Protocol, 1 poort 0
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, waarbij qm hash payload wordt geconstrueerd

Bevestig QM2. Dit proces isOmvatbevestiging van de identiteit van volmacht, tunneltype en een De controle wordt uitgevoerd voor gespiegelde crypto ACL's.

[IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE Responder bij verzenden 2e QM-pakket: msg id = 52481cf5
[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=52481cf5) met payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) totale lengte: 172

Verzend QM2.

<======================================"=========="=====
=================="="="="="="="="="="="="="="="="="="="=
"="
<="<="<="<="
="="="="="

QM2 ontvangen van een responder.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=7b80c2b0) met payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + MEDEDELING (11) + GEEN (0) totale lengte : 200

Verwerking van QM2. In dit proces remotionele eindsignaal stuurt parameters en de kortste voorgestelde fase 2 van de levenscyclus wordt gekozen .	[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkingslading [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerking SA lading [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerking eenmaal lading [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkings-ID-lading [IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID ontvangen—192.168.1.0—255.255.255.0 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerkings-ID-lading [IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID ontvangen—192.168.2.0—255.255.255.0 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, verwerking melden de lading [IKEv1-DECODE]: Responder Lifetime-decode volgt (buiten SPI[4]|eigenschappen): [IKEv1-DECODE]: 0000: DDE50931 80010001 0002004 00000E10 ...1..... [IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, afgedwongen verandering van IPSec-aflossingduur van 28800 tot 3600 seconden Op basis van de respons van peer verandert de ASA bepaalde IPSEC-eigenschappen. In dit geval het rekey interval [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, alle IPSEC SA's laden [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, genereert snelmodus!
Vonden het koppelen van crypto kaart "MAP" en ingang 10 en het matchen met toegangslijst "VPN".	[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, NP encryptie regelt het zoeken naar crypto kaart MAP 10 matching ACL VPN: teruggegeven cs_id=53f11198; regel=53f11a90
Dit apparaat heeft een SPI's 0xfd2d851f en 0xdde50931f gegenereerd voor respectievelijk inkomende en uitgaande verkeer.	[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, genereert snelmodus! IPSEC: Nieuwe embryonaal SA gemaakt bij 0x53FC3698, SCB: 0x53F910F0, Richting: uitgaand SPI : 0xDDE50931 Session-id: 0x00006000 VPIF num : 0x0000003 Tunneltype: l2l Protocol: esp Lifetime: 240 seconden IPSEC: Voltooide obSA-update van host, SPI 0xDDE50931 IPSEC: Een uitgaande VPN-context maken, SPI 0xDDE50931 Vlaggen: 0x0000005 SA : 0x53FC3698 SPI : 0xDDE50931 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB : 0x01F-218F Kanaal: 0x4C69CB80 IPSEC: Volledig uitgaande VPN-context, SPI 0xDDE50931 VPN-handle: 0x000161A4 IPSEC: Nieuwe uitgaande versleuteling, SPI 0xDDE50931 SRC-addr: 192.168.1.0 Src-masker: 255.255.255.0 Toevoegen desgewenst: 192.168.2.0 Tekstmasker: 255.255.255.0 SRC-poorten Bovenkant: 0 Lager: 0 Op : negeren Testpoorten Bovenkant: 0 Lager: 0 Op : negeren Protocol: 1 Protocol gebruiken: reëel

SPI: 0x0000000
SPI gebruiken: onjuist
IPSEC: Volledig uitgaande versleuteling, SPI 0xDDE50931
Regel ID: 0x53FC3AD8
IPSEC: Nieuwe regel voor uitgaande vergunningen, SPI 0xDDE50931
SRC-addr: 10.0.0.1
Src-masker: 255.255.255.255
Toevoegen desgewenst: 10.0.0.2
Tekstmasker: 255.255.255.255
SRC-poorten
Bovenkant: 0
Lager: 0
Op : negeren
Testpoorten
Bovenkant: 0
Lager: 0
Op : negeren
Protocol: 50
Protocol gebruiken: reëel
SPI: 0xDDE50931
SPI gebruiken: reëel
IPSEC: Ingevulde uitgaande vergunningsregel, SPI 0xDDE50931
Regel ID: 0x53F91538
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, NP encryptie regelt het zoeken naar crypto kaart MAP 10 matching ACL VPN: teruggegeven cs_id=53f11198; regel=53f11a90
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, Security onderhandeling voltooid voor LAN-to-LAN groep (10.0.0.2) Initiator, inkomende SPI = 0xfd2d851f, uitgaande SPI = 0xdde50931
IPSEC: Voltooide IBSA-update, SPI 0xFD2D851F
IPSEC: Een inkomende VPN-context maken, SPI 0xFD2D851F
Vlaggen: 0x0000006
SA : 0x53FC3C00
SPI : 0xFD2D851F
MTU : 0 bytes
VCID : 0x0000000
Peer : 0x000161A4
SCB : 0x01CEA-8EF
Kanaal: 0x4C69CB80
IPSEC: Volledig inkomende VPN-context, SPI 0xFD2D851F
VPN-handle: 0x000-18BBC
IPSEC: Bijwerken van uitgaande VPN-context 0x00161A4, SPI 0xDDE50931
Vlaggen: 0x0000005
SA : 0x53FC3698
SPI : 0xDDE50931
MTU : 1500 bytes
VCID : 0x0000000
Peer : 0x000-18BBC
SCB : 0x01F-218F
Kanaal: 0x4C69CB80
IPSEC: Volledig uitgaande VPN-context, SPI 0xDDE50931
VPN-handle: 0x000161A4
IPSEC: Volledig uitgaande binnenregel, SPI 0xDDE50931
Regel ID: 0x53FC3AD8
IPSEC: Voltooide buitenste SPD-regel, SPI 0xDDE50931
Regel ID: 0x53F91538
IPSEC: Nieuwe inkomende tunnelstroomregel, SPI 0xFD2D851F
SRC-addr: 192.168.2.0
Src-masker: 255.255.255.0
Toevoegen desgewenst: 192.168.1.0
Tekstmasker: 255.255.255.0
SRC-poorten
Bovenkant: 0

bouw QM3. Bevestig alle SPI's die aan een externe peer zijn gemaakt.

	Lager: 0 Op : negeren Testpoorten Bovenkant: 0 Lager: 0 Op : negeren Protocol: 1 Protocol gebruiken: reëel SPI: 0x0000000 SPI gebruiken: onjuist IPSEC: Voltooide inkomende tunnelstroomregel, SPI 0xFD2D851F Regel ID: 0x53F91970-software IPSEC: Nieuwe decryptie-regel, SPI 0xFD2D851F SRC-addr: 10.0.0.2 Src-masker: 255.255.255.255 Toevoegen desgewenst: 10.0.0.1 Tekstmasker: 255.255.255.255 SRC-poorten Bovenkant: 0 Lager: 0 Op : negeren Testpoorten Bovenkant: 0 Lager: 0 Op : negeren Protocol: 50 Protocol gebruiken: reëel SPI: 0xFD2D851F SPI gebruiken: reëel IPSEC: Voltooide decryptie-regel, SPI 0xFD2D851F Regel ID: 0x53F91A08-software IPSEC: Nieuwe regel voor inkomende vergunningen, SPI 0xFD2D851F SRC-addr: 10.0.0.2 Src-masker: 255.255.255.255 Toevoegen desgewenst: 10.0.0.1 Tekstmasker: 255.255.255.255 SRC-poorten Bovenkant: 0 Lager: 0 Op : negeren Testpoorten Bovenkant: 0 Lager: 0 Op : negeren Protocol: 50 Protocol gebruiken: reëel SPI: 0xFD2D851F SPI gebruiken: reëel IPSEC: Ingevulde vergunningsregel, SPI 0xFD2D851F Regel ID: 0x53F91A0	
Verzend QM3.	[IKEv1-DECODE]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE-initiator die een derde QM-pakket stuurt: msg id = 7b80c2b0 =	
	========== ========== ========== ========== ==========	
Fase 2 voltooid. De initiator is nu klaar om pakketten te versleutelen en te decrypteren met deze SPI-waarden.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=7b80c2b0) met payload: HDR + HASH (8) + NONE (0) totale lengte :76 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE kreeg een KEY_ADD msg voor SA: SPI = 0xdde50931 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2,	[IKEv1]: IP = 10.0.0.2, IKE_DECODE ONTVANGEN Bericht (msgid=52481cf5) QM3 ontvangen van initiatiefnemer.

Pitcher: ontvangen KEY_UPDATE, spi 0xfd2d851f
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Starttimer P2: 3060 seconden.
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, FASE 2 COMPLETED (msgid=7b80c2b0)

met payload: HDR + HASH (8) + NONE (0) totale lengte: 52

[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, lading verwerkingshangende lading
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, alle IPSEC SA's laden
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, genereert snelmodus!
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, NP encryptie regelt het zoeken naar crypto kaart MAP 10 matching ACL VPN: teruggegeven cs_id=53f11198; regel=53f11a90
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, genereert snelmodus!
IPSEC: Nieuwe embryonaal SA gemaakt bij 0x53F18B00,
SCB: 0x53F8A1C0,
Richting: uitgaand
SPI : 0xDB680406
Session-id: 0x00004000
VPIF num : 0x0000003
Tunneltype: l2l
Protocol: esp
Lifetime: 240 seconden
IPSEC: Voltooide obSA-update van host, SPI 0xDB680406
IPSEC: Een uitgaande VPN-context maken, SPI 0xDB680406
Vlaggen: 0x0000005
SA : 0x53F18B00-software
SPI : 0xDB680406
MTU : 1500 bytes
VCID : 0x0000000
Peer : 0x0000000
SCB : 0x005E4849
Kanaal: 0x4C69CB80
IPSEC: Volledig uitgaande VPN-context, SPI 0xDB680406
VPN-handle: 0x000E9B4
IPSEC: Nieuwe uitgaande encryptieregel, SPI 0xDB680406
SRC-addr: 192.168.1.0
Src-masker: 255.255.255.0
Toevoegen desgewenst: 192.168.2.0
Tekstmasker: 255.255.255.0
SRC-poorten
Bovenkant: 0
Lager: 0
Op : negeren
Testpoorten
Bovenkant: 0
Lager: 0
Op : negeren
Protocol: 1
Protocol gebruiken: reëel
SPI: 0x0000000
SPI gebruiken: onjuist
IPSEC: Volledig uitgaande versleutelde regel, SPI 0xDB680406
Regel ID: 0x53F89160
IPSEC: Nieuwe regel voor uitgaande vergunningen, SPI 0xDB680406
SRC-addr: 10.0.0.1
Src-masker: 255.255.255.255
Toevoegen desgewenst: 10.0.0.2
Tekstmasker: 255.255.255.255
SRC-poorten
Bovenkant: 0
Lager: 0
Op : negeren
Testpoorten
Bovenkant: 0

QM3-proces. Er worden encryptiesleutels gegenereerd voor de data-eenheden. Tijdens deze procedure: SPI's worden ingesteld om het verkeer over te brengen.

Lager: 0
Op : negeren
Protocol: 50
Protocol gebruiken: reëel
SPI: 0xDB680406
SPI gebruiken: reëel
IPSEC: Ingevulde uitgaande vergunningsregel, SPI 0xDB680406
Regel ID: 0x53E47E88
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, NP encryptie regelt het zoeken naar crypto kaart MAP 10 matching ACL VPN: teruggegeven cs_id=53f11198; regel=53f11a90
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, Security onderhandeling voltooid voor LAN-to-LAN groep (10.0.0.2) Responder, inkomende SPI = 0x1698cac7, uitgaande SPI = 0xdb680406
[IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, IKE kreeg een KEY_ADD msg voor SA: SPI = 0xdb680406
IPSEC: Voltooide IBSA-update, SPI 0x1698CAC7
IPSEC: Creëren van inkomende VPN-context, SPI 0x1698CAC7
Vlaggen: 0x0000006
SA : 0x53FC3698
SPI : 0x1698CAC7
MTU : 0 bytes
VCID : 0x0000000
Peer : 0x000E9B4
SCB : 0x005DAE51
Kanaal: 0x4C69CB80
IPSEC: Volledig inkomende VPN-context, SPI 0x1698CAC7
VPN-handle: 0x0011A8C
IPSEC: Bijwerken van uitgaande VPN-context 0x000E9B4, SPI 0xDB680406
Vlaggen: 0x0000005
SA : 0x53F18B00-software
SPI : 0xDB680406
MTU : 1500 bytes
VCID : 0x0000000
Peer : 0x0011A8C
SCB : 0x005E4849
Kanaal: 0x4C69CB80
IPSEC: Volledig uitgaande VPN-context, SPI 0xDB680406
VPN-handle: 0x000E9B4
IPSEC: Volledig uitgaande binnenregel, SPI 0xDB680406
Regel ID: 0x53F89160
IPSEC: Voltooide buitenste SPD-regel, SPI 0xDB680406
Regel ID: 0x53E47E88
IPSEC: Nieuwe inkomende tunnelstroomregel, SPI 0x1698CAC7
SRC-addr: 192.168.2.0
Src-masker: 255.255.255.0
Toevoegen desgewenst: 192.168.1.0
Tekstmasker: 255.255.255.0
SRC-poorten
Bovenkant: 0
Lager: 0
Op : negeren
Testpoorten
Bovenkant: 0
Lager: 0
Op : negeren
Protocol: 1
Protocol gebruiken: reëel
SPI: 0x0000000
SPI gebruiken: onjuist
IPSEC: Voltooide inkomende tunnelstroomregel, SPI 0x1698CAC7
Regel ID: 0x53FC3E4-E80
IPSEC: Nieuwe decrypt regel, SPI 0x1698CAC7

Aan de gegevens SA's worden SPI's toegewezen.

SRC-addr: 10.0.0.2 Src-masker: 255.255.255.255 Toevoegen desgewenst: 10.0.0.1 Tekstmasker: 255.255.255.255 SRC-poorten Bovenkant: 0 Lager: 0 Op : negeren Testpoorten Bovenkant: 0 Lager: 0 Op : negeren Protocol: 50 Protocol gebruiken: reëel SPI: 0x1698CAC7 SPI gebruiken: reëel IPSEC: Voltooide decryptie-regel, SPI 0x1698CAC7 Regel ID: 0x53FC3F18 IPSEC: Nieuwe regels voor inkomende vergunningen, SPI 0x1698CAC7 SRC-addr: 10.0.0.2 Src-masker: 255.255.255.255 Toevoegen desgewenst: 10.0.0.1 Tekstmasker: 255.255.255.255 SRC-poorten Bovenkant: 0 Lager: 0 Op : negeren Testpoorten Bovenkant: 0 Lager: 0 Op : negeren Protocol: 50 Protocol gebruiken: reëel SPI: 0x1698CAC7 SPI gebruiken: reëel IPSEC: Ingevulde vergunningsregel, SPI 0x1698CAC7 Regel ID: 0x53F8EA8 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Pitcher: ontvangen KEY_UPDATE, spi 0x1698cac7 [IKEv1 DEBUG]: Groep = 10.0.0.2, IP = 10.0.0.2, Starttimer P2: 3060 seconden.	Start IPsec opnieuw.
[IKEv1]: Groep = 10.0.0.2, IP = 10.0.0.2, FASE 2 COMPLETED (msgid=52481cf5)	Fase 2 voltooid. Zowel responder als initiator kunnen verkeer versleutelen/decrypteren.

Tunnelverificatie

Opmerking: Aangezien ICMP wordt gebruikt om de tunnel te activeren, is slechts één IPSec SA omhoog. 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

Gerelateerde informatie

- Een goede plek om te beginnen is wikipedia-artikel op IPSec2. Standaard en referenties bevatten veel nuttige informatie
- IPsec-probleemoplossing: Opdrachten begrijpen en gebruiken
- Technische ondersteuning en documentatie – Cisco Systems