IPSec ASA y debugs IKE (modo principal IKEv1) que resuelven problemas la Nota Técnica

Contenido

Introducción

Este documento describe los debugs en el dispositivo de seguridad adaptante (ASA) cuando utilizan al modo principal y la clave previamente compartida (PSK). También se trata la traducción de ciertas líneas de debug en la configuración.

Los temas no discutidos en este documento incluyen el paso del tráfico después de que se haya establecido el túnel y los conceptos básicos de IPSec o de Internet Key Exchange (IKE).

Prerequisites

Requisitos

Los Quien lea este documento deben tener conocimiento de estos temas.

- PSK
- IKE

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cisco ASA 9.3.2
- Routers que ejecuta el ® 12.4T del Cisco IOS

Cuestión central

Los debugs IKE y del IPSec son a veces secretos, pero usted puede utilizarlos para entender

donde se localiza un problema del establecimiento del túnel del IPSec VPN.

Situación

Utilizan al modo principal típicamente entre los túneles de LAN a LAN o, en el caso del Acceso Remoto (EzVPN), cuando los Certificados se utilizan para la autenticación.

Los debugs son a partir de dos ASA que funcionen con la versión de software 9.3.2. Los dos dispositivos formarán un túnel de LAN a LAN.

Se describen dos escenarios principales:

- ASA como el iniciador para el IKE
- ASA como el respondedor para el IKE

Comandos Debug usados

debug crypto ikev1 127

IPSec 127 del debug crypto

Configuración ASA

Configuración 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
```

Configuración 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
```

Configuración del 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
```

Depuración

Descripción del mensaje del iniciador	Depuraciones	Descripción del mensaje del respondedor
El intercambio del modo principal comienza; no se ha compartido ningunas directivas, y los pares todavía están adentro MM_NO_STATE. Como el iniciador, el ASA comienza a construir el payload.	DEBUG [IKEv1]: Jarra: recibió una clave adquieren el mensaje, el spi 0x0 IPSEC(crypto_map_check)-3: Buscar la correspondencia de criptografía que corresponde con 5-tuple: Prot=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3: Marcar el MAPA 10 de la correspondencia de criptografía: correspondido con. [IKEv1]: IP= 10.0.0.2, iniciador IKE: Nueva fase 1, Intf dentro, dirección del proxy local 192.168.1.0 de 10.0.0.2 del par IKE, dirección del proxy remota 192.168.2.0, correspondencia de criptografía (MAPA)	
Construcción MM1 Este proceso incluye la oferta inicial para el IKE y los vendedores soportados NAT-T.	DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el DEBUG del **payload** [IKEv1 **ISAKMP SA**]: IP= 10.0.0.2, construyendo el payload del ver 02 del NAT-Traversal VID DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload del ver 03 del NAT-Traversal VID DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload del ver RFC del NAT-Traversal VID DEBUG [IKEv1]: El IP= 10.0.0.2, construyendo la fragmentación VID + amplió el payload de las capacidades	
Envíe MM1.	[IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=0) con las cargas útiles: HDR + SA (1) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NINGUNOS (0) longitudes totales: 168 ==========MM1========== ====>	
	[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=0) con las cargas útiles: HDR + SA (1) + VENDEDOR (13) +VENDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NINGUNOS (0) longitudes totales: 164	MM1 recibido del iniciador.
	DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload SA DEBUG [IKEv1]: El IP= 10.0.0.2, oferta del Oakley es aceptable DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID DEBUG [IKEv1]: IP= 10.0.0.2, NAT-Traversal recibido RFC VID DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID DEBUG [IKEv1]: IP= 10.0.0.2, ver recibido 03 VID del NAT-Traversal DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID DEBUG [IKEv1]: IP= 10.0.0.2, ver recibido 02 VID del NAT-Traversal DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload IKE SA DEBUG [IKEv1]: El IP= 10.0.0.2, oferta IKE SA # 1, transforma # 1 entrada global de las coincidencias aceptables IKE # 2	Proceso MM1. La comparación de las directivas ISAKMP/IKE comienza. El peer remoto hace publicidad que puede utilizar el NAT-T. Configuración relacionada: *política isakmp crypto 10*

		authentication pre-share *cifrado 3des* *sha del hash* *group2* *lifetime 86400*
	DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload ISAKMP SA DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload del ver 02 del NAT-Traversal VID DEBUG [IKEv1]: El IP= 10.0.0.2, construyendo la fragmentación VID + amplió el payload de las capacidades	Construcción MM2. En este mensaje el respondedor selecciona que las configuraciones de la política isakmp a utilizar. También hace publicidad de las versiones NAT-T que puede utilizar.
	[IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=0) con las cargas útiles: HDR + SA (1) + VENDEDOR (13) + longitud total del VENDEDOR (13) + NONE(0): 128 <==========MM2==========	Envíe MM2.
MM2 recibido del respondedor.	[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=0) con las cargas útiles: HDR + SA (1) + VENDEDOR (13) + NINGUNOS (0) longitudes totales: 104	
Proceso MM2.	DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload SA DEBUG [IKEv1]: El IP= 10.0.0.2, oferta del Oakley es aceptable DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID DEBUG [IKEv1]: IP= 10.0.0.2, NAT-Traversal recibido RFC VID	
Construcción MM3. Cargas útiles de esta del proceso detección del includesNAT, cargas útiles del intercambio de claves del Diffie-Hellman (DH) (KE) (el initator incluye g, p, y A al respondedor), y soporte DPD.	30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, construyendo el payload KE 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, construyendo el payload del nonce 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, construyendo el payload del Cisco Unity VID 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, construyendo el payload del Xauth V6 VID 30 de noviembre DEBUG [IKEv1 de 10:38:29]: El IP= 10.0.0.2, envía IOS VID 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, construyendo el payload del Vendor ID IOS del spoofing ASA (versión: 1.0.0, capacidades: 20000001) 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, construyendo el payload VID 30 de noviembre DEBUG [IKEv1 de 10:38:29]: El IP= 10.0.0.2, envía Altiga/Cisco VPN3000/Cisco ASA GW VID 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, construyendo el payload de la NAT-detección 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, hash computacional de la detección NAT 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, construyendo el payload de la NAT-detección 30 de noviembre DEBUG [IKEv1 de 10:38:29]: IP= 10.0.0.2, hash computacional de la detección NAT	
Envíe MM3.	[IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=0) con las cargas útiles: HDR + KE (4) + NONCE (10) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (20) + NAT-D (20) + NINGUNOS (0) longitudes totales: 304 ==========MM3==========>	
	[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=0) con las cargas útiles: HDR + KE (4) + NONCE (10) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (130) + NAT-D (130) + NINGUNOS (0) longitudes totales: 284	MM3 recibido del iniciador.
	DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload KE	Proceso MM3.

DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload ISA_KE
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload del nonce
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID
DEBUG [IKEv1]: IP= 10.0.0.2, DPD recibido VID
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload del Vendor ID IOS/PIX (versión: 1.0.0, capacidades: 00000f6f)
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID
DEBUG [IKEv1]: IP= 10.0.0.2, Xauth recibido V6 VID
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload de la NAT-detección
DEBUG [IKEv1]: IP= 10.0.0.2, hash computacional de la detección NAT
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload de la NAT-detección

De las cargas útiles NAT-D el respondedor puede determinar si el initator está detrás de NAT y si el respondedor está detrás de NAT.
Del DH KE, el respondedor del payload consigue los valores de p, de g y del A.

DEBUG [IKEv1]: IP= 10.0.0.2, hash computacional de la detección NAT
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload KE
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload del nonce
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload del Cisco Unity VID
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload del Xauth V6 VID
DEBUG [IKEv1]: El IP= 10.0.0.2, envía IOS VID
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload del Vendor ID IOS del spoofing ASA (versión: 1.0.0, capacidades: 20000001)
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload VID
DEBUG [IKEv1]: El IP= 10.0.0.2, envía Altiga/Cisco VPN3000/Cisco ASA GW VID
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload de la NAT-detección
DEBUG [IKEv1]: IP= 10.0.0.2, hash computacional de la detección NAT
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload de la NAT-detección
DEBUG [IKEv1]: IP= 10.0.0.2, hash computacional de la detección NAT

Construcción MM4. Este proceso incluye el payload de la detección NAT, el respondedor DH KE genera “B” y “s” (devuelve “B” al initator), y DPD VID.

[IKEv1]: IP= 10.0.0.2, conexión aterrizada en el tunnel_group 10.0.0.2
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, generando las claves para el respondedor…

Asocian al par al grupo de túnel de 10.0.0.2 L2L, y el cifrado y las claves del hash se generan del “s” arriba y de la clave previamente compartida.

[IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=0) con las cargas útiles: HDR + KE (4) + NONCE (10) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (130) + NAT-D (130) + NINGUNOS (0) longitudes totales: 304
<==========MM4==========

Envíe MM4.

MM4 recibido del respondedor.

[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=0) con las cargas útiles: HDR + KE (4) + NONCE (10) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (20) + NAT-D (20) + NINGUNOS (0) longitudes totales: 304
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload del ike
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload ISA_KE
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload del nonce
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID
DEBUG [IKEv1]: IP= 10.0.0.2, cliente recibido VID del Cisco Unity
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID
DEBUG [IKEv1]: IP= 10.0.0.2, DPD recibido VID
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload del Vendor ID IOS/PIX (versión: 1.0.0, capacidades: 00000f7f)
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload VID
DEBUG [IKEv1]: IP= 10.0.0.2, Xauth recibido V6 VID
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload de la NAT-detección
DEBUG [IKEv1]: IP= 10.0.0.2, hash computacional de la detección NAT
DEBUG [IKEv1]: IP= 10.0.0.2, procesando el payload de la NAT-detección

Proceso MM4.
De las cargas útiles NAT-D, el initator puede ahora determinar si el iniator está detrás de NAT y si el respondedor está detrás de NAT.

Del DH KE, el iniciador recibe “B” y puede ahora generar el “S.”

DEBUG [IKEv1]: IP= 10.0.0.2, hash computacional de la detección NAT

Asocian al par al grupo de túnel de 10.0.0.2 L2L, y el initator genera las claves del cifrado y del hash usando “s” arriba y la clave previamente compartida.

[IKEv1]: IP= 10.0.0.2, conexión aterrizada en el tunnel_group 10.0.0.2
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, generando las claves para el iniciador…

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload ID
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload del hash
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, hash computacional para el ISAKMP
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload de la señal de mantenimiento IOS: sec proposal=32767/32767.
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload del vid del dpd
[IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=0) con las cargas útiles: HDR + ID (5) + HASH (8) + KEEPALIVE IOS (128) +VENDOR (13) + NINGUNOS (0) longitudes totales: 96

Construcción MM5. Configuración relacionada:
auto crypto de la identidad del isakmp

Envíe MM5.

==========MM5==========>

El respondedor no está detrás de ningún NAT. Ningún NAT-T requerido.

[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, estatus automático de la detección NAT: El extremo remoto no está detrás de un dispositivo NAT para este fin no está detrás de un dispositivo NAT

[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=0) con las cargas útiles: HDR + ID (5) + HASH (8) + NINGUNOS (0) longitudes totales: 64

MM5 recibido del iniciador.
Este proceso incluye la identidad del peer remoto (ID) y el aterrizaje de la conexión en un grupo del túnel particular.

Proceso MM5.
La autenticación con las claves previamente compartidas ahora comienza.
La autenticación ocurre en ambos pares; por lo tanto, usted verá dos conjuntos de los procesos de autenticación correspondientes.
Configuración relacionada:
tipo ipsec-l2l de 10.0.0.2 del grupo de túnel
Ningún NAT-T requerido en este caso.

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload identificador de proceso
[IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR ID recibido 10.0.0.2
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload del hash
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, hash computacional para el ISAKMP
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, procesando notifican el payload
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2,Automatic NAT
[IKEv1]: IP= 10.0.0.2, conexión aterrizada en el tunnel_group 10.0.0.2

Estatus de la detección: El extremo remoto no está detrás de un dispositivo NAT para este fin no está detrás de un dispositivo NAT
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload ID
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload del hash
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, hash computacional para el ISAKMP
DEBUG [IKEv1]: IP= 10.0.0.2, construyendo el payload de la señal de

Construcción MM6.
Envíe la identidad incluye reintroducen las épocas comenzadas y la identidad enviada al peer remoto.

		mantenimiento IOS: sec proposal=32767/32767. DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload del vid del dpd [IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=0) con las cargas útiles: HDR + ID (5) + HASH (8) + KEEPALIVE IOS (128) +VENDOR (13) + NINGUNOS (0) longitudes totales: 96 <==========MM6==========	Envíe MM6.
MM6 recibido del respondedor.	[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=0) con las cargas útiles: HDR + ID (5) + HASH (8) + NINGUNOS (0) longitudes totales: 64	[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, FASE 1 COMPLETADA [IKEv1]: IP= 10.0.0.2, tipo señal de mantenimiento para esta conexión: DPD DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, comenzando el P1 reintroducen el temporizador: 64800 segundos.	Fase 1 completa. El isakmp del comienzo reintroduce el temporizador. Configuración relacionada: política isakmp crypto 10 authentication pre-share cifrado 3des sha del hash group2 lifetime 86400 ciscoasa # sh run todo el isakmp crypto auto crypto de la identidad del isakmp
Proceso MM6. Este proceso incluye la identidad remota enviada del par y de la decisión final con respecto al grupo de túnel de escoger.	DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload identificador de proceso [IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR ID recibido 10.0.0.2 DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload del hash DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, hash computacional para el ISAKMP [IKEv1]: IP= 10.0.0.2, conexión aterrizada en el tunnel_group 10.0.0.2 DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, Oakley comienzan el Quick Mode [IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, iniciador IKE que comienza el QM: msg identificación = 7b80c2b0		
Fase 1 completa. El comienzo ISAKMP reintroduce el temporizador. Configuración relacionada: tipo ipsec-l2l de 10.0.0.2 del grupo de túnel IPSec-atributos de 10.0.0.2 del grupo de túnel pre-shared-key cisco	[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, FASE 1 COMPLETADA [IKEv1]: IP= 10.0.0.2, tipo señal de mantenimiento para esta conexión: DPD El DPD tiene abeja negociada y la fase 1 es completa ahora. DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, comenzando el P1 reintroducen el temporizador: 82080 segundos.		
La fase 2 (Quick Mode) comienza.	IPSEC: Nuevo @ 0x53FC3C00 creado SA embrionario, SCB: 0x53F90A00, Dirección: entrante SPI: 0xFD2D851F ID de sesión: 0x00006000 VPIF numérico: 0x00000003 Tipo de túnel: l2l Protocolo: especialmente Vida útil: 240 segundos		
Construcción QM1. Este proceso	DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, IKE consiguieron SPI del motor dominante: SPI = 0xfd2d851f		

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, Quick Mode constucting del oakley

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload en blanco del hash

incluye los ID de proxy y las directivas del IPSec.
Configuración relacionada:
el transforme el conjunto crypto del IPSec
TRANSFORMA el esp-sha-hmac del ESP-aes
la lista de acceso VPN extendió ICMP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 del permiso

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload IPSec SA

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload del nonce del IPSec

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el ID de proxy

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID de proxy que transmite:
Subred local: puerto 0 del protocolo 1 de 255.255.255.0 de la máscara de 192.168.1.0
Subred remota: Puerto 0 del protocolo 1 de 255.255.255.0 de la máscara de 192.168.2.0
Se están enviando la subred local (192.168.1.0/24) y la subred remota expcted (192.168.2.0/24)

[IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, iniciador IKE que envía el contacto inicial

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload del hash del qm

[IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, iniciador IKE que envía el 1r pkt QM: msg identificación = 7b80c2b0

Envíe QM1.

[IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=7b80c2b0) con las cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + el ID (5) + ID (5) + NOTIFICA (11) + NINGUNOS (0) longitudes totales: 200

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

[IKEv1 DECODIFICAN]: IP= 10.0.0.2, respondedor IKE que comienza el QM: msg identificación = 52481cf5

QM1 recibido del iniciador.

[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=52481cf5) con las cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NINGUNOS (0) longitudes totales: 172

El respondedor comienza la fase 2 (QM).
Proceso QM1.
Este proceso compara los proxys remotos con el local
y selecciona la directiva aceptable del IPSec.
Configuración relacionada: el transforme el conjunto crypto del IPSec
TRANSFORMA el esp-sha-hmac del ESP-aes
la lista de acceso VPN extendió ICMP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 del permiso
direccionamiento VPN de la coincidencia del MAPA 10 de la correspondencia de criptografía

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload del hash

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload SA

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload del nonce

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload identificador de proceso

[IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR_SUBNET ID received--192.168.2.0--

Se reciben el telecontrol y las subredes locales

255.255.255.0[IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, recibieron los datos de la subred del proxy del IP remoto en el payload ID: Dirija 192.168.2.0, máscara 255.255.255.0, el protocolo 1, el puerto 0
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload identificador de proceso
[IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR_SUBNET ID received--192.168.1.0--255.255.255.0
[IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, recibieron los datos de la subred del proxy del IP local en el payload ID: Dirija 192.168.1.0, máscara 255.255.255.0, el protocolo 1, el puerto 0

(192.168.2.0/24 y 192.168.1.0/24).

[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, sa viejo QM IsRekeyed no encontrado por el addr
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, control de la correspondencia de criptografía estática, marcando la correspondencia = el MAPA, = 10 seq…
[IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, control de la correspondencia de criptografía estática, MAPA de la correspondencia, = 10 seq es una correspondencia con éxito
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, peer remoto IKE configurado para la correspondencia de criptografía: MAPA

Se busca y se encuentra una entrada crypto estática que corresponde con.

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload IPSec SA
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, oferta IPSec SA # 1, transforman # 1 entrada global IPSec SA de las coincidencias aceptables # 10
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, IKE: ¡petición de SPI!
IPSEC: Nuevo @ 0x53FC3698 creado SA embrionario,
SCB: 0x53FC2998,
Dirección: entrante
SPI: 0x1698CAC7
ID de sesión: 0x00004000
VPIF numérico: 0x00000003
Tipo de túnel: l2l
Protocolo: especialmente
Vida útil: 240 segundos
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, IKE consiguieron SPI del motor dominante: SPI = 0x1698cac7
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, oakley que construye el Quick Mode
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload en blanco del hash
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload IPSec SA
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload del nonce del IPSec
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el ID de proxy
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID de proxy que transmite:
Subred remota: Puerto 0 del protocolo 1 de 255.255.255.0 de la máscara de 192.168.2.0
Subred local: puerto 0 del protocolo 1 de 255.255.255.0 de la máscara de 192.168.1.0
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, construyendo el payload del hash del qm
[IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, respondedor IKE que envía el 2do pkt QM: msg identificación = 52481cf5

Construcción QM2. Este proceso incluye la confirmación de las identidades de representación, tipo de túnel, y un control se realiza para el ACL de criptografía duplicado.

[IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=52481cf5) con las cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NINGUNOS (0) longitudes totales: 172

Envíe QM2.

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

QM2 recibido del respondedor.

[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=7b80c2b0) con las cargas útiles: HDR + HASH (8) + SA (1) +

	NONCE (10) + el ID (5) + ID (5) + NOTIFICA (11) + NINGUNOS (0) longitudes totales: 200 DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload del hash DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload SA DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload del nonce DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload identificador de proceso [IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR_SUBNET ID received--192.168.1.0--255.255.255.0 DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload identificador de proceso [IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR_SUBNET ID received--192.168.2.0--255.255.255.0 DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, procesando notifican el payload [IKEv1 DECODIFICAN]: El respondedor que el curso de la vida decodifica sigue (outb SPI[4]|attributes): [IKEv1 DECODIFICAN]: 0000: DDE50931 80010001 00020004 00000E10… 1 ..... [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, respondedor que fuerza el cambio del IPSec que reintroduce la duración a partir del 28800 a 3600 segundos de acuerdo con la respuesta del par, el ASA está cambiando ciertos atributos del IPSEC. En este caso el intervalo de la reintroducción DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, cargando todo el SA de IPSec DEBUG [IKEv1]: ¡Grupo = 10.0.0.2, IP= 10.0.0.2, generando la clave del Quick Mode!
Proceso QM2. En este proceso, el extremo remoto envía los parámetros y se escogen los cursos de la vida propuestos más cortos de la fase 2.	
Correspondencia de criptografía que corresponde con “MAPA” Found y entrada 10 y correspondido con le contra la lista de acceso “VPN.”	DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, NP cifran la regla miran para arriba para el MAPA 10 ACL que corresponde con VPN de la correspondencia de criptografía: cs_id=53f11198 vuelto; rule=53f11a90
El dispositivo ha generado el tráfico entrante y saliente 0xfd2d851f y 0xdde50931for SPI respectivamente.	DEBUG [IKEv1]: ¡Grupo = 10.0.0.2, IP= 10.0.0.2, generando la clave del Quick Mode! IPSEC: Nuevo @ 0x53FC3698 creado SA embrionario, SCB: 0x53F910F0, Dirección: saliente SPI: 0xDDE50931 ID de sesión: 0x00006000 VPIF numérico: 0x00000003 Tipo de túnel: l2l Protocolo: especialmente Vida útil: 240 segundos IPSEC: Actualización completada del host OBSA, SPI 0xDDE50931 IPSEC: Crear el contexto saliente VPN, SPI 0xDDE50931 Indicadores: 0x00000005 SA: 0x53FC3698 SPI: 0xDDE50931 MTU: 1500 bytes VCID: 0x00000000 Entidad par: 0x00000000 SCB: 0x01CF218F Canal: 0x4C69CB80 IPSEC: Contexto saliente completado VPN, SPI 0xDDE50931 Manija VPN: 0x000161A4 IPSEC: Nuevo saliente cifra la regla, SPI 0xDDE50931 Addr del src: 192.168.1.0 Máscara del src: 255.255.255.0 Addr del dst: 192.168.2.0

Máscara del dst: 255.255.255.0
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 1
Protocolo del uso: verdad
SPI: 0x00000000
Uso SPI: falso
IPSEC: Saliente completado cifra la regla, SPI 0xDDE50931
Regla ID: 0x53FC3AD8
IPSEC: Nueva regla saliente del permiso, SPI 0xDDE50931
Addr del src: 10.0.0.1
Máscara del src: 255.255.255.255
Addr del dst: 10.0.0.2
Máscara del dst: 255.255.255.255
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 50
Protocolo del uso: verdad
SPI: 0xDDE50931
Uso SPI: verdad
IPSEC: Regla saliente completada del permiso, SPI 0xDDE50931
Regla ID: 0x53F91538
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, NP cifran la regla miran para arriba para el MAPA 10 ACL que corresponde con VPN de la correspondencia de criptografía: cs_id=53f11198 vuelto; rule=53f11a90
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, negociación de seguridad completa para el iniciador del grupo del LAN a LAN (10.0.0.2), SPI entrante = 0xfd2d851f, SPI saliente = 0xdde50931
IPSEC: Actualización completada del host IBSA, SPI 0xFD2D851F
IPSEC: Crear el contexto entrante VPN, SPI 0xFD2D851F
Indicadores: 0x00000006
SA: 0x53FC3C00
SPI: 0xFD2D851F
MTU: bytes 0
VCID: 0x00000000
Entidad par: 0x000161A4
SCB: 0x01CEA8EF
Canal: 0x4C69CB80
IPSEC: Contexto entrante completado VPN, SPI 0xFD2D851F
Manija VPN: 0x00018BBC
IPSEC: Puesta al día del contexto saliente 0x000161A4 VPN, SPI 0xDDE50931
Indicadores: 0x00000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 bytes
VCID: 0x00000000
Entidad par: 0x00018BBC
SCB: 0x01CF218F
Canal: 0x4C69CB80
IPSEC: Contexto saliente completado VPN, SPI 0xDDE50931
Manija VPN: 0x000161A4

Construcción QM3. Confirme todos los SPI creados al peer remoto.

IPSEC: Regla interna saliente completada, SPI 0xDDE50931
Regla ID: 0x53FC3AD8
IPSEC: Regla externa saliente completada SPD, SPI 0xDDE50931
Regla ID: 0x53F91538
IPSEC: Nueva regla entrante del flujo del túnel, SPI 0xFD2D851F
Addr del src: 192.168.2.0
Máscara del src: 255.255.255.0
Addr del dst: 192.168.1.0
Máscara del dst: 255.255.255.0
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 1
Protocolo del uso: verdad
SPI: 0x00000000
Uso SPI: falso
IPSEC: Regla entrante completada del flujo del túnel, SPI 0xFD2D851F
Regla ID: 0x53F91970
IPSEC: Nueva regla entrante del decrypt, SPI 0xFD2D851F
Addr del src: 10.0.0.2
Máscara del src: 255.255.255.255
Addr del dst: 10.0.0.1
Máscara del dst: 255.255.255.255
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 50
Protocolo del uso: verdad
SPI: 0xFD2D851F
Uso SPI: verdad
IPSEC: Regla entrante completada del decrypt, SPI 0xFD2D851F
Regla ID: 0x53F91A08
IPSEC: Nueva regla entrante del permiso, SPI 0xFD2D851F
Addr del src: 10.0.0.2
Máscara del src: 255.255.255.255
Addr del dst: 10.0.0.1
Máscara del dst: 255.255.255.255
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 50
Protocolo del uso: verdad
SPI: 0xFD2D851F
Uso SPI: verdad
IPSEC: Regla entrante completada del permiso, SPI 0xFD2D851F
Regla ID: 0x53F91AA0

Envíe QM3.

[IKEv1 DECODIFICAN]: Grupo = 10.0.0.2, IP= 10.0.0.2, iniciador IKE que envía el 3ro pkt QM: msg identificación = 7b80c2b0

==========QM3==========

Fase 2 completa.
El iniciador está listo ahora para cifrar y para desencriptar los paquetes usando estos valores de SPI.

====>
[IKEv1]: IP= 10.0.0.2, IKE_DECODE QUE ENVÍA el mensaje (msgid=7b80c2b0) con las cargas útiles: HDR + HASH (8) + NINGUNOS (0) longitudes totales: 76
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, IKE consiguieron un msg KEY_ADD para el SA: SPI = 0xdde50931
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, jarra: KEY_UPDATE recibido, spi 0xfd2d851f
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, comenzando el P2 reintroducen el temporizador: 3060 segundos.
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, FASE 2 COMPLETADA (msgid=7b80c2b0)

[IKEv1]: El IP= 10.0.0.2, IKE_DECODE RECIBIÓ el mensaje (msgid=52481cf5) con las cargas útiles: HDR + HASH (8) + NINGUNOS (0) longitudes totales: 52

Iniciador del fom del receivd QM3.

DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, procesando el payload del hash
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, cargando todo el SA de IPSec
DEBUG [IKEv1]: ¡Grupo = 10.0.0.2, IP= 10.0.0.2, generando la clave del Quick Mode!
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, NP cifran la regla miran para arriba para el MAPA 10 ACL que corresponde con VPN de la correspondencia de criptografía: cs_id=53f11198 vuelto; rule=53f11a90
DEBUG [IKEv1]: ¡Grupo = 10.0.0.2, IP= 10.0.0.2, generando la clave del Quick Mode!
IPSEC: Nuevo @ 0x53F18B00 creado SA embrionario,
SCB: 0x53F8A1C0,
Dirección: saliente
SPI: 0xDB680406
ID de sesión: 0x00004000
VPIF numérico: 0x00000003
Tipo de túnel: l2l
Protocolo: especialmente
Vida útil: 240 segundos
IPSEC: Actualización completada del host OBSA, SPI 0xDB680406
IPSEC: Crear el contexto saliente VPN, SPI 0xDB680406
Indicadores: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 bytes
VCID: 0x00000000
Entidad par: 0x00000000
SCB: 0x005E4849
Canal: 0x4C69CB80
IPSEC: Contexto saliente completado VPN, SPI 0xDB680406
Manija VPN: 0x0000E9B4
IPSEC: Nuevo saliente cifra la regla, SPI 0xDB680406
Addr del src: 192.168.1.0
Máscara del src: 255.255.255.0
Addr del dst: 192.168.2.0
Máscara del dst: 255.255.255.0
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 1
Protocolo del uso: verdad
SPI: 0x00000000
Uso SPI: falso
IPSEC: Saliente completado cifra la regla, SPI 0xDB680406

Proceso QM3.
Las claves de encripción se generan para los datos SA.
Durante este proceso, Los SPI se fijan para pasar el tráfico.

Regla ID: 0x53F89160
IPSEC: Nueva regla saliente del permiso, SPI 0xDB680406
Addr del src: 10.0.0.1
Máscara del src: 255.255.255.255
Addr del dst: 10.0.0.2
Máscara del dst: 255.255.255.255
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 50
Protocolo del uso: verdad
SPI: 0xDB680406
Uso SPI: verdad
IPSEC: Regla saliente completada del permiso, SPI 0xDB680406
Regla ID: 0x53E47E88
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, NP cifran la regla miran para arriba para el MAPA 10 ACL que corresponde con VPN de la correspondencia de criptografía: cs_id=53f11198 vuelto; rule=53f11a90
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, negociación de seguridad completa para el respondedor del grupo del LAN a LAN (10.0.0.2), SPI entrante = 0x1698cac7, SPI saliente = 0xdb680406
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, IKE consiguieron un msg KEY_ADD para el SA: SPI = 0xdb680406
IPSEC: Actualización completada del host IBSA, SPI 0x1698CAC7
IPSEC: Crear el contexto entrante VPN, SPI 0x1698CAC7
Indicadores: 0x00000006
SA: 0x53FC3698
SPI: 0x1698CAC7
MTU: bytes 0
VCID: 0x00000000
Entidad par: 0x0000E9B4
SCB: 0x005DAE51
Canal: 0x4C69CB80
IPSEC: Contexto entrante completado VPN, SPI 0x1698CAC7
Manija VPN: 0x00011A8C
IPSEC: Puesta al día del contexto saliente 0x0000E9B4 VPN, SPI 0xDB680406
Indicadores: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 bytes
VCID: 0x00000000
Entidad par: 0x00011A8C
SCB: 0x005E4849
Canal: 0x4C69CB80
IPSEC: Contexto saliente completado VPN, SPI 0xDB680406
Manija VPN: 0x0000E9B4
IPSEC: Regla interna saliente completada, SPI 0xDB680406
Regla ID: 0x53F89160
IPSEC: Regla externa saliente completada SPD, SPI 0xDB680406
Regla ID: 0x53E47E88
IPSEC: Nueva regla entrante del flujo del túnel, SPI 0x1698CAC7
Addr del src: 192.168.2.0
Máscara del src: 255.255.255.0
Addr del dst: 192.168.1.0
Máscara del dst: 255.255.255.0
Puertos del src
Parte superior: 0
Baje: 0

Los SPI se asignan a los datos SA.

De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 1
Protocolo del uso: verdad
SPI: 0x00000000
Uso SPI: falso
IPSEC: Regla entrante completada del flujo del túnel, SPI 0x1698CAC7
Regla ID: 0x53FC3E80
IPSEC: Nueva regla entrante del decrypt, SPI 0x1698CAC7
Addr del src: 10.0.0.2
Máscara del src: 255.255.255.255
Addr del dst: 10.0.0.1
Máscara del dst: 255.255.255.255
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 50
Protocolo del uso: verdad
SPI: 0x1698CAC7
Uso SPI: verdad
IPSEC: Regla entrante completada del decrypt, SPI 0x1698CAC7
Regla ID: 0x53FC3F18
IPSEC: Nueva regla entrante del permiso, SPI 0x1698CAC7
Addr del src: 10.0.0.2
Máscara del src: 255.255.255.255
Addr del dst: 10.0.0.1
Máscara del dst: 255.255.255.255
Puertos del src
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Puertos del dst
Parte superior: 0
Baje: 0
De Op. Sys.: ignore
Protocolo: 50
Protocolo del uso: verdad
SPI: 0x1698CAC7
Uso SPI: verdad
IPSEC: Regla entrante completada del permiso, SPI 0x1698CAC7
Regla ID: 0x53F8AEA8
DEBUG [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, jarra: KEY_UPDATE recibido, spi 0x1698cac7
DEBUG [IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, comenzando el P2 reintroducen el temporizador: 3060 segundos.

El IPSec del comienzo reintroduce las épocas.

[IKEv1]: El grupo = 10.0.0.2, IP= 10.0.0.2, la FASE 2 COMPLETARON (msgid=52481cf5)

Fase 2 completa. El respondedor y el iniciador pueden cifrar/tráfico del decrypt.

Verificación del túnel

Note: Puesto que el ICMP se utiliza para accionar el túnel, sólo un IPSec SA está para arriba.

Protocolo 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
```

Información Relacionada

- Un lugar bueno a comenzar es artículo del wikipedia sobre el IPSec. El estándar y las referencias contiene mucha información útil
- Troubleshooting de IPSec: Entendiendo y con los comandos debug
- **Soporte Técnico y Documentación - Cisco Systems**