Depuración de IPsec e IKE de ASA (modo principal IKEv1) Solución de problemas TechNote

Contenido

Introducción

Este documento describe las depuraciones en Adaptive Security Appliance (ASA) cuando se utilizan el modo principal y la clave previamente compartida (PSK). También se trata la traducción de ciertas líneas de debug en la configuración.

Los temas no tratados en este documento incluyen el tráfico de paso después de que se haya establecido el túnel y los conceptos básicos de IPsec o Intercambio de claves de Internet (IKE).

Prerequisites

Requirements

Quienes lean este documento deben tener conocimiento de los siguientes 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 ejecutan Cisco IOS® 12.4T

Problema principal

Las depuraciones IKE e IPsec son a veces crípticas, pero puede usarlas para comprender dónde se encuentra un problema de establecimiento de túnel VPN IPSec.

Situación

El modo principal se utiliza normalmente entre los túneles de LAN a LAN o, en el caso del acceso remoto (EzVPN), cuando se utilizan certificados para la autenticación.

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

Se describen dos escenarios principales:

- ASA como iniciador de IKE
- ASA como respondedor de IKE

Comandos Debug Utilizados

debug crypto ikev1 127

debug crypto ipsec 127

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 de 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
Comienza el intercambio de modo principal; no se ha compartido ninguna política y los pares todavía están en MM_NO_STATE. Como iniciador, el ASA comienza a construir la carga útil.	[DEPURACIÓN IKEv1]: Pitcher: recibió un mensaje de adquisición de clave, spi 0x0 IPSEC(crypto_map_check)-3: Buscando mapa criptográfico que coincida con 5 tuplas: Prot=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3: Verificando el MAPA de mapa criptográfico 10: coincidente. [IKEv1]: IP = 10.0.0.2, iniciador IKE: Nueva fase 1, Intf interior, IKE par 10.0.0.2 dirección de proxy local 192.168.1.0, dirección de proxy remoto 192.168.2.0, mapa criptográfico (MAP) [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil	
Construcción MM1 Este proceso esincluye ipropuesta inicial para IKE y sproveedores de NAT-T compatibles.	**ISAKMP SA** [IKEv1 DEBUG]: IP = 10.0.0.2, construyendo la carga útil NAT-Traversal VID ver 02 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil de NAT-Traversal VID ver 03 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la VID NAT-Traversal sobre la carga útil RFC [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construcción de VID de fragmentación + carga útil de capacidades extendidas	
Enviar MM1.	[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=0) con cargas útiles: HDR + SA (1) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + NINGUNA (0) longitud total: 168	
	==========>	
	[IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=0) con cargas útiles: HDR + SA (1) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + NINGUNA (0) longitud total: 164	MM1 recibido del iniciador.
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de carga útil SA	Proceso MM1.
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, la propuesta de Oakley es aceptable	Comienza la
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID	comparación de las
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, RFC VID de NAT-Traversal recibido	políticas ISAKMP/IKE.
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID	El par remoto anuncia
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID	que puede utilizar
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, NAT-Traversal recibida por VID de 03	NAT-T. Configuración
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID	relacionada:
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, NAT-Traversal recibida por 02 VID	*política crypto isakmp*

		10 *authentication pre-share* *encryption 3des* *hash sha* *grupo 2* *lifetime 86400*
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de carga útil SA IKE	Construir MM2. En este mensaje, el respondedor selecciona la configuración de política isakmp que se utilizará. También anuncia las versiones NAT-T que puede utilizar.
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, propuesta IKE SA nº 1, transformación # 1 aceptable coincide con la entrada IKE global nº 2	
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil SA ISAKMP	
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil NAT-Traversal VID ver 02	
	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, construcción de VID de fragmentación + carga útil de capacidades extendidas	
	[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=0) con cargas útiles: HDR + SA (1) + PROVEEDOR (13) + PROVEEDOR (13) + NONE(0) longitud total: 128	Enviar MM2.
	<==	
MM2 recibido del respondedor.	[IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=0) con cargas útiles: HDR + SA (1) + PROVEEDOR (13) + NONE (0) longitud total: 104	
Proceso MM2.	[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de carga útil SA [DEPURACIÓN IKEv1]: IP = 10.0.0.2, la propuesta de Oakley es aceptable [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, RFC VID de NAT-Traversal recibido	
Construir MM3. Este proceso esinclusionescargas útiles de detección de NAT, Difícil-Carga útil de Hellman (DH) Key Exchange (KE) (iel nitator incluye g, p y A al respondedor), y Compatibilidad con DPD.	30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo carga útil de ke 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo carga útil nonce 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil VID de Cisco Unity 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil VID de xauth V6 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, Enviar VID de IOS 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, Construcción de carga útil de ID de proveedor del IOS de simulación de ASA (versión: 1.0.0, capacidades: 20000001) 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo carga útil VID 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, Enviar Altiga/Cisco VPN3000/Cisco ASA GW VID 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil NAT-Discovery 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, hash de descubrimiento de NAT informático 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil NAT-Discovery 30 de noviembre 10:38:29 [DEPURACIÓN IKEv1]: IP = 10.0.0.2, hash de descubrimiento de NAT informático	
Enviar MM3.	[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=0) con cargas útiles: HDR + KE (4) + NONCE (10) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) longitud total: 304	
	== =========>	
	[IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=0) con cargas útiles: HDR + KE (4) + NONCE (10) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) longitud total : 284	MM3 recibido del iniciador.

[DEPURACIÓN IKEv1]: IP = 10.0.0.2, carga útil de ke de procesamiento [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de carga útil ISA_KE [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de carga útil única [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, VID DPD recibido [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, Procesando carga útil de ID de proveedor IOS/PIX (versión: 1.0.0, capacidades: 00000f6f) [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, xauth V6 recibido VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil NAT-Discovery [DEPURACIÓN IKEv1]: IP = 10.0.0.2, hash de descubrimiento de NAT informático [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil NAT-Discovery [DEPURACIÓN IKEv1]: IP = 10.0.0.2, hash de descubrimiento de NAT informático	Proceso MM3. El respondedor de cargas útiles de NAT-D puede determinar si el el iniciador está detrás de NAT y si el el respondedor está detrás de NAT. Desde el DH KE, el respondedor de carga recibe valores de p, g y A.
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga ke [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo carga útil nonce [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil VID de Cisco Unity [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil xauth V6 VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, Enviar VID de IOS [DEPURACIÓN IKEv1]: IP = 10.0.0.2, Construcción de carga útil de ID de proveedor del IOS de simulación de ASA (versión: 1.0.0, capacidades: 20000001) [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo carga útil VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, Enviar Altiga/Cisco VPN3000/Cisco ASA GW VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil NAT-Discovery [DEPURACIÓN IKEv1]: IP = 10.0.0.2, hash de descubrimiento de NAT informático [DEPURACIÓN IKEv1]: IP = 10.0.0.2, construyendo la carga útil NAT-Discovery [DEPURACIÓN IKEv1]: IP = 10.0.0.2, hash de descubrimiento de NAT informático	Construir MM4. Este proceso esinclusiones carga útil de detección de NAT, DH KE rel respondedor genera "B" y "s" (devuelve "B" al iniciador), y VID de DPD.
[IKEv1]: IP = 10.0.0.2, la conexión aterrizó en tunnel_group 10.0.0.2 [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Generando claves para Respondedor..	El par se asocia con el grupo de túnel L2L 10.0.0.2 y las claves de cifrado y hash se generan a partir de las "s" anteriores y la clave previamente compartida.
[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=0) con cargas útiles: HDR + KE (4) + NONCE (10) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) longitud total: 304 <========== [IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=0) con cargas útiles: HDR + KE (4) + NONCE (10) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + PROVEEDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) longitud total: 304	Enviar MM4. MM4 recibido del respondedor.
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento como carga útil [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de carga útil ISA_KE [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de carga útil única [DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID [DEPURACIÓN IKEv1]: IP = 10.0.0.2, VID de cliente de Cisco Unity recibido	Proceso MM4. Desde las cargas útiles de NAT-D, el iniciador ahora puede determinar si el El indicador está detrás de NAT y si el el

respondedor está detrás de NAT.

[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, VID DPD recibido
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, Procesando carga útil de ID de proveedor IOS/PIX (versión: 1.0.0, capacidades: 00000f7f)
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil VID
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, xauth V6 recibido VID

Desde el DH KE,el iniciador recibe "B" y ahora puede generar "s".

[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil NAT-Discovery
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, hash de descubrimiento de NAT informático
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, procesamiento de la carga útil NAT-Discovery
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, hash de descubrimiento de NAT informático

El par se asocia con el grupo de túnel L2L 10.0.0.2 y el iniciador genera claves de cifrado y hash usando las "s" anteriores y la clave previamente compartida.

[IKEv1]: IP = 10.0.0.2, la conexión aterrizó en tunnel_group 10.0.0.2
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Generando claves para el iniciador...

Construir MM5.
Configuración relacionada:
auto de identidad crypto isakmp

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo carga útil de ID
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo carga útil de troceo
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, hash informático para ISAKMP
[DEPURACIÓN IKEv1]: IP = 10.0.0.2, Construcción de carga útil de mantenimiento del IOS: propotion=32767/32767 sec.
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo la carga útil dpd vid

Enviar MM5.

[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=0) con cargas útiles: HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +PROVEEDOR (13) + NONE (0) longitud total: 96

==========>

Responder no está detrás de ninguna NAT. No se requiere NAT-T.

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Estado de detección NAT automática: El extremo remoto NO está detrás de un dispositivo NAT Este extremo NO está detrás de un dispositivo NAT

[IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=0) con cargas útiles: HDR + ID (5) + HASH (8) + NONE (0) longitud total : 64

MM5 recibido del iniciador.
Este proceso esincluye rIdentidad de peer remoto (ID) y cConexión que aterriza en un grupo de túnel determinado.

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de ID de procesamiento
[IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID recibido 10.0.0.2
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de troceo de procesamiento
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, hash informático para ISAKMP
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de notificación de procesamiento
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2,NAT automática
[IKEv1]: IP = 10.0.0.2, la conexión aterrizó en tunnel_group 10.0.0.2

Proceso MM5.
La autenticación con claves previamente compartidas comienza ahora.
La autenticación ocurre en ambos peers; por lo tanto, verá dos conjuntos de procesos de autenticación correspondientes.
Configuración relacionada:

			tunnel group 10.0.0.2 type ipsec-l2l
		Estado de detección: El extremo remoto NO está detrás de un dispositivo NAT Este extremo NO está detrás de un dispositivo NAT	No Se requiere NAT-T en este caso.
		[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo carga útil de ID [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo carga útil de troceo [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, hash informático para ISAKMP [DEPURACIÓN IKEv1]: IP = 10.0.0.2, Construcción de carga útil de mantenimiento del IOS: propotion=32767/32767 sec. [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo la carga útil dpd vid	Construir MM6. Enviar identidad incluye los tiempos de reinicio y la identidad enviada al par remoto.
		[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=0) con cargas útiles: HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +PROVEEDOR (13) + NONE (0) longitud total: 96 <==========	Enviar MM6.
			Fase 1 completa. Inicie el temporizador isakmp rekey. Configuración relacionada: política crypto isakmp 10 authentication pre-share encryption 3des hash sha grupo 2 lifetime 86400 ciscoasa# sh run all crypto isakmp auto de identidad crypto isakmp
MM6 recibido del respondedor.	[IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=0) con cargas útiles: HDR + ID (5) + HASH (8) + NONE (0) longitud total : 64	[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, FASE 1 COMPLETADA [IKEv1]: IP = 10.0.0.2, tipo de señal de mantenimiento para esta conexión: DPD [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Temporizador de reinicio P1: 64800 segundos.	
Proceso MM6. Este proceso esincluye ridentidad remota enviada desde peer y fdecisión final con respecto al grupo de túnel que se debe elegir.	[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de ID de procesamiento [IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID recibido 10.0.0.2 [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de troceo de procesamiento [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, hash informático para ISAKMP [IKEv1]: IP = 10.0.0.2, la conexión aterrizó en tunnel_group 10.0.0.2 [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, modo rápido de inicio de Oakley [IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2, Iniciador IKE que inicia QM: msg id = 7b80c2b0		
Fase 1 completa. Inicie el temporizador de nueva clave ISAKMP. Relacionado cconfiguración: tunnel group 10.0.0.2 type ipsec-l2l tunnel group 10.0.0.2 ipsec-atributos 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 de señal de mantenimiento para esta conexión: DPD La DPD ha sido negociada y la fase 1 ha concluido. [DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Temporizador de reinicio P1: 82080 segundos.		
Comienza la fase 2 (modo rápido).	: Nueva SA embrionaria creada a @ 0x53FC3C00, SCB: 0x53F90A00, Dirección: entrantes SPI: 0xFD2D851F		

ID de Sesión: 0x00006000
núm. VPIF: 0x0000003
Tipo de túnel: l2l
Protocolo: esp
Vida útil: 240 segundos

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE obtuvo SPI del motor de claves: SPI = 0xfd2d851f

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, modo rápido de configuración de carro

Construir QM1. Este proceso incluye ID de proxy e IPs políticas. Configuración relacionada: crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo carga útil de troceo en blanco

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo la carga útil IPSec SA

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo la carga útil IPSec nonce

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

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID de proxy de transmisión:
Subred local: 192.168.1.0 máscara 255.255.255.0 Protocolo 1 puerto 0
Subred remota: 192.168.2.0 Máscara 255.255.255.0 Protocolo 1 Puerto 0

Se están enviando la subred local (192.168.1.0/24) y la subred remota esperada (192.168.2.0/24)

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

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo carga de troceo qm

[IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2, Iniciador IKE que envía el primer paquete QM: msg id = 7b80c2b0

Enviar QM1.

[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=7b80c2b0) con cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFICACIÓN (11) + NONE (0) longitud total: 200

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

[IKEv1 DECODE]: IP = 10.0.0.2, IKE Responder comienza QM: msg id = 52481cf5

QM1 recibido del iniciador. El respondedor inicia la fase 2 (QM).

[IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=52481cf5) con cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) longitud total : 172

Proceso QM1. Este proceso compara los proxies remotos con los selecciona IP aceptables política. Configuración relacionada: crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 crypto map MAP 10 match address VPN

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de troceo de procesamiento

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, procesamiento de carga útil SA

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, procesamiento de carga útil única

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de ID de procesamiento

[IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID recibido—192.168.2.0—255.255.0[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Datos de subred de proxy IP remoto recibido en carga útil de ID: Dirección 192.168.2.0, Máscara 255.255.255.0, Protocolo 1, Puerto 0

Se reciben las subredes remotas y locales (192.168.2.0/24 y 192.168.1.0/24).

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de ID de procesamiento

[IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID recibido: 192.168.1.0—255.255.0

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Datos de subred de proxy IP local recibidos en carga útil de ID: Dirección 192.168.1.0, Máscara 255.255.255.0, Protocolo 1, Puerto 0

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed old sa no encontrado por addr

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Verificación de mapa criptográfico estático, verificación de mapa = MAP, seq = 10...

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Verificación de mapa criptográfico estático, MAP de mapa, seq = 10 es una coincidencia exitosa

Se busca y se encuentra una entrada de criptografía estática coincidente.

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Peer remoto IKE configurado para mapa criptográfico: MAP

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, procesamiento de la carga útil IPSec SA

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IPSec propuesta SA nº 1, transformación # 1 aceptable coincide con la entrada SA IPSec global # 10

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE: ¡Pidiendo SPI!

: Nueva SA embrionaria creada a @ 0x53FC3698,
SCB: 0x53FC2998,
Dirección: entrantes
SPI: 0x1698CAC7
ID de Sesión: 0x00004000
núm. VPIF: 0x0000003
Tipo de túnel: l2l
Protocolo: esp
Vida útil: 240 segundos

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE obtuvo SPI del motor de claves: SPI = 0x1698cac7

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Oakley construyendo modo rápido

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo carga útil de troceo en blanco

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo la carga útil IPSec SA

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo la carga útil IPSec nonce

Construir QM2. Este proceso esincludes cconfirmación de identidades proxy, tipo de túnel y un se realiza la verificación para las ACL crypto duplicadas.

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

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID de proxy de transmisión:
Subred remota: 192.168.2.0 Máscara 255.255.255.0 Protocolo 1 Puerto 0
Subred local: 192.168.1.0 máscara 255.255.255.0 Protocolo 1 puerto 0

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construyendo carga de troceo qm

[IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE Responder enviando 2º paquete QM: msg id = 52481cf5

[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=52481cf5) con cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) longitud total : 172

Enviar QM2.

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

QM2 recibido del respondedor.

[IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=7b80c2b0) con cargas útiles: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFICACIÓN (11) + NONE (0) longitud total: 200

Procesar QM2.
En este proceso, rel extremo remoto envía parámetros y se escoge la fase 2 más corta propuesta.

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de troceo de procesamiento

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, procesamiento de carga útil SA

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, procesamiento de carga útil única

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de ID de procesamiento

[IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2,
ID_IPV4_ADDR_SUBNET ID recibido: 192.168.1.0—255.255.0
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de ID de procesamiento
[IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2,
ID_IPV4_ADDR_SUBNET ID recibido: 192.168.2.0—255.255.0
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de notificación de procesamiento
[IKEv1 DECODE]: El código de vida del respondedor es el siguiente (outb SPI[4]|atributos):
[IKEv1 DECODE]: 0000: DDE50931 80010001 00020004 00000E10
...1.....
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, cambio de fuerza del respondedor de la duración de la renovación de claves IPSec de 28800 a 3600 segundos en función de la respuesta del par, el ASA está cambiando ciertos atributos IPSEC. En este caso, el intervalo de nueva clave
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, cargando todas las SA IPSEC
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Generando clave de modo rápido

Se encontró correspondencia de crypto map "MAP" y la entrada 10 y coincidió con la lista de acceso "VPN".

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, regla de cifrado NP buscar crypto map MAP 10 que coincida con ACL VPN: return cs_id=53f11198; rule=53f11a90

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Generando clave de modo rápido
: Nueva SA embrionaria creada a @ 0x53FC3698,
SCB: 0x53F910F0,
Dirección: saliente
SPI: 0xDDE50931
ID de Sesión: 0x00006000
núm. VPIF: 0x0000003
Tipo de túnel: l2l
Protocolo: esp
Vida útil: 240 segundos
: Actualización de OBSA de host finalizada, SPI 0xDDE50931
: Creación del contexto de VPN saliente, SPI 0xDDE50931
Indicadores: 0x0000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 bytes
VCID: 0x00000000
Entidad par: 0x00000000
SCB: 0x01CF218F
Canal: 0x4C69CB80
: Contexto de VPN saliente completado, SPI 0xDDE50931
Identificador de VPN: 0x000161A4
: Nueva regla de cifrado saliente, SPI 0xDDE50931
Src addr: 192.168.1.0
Máscara Src: 255.255.255.0
Dst addr: 192.168.2.0
Máscara Dst: 255.255.255.0
Puertos Src
Superior: 0
Menor: 0
Op: ignore
Puertos Dst
Superior: 0
Menor: 0
Op: ignore
Protocolo: 1
Usar protocolo: verdadero

El dispositivo ha generado los SPI 0xfd2d851f y 0xdde50931para el tráfico entrante y saliente respectivamente.

SPI: 0x00000000
Utilice SPI: falso
: Regla de cifrado saliente completada, SPI 0xDDE50931
ID de regla: 0x53FC3AD8
: Nueva regla de permiso de salida, SPI 0xDDE50931
Src addr: 10.0.0.1
Máscara Src: 255.255.255.255
Dst addr: 10.0.0.2
Máscara Dst: 255.255.255.255
Puertos Src
Superior: 0
Menor: 0
Op: ignore
Puertos Dst
Superior: 0
Menor: 0
Op: ignore
Protocolo: 50
Usar protocolo: verdadero
SPI: 0xDDE50931
Utilice SPI: verdadero
: Regla de permiso saliente completada, SPI 0xDDE50931
ID de regla: 0x53F91538
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, regla de cifrado NP buscar crypto map MAP 10 que coincida con ACL VPN: return cs_id=53f11198; rule=53f11a90
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Negociación de seguridad completa para el iniciador de grupo de LAN a LAN (10.0.0.2), SPI entrante = 0xfd2d851f, SPI saliente = 0xdde50931
: Actualización de IBSA de host finalizada, SPI 0xFD2D851F
: Creación del contexto de VPN entrante, SPI 0xFD2D851F
Indicadores: 0x0000006
SA: 0x53FC3C00
SPI: 0xFD2D851F
MTU: 0 bytes
VCID: 0x00000000
Entidad par: 0x000161A4
SCB: 0x01CEA8EF
Canal: 0x4C69CB80
: Contexto de VPN entrante completado, SPI 0xFD2D851F
Identificador de VPN: 0x00018BBC
: Actualización del contexto de VPN saliente 0x000161A4, SPI 0xDDE50931
Indicadores: 0x0000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 bytes
VCID: 0x00000000
Entidad par: 0x00018BBC
SCB: 0x01CF218F
Canal: 0x4C69CB80
: Contexto de VPN saliente completado, SPI 0xDDE50931
Identificador de VPN: 0x000161A4
: Regla interna saliente completada, SPI 0xDDE50931
ID de regla: 0x53FC3AD8
: Regla SPD externa saliente completada, SPI 0xDDE50931
ID de regla: 0x53F91538
: Nueva regla de flujo de túnel entrante, SPI 0xFD2D851F
Src addr: 192.168.2.0
Máscara Src: 255.255.255.0
Dst addr: 192.168.1.0
Máscara Dst: 255.255.255.0
Puertos Src
Superior: 0

Construir QM3. Confirmar todos los SPI creados a peer remoto.

Menor: 0
Op: ignore
Puertos Dst
Superior: 0
Menor: 0
Op: ignore
Protocolo: 1
Usar protocolo: verdadero
SPI: 0x00000000
Utilice SPI: falso
: Regla de flujo de túnel entrante completada, SPI 0xFD2D851F
ID de regla: 0x53F91970
: Nueva regla de descifrado entrante, SPI 0xFD2D851F
Src addr: 10.0.0.2
Máscara Src: 255.255.255.255
Dst addr: 10.0.0.1
Máscara Dst: 255.255.255.255
Puertos Src
Superior: 0
Menor: 0
Op: ignore
Puertos Dst
Superior: 0
Menor: 0
Op: ignore
Protocolo: 50
Usar protocolo: verdadero
SPI: 0xFD2D851F
Utilice SPI: verdadero
: Regla de descifrado entrante completada, SPI 0xFD2D851F
ID de regla: 0x53F91A08
: Nueva regla de permiso entrante, SPI 0xFD2D851F
Src addr: 10.0.0.2
Máscara Src: 255.255.255.255
Dst addr: 10.0.0.1
Máscara Dst: 255.255.255.255
Puertos Src
Superior: 0
Menor: 0
Op: ignore
Puertos Dst
Superior: 0
Menor: 0
Op: ignore
Protocolo: 50
Usar protocolo: verdadero
SPI: 0xFD2D851F
Utilice SPI: verdadero
: Regla de permiso entrante completada, SPI 0xFD2D851F
ID de regla: 0x53F91AA0

Enviar QM3.

[IKEv1 DECODE]: Grupo = 10.0.0.2, IP = 10.0.0.2, Iniciador IKE enviando 3er paquete QM: msg id = 7b80c2b0

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

[IKEv1]: IP = 10.0.0.2, mensaje de envío IKE_DECODE (msgid=7b80c2b0) con cargas útiles: HDR + HASH (8) + NONE (0) longitud total :76

[IKEv1]: IP = 10.0.0.2, mensaje RECIBIDO IKE_DECODE (msgid=52481cf5) con cargas útiles: HDR + HASH (8) + NONE (0) longitud total : 52

QM3 recibido del iniciador.

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

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE recibió un mensaje KEY_ADD para SA: SPI = 0xdde50931

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Pitcher: received KEY_UPDATE, spi 0xfd2d851f

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Temporizador de reinicio P2: 3060 segundos.
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, FASE 2 COMPLETADA (msgid=7b80c2b0)

[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carga útil de troceo de procesamiento
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, cargando todas las SA IPSEC
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Generando clave de modo rápido
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, regla de cifrado NP buscar crypto map MAP 10 que coincida con ACL VPN: return cs_id=53f11198; rule=53f11a90
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Generando clave de modo rápido
: Nueva SA embrionaria creada a @ 0x53F18B00,
SCB: 0x53F8A1C0,
Dirección: saliente
SPI: 0xDB680406
ID de Sesión: 0x00004000
núm. VPIF: 0x0000003
Tipo de túnel: l2l
Protocolo: esp
Vida útil: 240 segundos
: Actualización de OBSA de host finalizada, SPI 0xDB680406
: Creación del contexto de VPN saliente, SPI 0xDB680406
Indicadores: 0x0000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 bytes
VCID: 0x00000000
Entidad par: 0x00000000
SCB: 0x005E4849
Canal: 0x4C69CB80
: Contexto de VPN saliente completado, SPI 0xDB680406
Identificador de VPN: 0x0000E9B4
: Nueva regla de cifrado saliente, SPI 0xDB680406
Src addr: 192.168.1.0
Máscara Src: 255.255.255.0
Dst addr: 192.168.2.0
Máscara Dst: 255.255.255.0
Puertos Src
Superior: 0
Menor: 0
Op: ignore
Puertos Dst
Superior: 0
Menor: 0
Op: ignore
Protocolo: 1
Usar protocolo: verdadero
SPI: 0x00000000
Utilice SPI: falso
: Regla de cifrado saliente completada, SPI 0xDB680406
ID de regla: 0x53F89160
: Nueva regla de permiso de salida, SPI 0xDB680406
Src addr: 10.0.0.1
Máscara Src: 255.255.255.255
Dst addr: 10.0.0.2
Máscara Dst: 255.255.255.255
Puertos Src
Superior: 0
Menor: 0
Op: ignore

Procesar QM3.
Se generan claves de cifrado para las SA de datos.
Durante este proceso, Los SPI se configuran para pasar tráfico.

Puertos Dst
Superior: 0
Menor: 0
Op: ignore
Protocolo: 50
Usar protocolo: verdadero
SPI: 0xDB680406
Utilice SPI: verdadero
: Regla de permiso saliente completada, SPI 0xDB680406
ID de regla: 0x53E47E88
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, regla de cifrado
NP buscar crypto map MAP 10 que coincida con ACL VPN: return
cs_id=53f11198; rule=53f11a90
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Negociación de seguridad
completa para el respondedor de grupo de LAN a LAN (10.0.0.2), SPI
entrante = 0x1698cac7, SPI saliente = 0xdb680406
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE recibió un
mensaje KEY_ADD para SA: SPI = 0xdb680406
: Actualización de IBSA de host finalizada, SPI 0x1698CAC7
: Creación del contexto de VPN entrante, SPI 0x1698CAC7
Indicadores: 0x0000006
SA: 0x53FC3698
SPI: 0x1698CAC7
MTU: 0 bytes
VCID: 0x00000000
Entidad par: 0x0000E9B4
SCB: 0x005DAE51
Canal: 0x4C69CB80
: Contexto de VPN entrante completado, SPI 0x1698CAC7
Identificador de VPN: 0x00011A8C
: Actualización del contexto de VPN saliente 0x0000E9B4, SPI
0xDB680406
Indicadores: 0x0000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 bytes
VCID: 0x00000000
Entidad par: 0x00011A8C
SCB: 0x005E4849
Canal: 0x4C69CB80

Los SPI se asignan a las SA de datos.

: Contexto de VPN saliente completado, SPI 0xDB680406
Identificador de VPN: 0x0000E9B4
: Regla interna saliente completada, SPI 0xDB680406
ID de regla: 0x53F89160
: Regla SPD externa saliente completada, SPI 0xDB680406
ID de regla: 0x53E47E88
: Nueva regla de flujo de túnel entrante, SPI 0x1698CAC7
Src addr: 192.168.2.0
Máscara Src: 255.255.255.0
Dst addr: 192.168.1.0
Máscara Dst: 255.255.255.0
Puertos Src
Superior: 0
Menor: 0
Op: ignore
Puertos Dst
Superior: 0
Menor: 0
Op: ignore
Protocolo: 1
Usar protocolo: verdadero
SPI: 0x00000000
Utilice SPI: falso
: Regla de flujo de túnel entrante finalizada, SPI 0x1698CAC7

ID de regla: 0x53FC3E80 : Nueva regla de descifrado entrante, SPI 0x1698CAC7 Src addr: 10.0.0.2 Máscara Src: 255.255.255.255 Dst addr: 10.0.0.1 Máscara Dst: 255.255.255.255 Puertos Src Superior: 0 Menor: 0 Op: ignore Puertos Dst Superior: 0 Menor: 0 Op: ignore Protocolo: 50 Usar protocolo: verdadero SPI: 0x1698CAC7 Utilice SPI: verdadero : Regla de descifrado entrante completada, SPI 0x1698CAC7 ID de regla: 0x53FC3F18 : Nueva regla de permiso entrante, SPI 0x1698CAC7 Src addr: 10.0.0.2 Máscara Src: 255.255.255.255 Dst addr: 10.0.0.1 Máscara Dst: 255.255.255.255 Puertos Src Superior: 0 Menor: 0 Op: ignore Puertos Dst Superior: 0 Menor: 0 Op: ignore Protocolo: 50 Usar protocolo: verdadero SPI: 0x1698CAC7 Utilice SPI: verdadero : Regla de permiso entrante completada, SPI 0x1698CAC7 ID de regla: 0x53F8AEA8	
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Pitcher: KEY_UPDATE recibido, spi 0x1698cac7	
[DEPURACIÓN IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Temporizador de reinicio P2: 3060 segundos.	Comience los tiempos de nueva clave IPsec.
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, FASE 2 COMPLETADA (msgid=52481cf5)	Fase 2 completa. Tanto el respondedor como el iniciador pueden cifrar/descifrar el tráfico.

Verificación del túnel

Nota: Dado que ICMP se utiliza para activar el túnel, sólo una SA IPSec está activa. 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 buen lugar para empezar es artículo de wikipedia sobre IPSec. El estándar y las referencias contienen mucha información útil
- Resolución de problemas de IPsec: Introducción y uso de los comandos debug
- Soporte Técnico y Documentación - Cisco Systems