O IPsec ASA e o IKE debugam (modo principal IKEv1) pesquisar defeitos TechNote

Índice

Introdução

Este documento descreve debuga na ferramenta de segurança adaptável (ASA) quando o modo principal e a chave pré-compartilhada (PSK) são usados. A tradução de determinadas linhas de debugação na configuração também é discutida.

Os assuntos não discutidos neste documento incluem a passagem do tráfego após o túnel foram estabelecidos e conceitos básicos do IPsec ou do Internet Key Exchange (IKE).

Pré-requisitos

Requisitos

Os leitores deste documento devem ter o conhecimento destes assuntos.

- PSK
- IKE

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Cisco ASA 9.3.2
- Roteadores que executa o ® 12.4T do Cisco IOS

Edição de núcleo

O IKE e o IPsec debugam são às vezes enigmáticos, mas você pode usá-lo para compreender

onde um problema do estabelecimento de túnel do IPSec VPN é encontrado.

Cenário

O modo principal é usado tipicamente entre túneis de LAN para LAN ou, no caso do Acesso remoto (EzVPN), quando os Certificados são usados para a autenticação.

Debuga são de dois ASA que executam a versão de software 9.3.2. Os dois dispositivos formarão um túnel de LAN para LAN.

Dois cenários principais são descritos:

- ASA como o iniciador para o IKE
- ASA como o que responde para o IKE

Comandos Debug usados

debug crypto ikev1 127

IPsec 127 do debug crypto

Configuração ASA

Configuração 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
```

Configuração 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
```

Configuração 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
```

Depuração

Descrição de mensagem do iniciador	Debugs	Descrição de mensagem do que responde
A troca do modo principal começa; nenhuma política foi compartilhada, e os pares estão ainda em MM_NO_STATE. Como o iniciador, o ASA começa construir o payload.	[IKEv1 DEBUGAM]: Jarro: recebeu uma chave adquirem a mensagem, o spi 0x0 IPSEC(crypto_map_check)-3: Procurando o crypto map que combina 5-tuple: Prot=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3: Verificando o MAPA 10 do crypto map: combinado. [IKEv1]: IP= 10.0.0.2, iniciador IKE: Fase nova 1, Intf para dentro, endereço de proxy local 192.168.1.0 de 10.0.0.2 do par IKE, endereço de proxy remoto 192.168.2.0, crypto map (MAPA) [IKEv1 DEBUGAM]: O IP= 10.0.0.2, construindo o **payload** [IKEv1 **ISAKMP SA** DEBUGA]: IP= 10.0.0.2, construindo o payload do ver 02 de NAT-Traversal VID [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do ver 03 de NAT-Traversal VID [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do ver RFC de NAT-Traversal VID [IKEv1 DEBUGAM]: O IP= 10.0.0.2, construindo a fragmentação VID + estendeu o payload das capacidades	
Construção MM1 Este processo inclui a proposta inicial para o IKE e vendedores apoiados NAT-T.		
Envie MM1.	[IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=0) com cargas úteis: HDR + SA (1) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NENHUNS (0) comprimentos total: 168 ==========MM1==========>	
	[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=0) com cargas úteis: HDR + SA (1) + VENDEDOR (13) +VENDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NENHUNS (0) comprimentos total: 164	MM1 recebido do iniciador.
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload SA [IKEv1 DEBUGAM]: O IP= 10.0.0.2, proposta de Oakley é aceitável [IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID [IKEv1 DEBUGAM]: IP= 10.0.0.2, NAT-Traversal recebido RFC VID [IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID [IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID [IKEv1 DEBUGAM]: IP= 10.0.0.2, ver recebido 03 VID de NAT-Traversal [IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID [IKEv1 DEBUGAM]: IP= 10.0.0.2, ver recebido 02 VID de NAT-Traversal [IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload IKE SA [IKEv1 DEBUGAM]: O IP= 10.0.0.2, proposta IKE SA # 1, transforma # 1 entrada global dos fósforos aceitáveis IKE # 2	Processo MM1. A comparação de políticas ISAKMP/IKE começa. O peer remoto anuncia que pode usar o NAT-T. Configuração relacionada: *política cripto 10 do isakmp* *Pré-compartilhamento de autenticação* *criptografia 3des* *sha da mistura* *grupo2* *vida 86400*
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload ISAKMP SA [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do ver 02 de NAT-Traversal VID	Construção MM2. Nesta mensagem o que responde

		seleciona que os ajustes da política do isakmp a se usar. Igualmente anuncia as versões que NAT-T pode se usar.
	[IKEv1 DEBUGAM]: O IP= 10.0.0.2, construindo a fragmentação VID + estendeu o payload das capacidades	
	[IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=0) com cargas úteis: HDR + SA (1) + VENDEDOR (13) + comprimento total do VENDEDOR (13) + NONE(0): 128	Envie MM2.
	<==========MM2==========	
MM2 recebido do que responde.	[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=0) com cargas úteis: HDR + SA (1) + VENDEDOR (13) + NENHUNS (0) comprimentos total: 104	
Processo MM2.	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload SA [IKEv1 DEBUGAM]: O IP= 10.0.0.2, proposta de Oakley é aceitável [IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID [IKEv1 DEBUGAM]: IP= 10.0.0.2, NAT-Traversal recebido RFC VID	
Construção MM3. Cargas úteis desta descoberta do includesNAT do processo, cargas úteis das trocas de chave do Diffie-Hellman (DH) (KE) (o initator inclui g, p, e A ao que responde), e apoio DPD.	30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload KE 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do nonce 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do Cisco Unity VID 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do Xauth V6 VID 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: O IP= 10.0.0.2, envia IO VID 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do Vendor ID da falsificação IO ASA (versão: 1.0.0, capacidades: 20000001) 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload VID 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: O IP= 10.0.0.2, envia Altiga/Cisco VPN3000/Cisco ASA GW VID 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload da NAT-descoberta 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, mistura de computação da descoberta NAT 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload da NAT-descoberta 30 de novembro 10:38:29 [IKEv1 DEBUGAM]: IP= 10.0.0.2, mistura de computação da descoberta NAT	
Envie MM3.	[IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=0) com cargas úteis: HDR + KE (4) + NONCE (10) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (20) + NAT-D (20) + NENHUNS (0) comprimentos total: 304	
	==========MM3==========>	
	[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=0) com cargas úteis: HDR + KE (4) + NONCE (10) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (130) + NAT-D (130) + NENHUNS (0) comprimentos total: 284	MM3 recebido do iniciador.
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload KE	Processo MM3.
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload ISA_KE	Das cargas úteis NAT-D o que responde pode determinar se o initator é atrás do NAT e se o que responde é atrás do NAT.
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload do nonce	
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID	
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, DPD recebido VID	
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID	
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload do Vendor ID IOS/PIX (versão: 1.0.0, capacidades: 00000f6f)	
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID	Do DH KE, o que responde do payload obtém valores de p, de
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, Xauth recebido V6 VID	
	[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload da NAT-	

descoberta
[IKEv1 DEBUGAM]: IP= 10.0.0.2, mistura de computação da descoberta NAT

g e de A.

[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload da NAT-descoberta
[IKEv1 DEBUGAM]: IP= 10.0.0.2, mistura de computação da descoberta NAT
[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload KE
[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do nonce
[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do Cisco Unity VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do Xauth V6 VID

Construção MM4.
Este processo inclui o payload da descoberta NAT, o que responde DH KE gerencie "B" e "s" (envia para trás "B" ao initator), e DPD VID.

[IKEv1 DEBUGAM]: O IP= 10.0.0.2, envia IO VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload do Vendor ID da falsificação IO ASA (versão: 1.0.0, capacidades: 20000001)
[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload VID
[IKEv1 DEBUGAM]: O IP= 10.0.0.2, envia Altiga/Cisco VPN3000/Cisco ASA GW VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload da NAT-descoberta
[IKEv1 DEBUGAM]: IP= 10.0.0.2, mistura de computação da descoberta NAT
[IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload da NAT-descoberta
[IKEv1 DEBUGAM]: IP= 10.0.0.2, mistura de computação da descoberta NAT

O par é associado com o grupo de túneis de 10.0.0.2 L2L, e a criptografia e as chaves da mistura são geradas do "s" acima e da chave pré-compartilhada.

[IKEv1]: IP= 10.0.0.2, conexão aterrada no tunnel_group 10.0.0.2
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, gerando chaves para o que responde…

Envie MM4.

[IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=0) com cargas úteis: HDR + KE (4) + NONCE (10) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (130) + NAT-D (130) + NENHUNS (0) comprimentos total: 304
<==========MM4==========

MM4 recebido do que responde.

[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=0) com cargas úteis: HDR + KE (4) + NONCE (10) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (20) + NAT-D (20) + NENHUNS (0) comprimentos total: 304
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload do ike
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload ISA_KE
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload do nonce
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, cliente recebido VID do Cisco Unity
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, DPD recebido VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload do Vendor ID IOS/PIX (versão: 1.0.0, capacidades: 00000f7f)
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, Xauth recebido V6 VID
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload da NAT-descoberta
[IKEv1 DEBUGAM]: IP= 10.0.0.2, mistura de computação da descoberta NAT
[IKEv1 DEBUGAM]: IP= 10.0.0.2, processando o payload da NAT-descoberta
[IKEv1 DEBUGAM]: IP= 10.0.0.2, mistura de computação da descoberta

Processo MM4.
Das cargas úteis NAT-D, o initator pode agora determinar se o iniator é atrás do NAT e se o que responde é atrás do NAT.

Do DH KE, o iniciador recebe "B" e pode agora gerar o "S."

	NAT		
O par é associado com o grupo de túneis de 10.0.0.2 L2L, e o initator gerencie chaves da criptografia e da mistura usando “s” acima e a chave pré-compartilhada.	[IKEv1]: IP= 10.0.0.2, conexão aterrada no tunnel_group 10.0.0.2 [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, gerando chaves para o iniciador…		
Construção MM5. Configuração relacionada: automóvel cripto da identidade do isakmp	[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload ID [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload da mistura [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, mistura de computação para o ISAKMP [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload da manutenção de atividade IO: segundo proposal=32767/32767. [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload do vid do dpd		
Envie MM5.	[IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=0) com cargas úteis: HDR + ID (5) + MISTURA (8) + KEEPALIVE IO (128) +VENDOR (13) + NENHUNS (0) comprimentos total: 96 ==========MM5==========>		
O que responde não é atrás de nenhum NAT. Nenhum NAT-T exigido.	[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, estado automático da detecção NAT: A extremidade remota não é atrás de um dispositivo que NAT esta extremidade não é atrás de um dispositivo NAT	[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=0) com cargas úteis: HDR + ID (5) + MISTURA (8) + NENHUNS (0) comprimentos total: 64	MM5 recebido do iniciador. Este processo inclui a identidade do peer remoto (ID) e a aterrissagem da conexão em um grupo do túnel específico.
		[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload do processamento ID [IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR ID recebido 10.0.0.2 [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o payload da mistura [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, mistura de computação para o ISAKMP [IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, processando notificam o payload [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2,Automatic NAT [IKEv1]: IP= 10.0.0.2, conexão aterrada no tunnel_group 10.0.0.2	Processo MM5. A autenticação com chaves pré-compartilhada começa agora. A autenticação ocorre em ambos os pares; consequentemente, você verá dois grupos de processos de autenticação correspondentes. Configuração relacionada: tipo ipsec-l2l de 10.0.0.2 do grupo de túneis
	Estado da detecção: A extremidade remota não é atrás de um dispositivo que NAT esta extremidade não é atrás de um dispositivo NAT		Nenhum NAT-T exigido neste caso.
	[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload ID [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload da mistura [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, mistura de computação para o ISAKMP [IKEv1 DEBUGAM]: IP= 10.0.0.2, construindo o payload da manutenção de atividade IO: segundo proposal=32767/32767. [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o		Construção MM6. Envie a identidade inclui rekey as épocas começadas e a identidade enviada ao peer remoto.

payload do vid do dpd

[IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=0) com cargas úteis: HDR + ID (5) + MISTURA (8) + KEEPALIVE IO (128) +VENDOR (13) + NENHUNS (0) comprimentos total: 96

<==========MM6==========

Envie MM6.

Fase 1 completa.
O isakmp do começo rekey o temporizador.
Configuração relacionada:
política cripto 10 do isakmp
Pré-compartilhamento de autenticação
criptografia 3des
sha da mistura
grupo2
vida 86400
ciscoasa # sh run todo o isakmp cripto
automóvel cripto da identidade do isakmp

[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, FASE 1 TERMINADA

[IKEv1]: IP= 10.0.0.2, tipo da manutenção de atividade para esta conexão: DPD

[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, começando o P1 rekey o temporizador: 64800 segundos.

MM6 recebido do que responde.

[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=0) com cargas úteis: HDR + ID (5) + MISTURA (8) + NENHUNS (0) comprimentos total: 64

Processo MM6.
Este processo inclui a identidade remota enviada do par e da decisão final em relação ao grupo de túneis escolher.

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload do processamento ID
[IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR ID recebido
10.0.0.2
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o payload da mistura
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, mistura de computação para o ISAKMP
[IKEv1]: IP= 10.0.0.2, conexão aterrada no tunnel_group 10.0.0.2
[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, Oakley começam o Quick Mode
[IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, iniciador IKE que começa o QM: msg identificação = 7b80c2b0

Fase 1 completa.
O começo ISAKMP rekey o temporizador.
Configuração relacionada:
tipo ipsec-l2l de 10.0.0.2 do grupo de túneis
IPsec-atributos de 10.0.0.2 do grupo de túneis
chave pré-compartilhada Cisco

[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, FASE 1 TERMINADA
[IKEv1]: IP= 10.0.0.2, tipo da manutenção de atividade para esta conexão: DPD
O DPD tem a abelha negociada e a fase 1 está agora completa.
[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, começando o P1 rekey o temporizador: 82080 segundos.

A fase 2 (Quick Mode) começa.

IPSEC: @ 0x53FC3C00 criado SA embrionário novo,
SCB: 0x53F90A00,
Direção: de entrada
SPI: 0xFD2D851F
ID de sessão: 0x00006000
VPIF numérico: 0x00000003
Tipo de túnel: l2l
Protocolo: esp
Duração: 240 segundos

Construção QM1.
Este processo inclui o proxy ID e as políticas de IPsec.
Configuração

[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, IKE obtiveram o SPI do motor chave: SPI = 0xfd2d851f
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, Quick Mode constucting do oakley
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload

	vazio da mistura [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload IPsec SA [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload do nonce do IPsec [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o ID de proxy [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, identificação transmissora do proxy: Sub-rede local: porta 0 do protocolo 1 de 255.255.255.0 da máscara de 192.168.1.0 Sub-rede remota: Porta 0 do protocolo 1 de 255.255.255.0 da máscara de 192.168.2.0 A sub-rede local (192.168.1.0/24) e a sub-rede remota expcted (192.168.2.0/24) estão sendo enviadas [IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, iniciador IKE que envia o contato inicial [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload da mistura do qm [IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, iniciador IKE que envia o ø pkt QM: msg identificação = 7b80c2b0 [IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=7b80c2b0) com cargas úteis: HDR + a MISTURA (8) + SA (1) + o NONCE (10) + ID (5) + ID (5) + NOTIFICAM (11) + NENHUNS (0) comprimentos total: 200
relacionada: o conjunto de transformação cripto do IPsec TRANSFORMA o esp-sha-hmac ESP-aes a lista de acesso VPN estendeu ICMP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 da licença	==========QM1==========>
	[IKEv1 DESCODIFICAM]: IP= 10.0.0.2, que responde IKE que começa o QM: msg identificação = 52481cf5
	[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=52481cf5) com cargas úteis: HDR + MISTURA (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NENHUNS (0) comprimentos total: 172
	[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o payload da mistura [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o payload SA [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o payload do nonce [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload do processamento ID
	[IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR_SUBNET ID received--192.168.2.0--255.255.255.0[IKEv1]: O grupo = 10.0.0.2, IP= 10.0.0.2, receberam dados da sub-rede do proxy do IP remoto no payload ID: Enderece 192.168.2.0, máscara 255.255.255.0, o protocolo 1, a porta 0 [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload do processamento ID [IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2,
Envie QM1.	QM1 recebido do iniciador. O que responde começa a fase 2 (QM). Processo QM1. Este processo compara proxys remotos com o local e seleciona a política de IPsec aceitável. Configuração relacionada: o conjunto de transformação cripto do IPsec TRANSFORMA o esp-sha-hmac ESP-aes a lista de acesso VPN estendeu ICMP 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 da licença endereço VPN do fósforo do MAPA 10 do crypto map O telecontrole e as sub-redes local (192.168.2.0/24 e 192.168.1.0/24) são recebidos.

ID_IPV4_ADDR_SUBNET ID received--192.168.1.0--255.255.255.0

[IKEv1]: O grupo = 10.0.0.2, IP= 10.0.0.2, receberam dados da sub-rede do proxy do IP local no payload ID: Enderece 192.168.1.0, máscara 255.255.255.0, o protocolo 1, a porta 0

[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, sa velho QM IsRekeyed não encontrado pelo ADDR

[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, verificação do mapa estático de criptografia, verificando o mapa = o MAPA, segs.s = 10…

[IKEv1]: O grupo = 10.0.0.2, IP= 10.0.0.2, verificação do mapa estático de criptografia, MAPA do mapa, segs. = 10 são uma compatibilidade bem sucedida

Uma entrada cripto estática de harmonização é procurada e encontrada.

[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, peer remoto IKE configurado para o crypto map: MAPA

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o payload IPsec SA

[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, proposta IPsec SA # 1, transformam # 1 entrada IPsec SA dos fósforos aceitáveis # 10 globais

[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, IKE: pedindo o SPI!

IPSEC: @ 0x53FC3698 criado SA embrionário novo,
SCB: 0x53FC2998,
Direção: de entrada
SPI: 0x1698CAC7
ID de sessão: 0x00004000
VPIF numérico: 0x00000003
Tipo de túnel: l2l
Protocolo: esp
Duração: 240 segundos

[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, IKE obtiveram o SPI do motor chave: SPI = 0x1698cac7

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, oakley que constrói o Quick Mode

Construção QM2. Este processo inclui a confirmação das identidades de proxy, tipo de túnel, e uma verificação é executada para ACLs cript. espelhados.

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload vazio da mistura

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload IPsec SA

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload do nonce do IPsec

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o ID de proxy

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, identificação transmissora do proxy:
Sub-rede remota: Porta 0 do protocolo 1 de 255.255.255.0 da máscara de 192.168.2.0
Sub-rede local: porta 0 do protocolo 1 de 255.255.255.0 da máscara de 192.168.1.0

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, construindo o payload da mistura do qm

[IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, que responde IKE que envia o ò pkt QM: msg identificação = 52481cf5

[IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=52481cf5) com cargas úteis: HDR + MISTURA (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NENHUNS (0) comprimentos total: 172

Envie QM2.

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

[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=7b80c2b0) com cargas úteis: HDR + a MISTURA (8) + SA (1) + o NONCE (10) + ID (5) + ID (5) + NOTIFICAM (11) + NENHUNS (0) comprimentos total: 200

QM2 recebido do que responde.

Processo QM2. Neste processo, a extremidade remota envia parâmetros e as vidas propostas as

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o payload da mistura

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o payload SA

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o

	payload do nonce [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload do processamento ID [IKEv1 DESCODIFICAM]: 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 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, payload do processamento ID [IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, ID_IPV4_ADDR_SUBNET ID received--192.168.2.0--255.255.255.0 [IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, processando notificam o payload
mais curtos da fase 2 são escolhidas.	[IKEv1 DESCODIFICAM]: O que responde que a vida descodifica segue (outb SPI[4]|attributes): [IKEv1 DESCODIFICAM]: 0000: DDE50931 80010001 00020004 00000E10… 1 ..... [IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, que responde que força a mudança do IPsec que rekeying a duração de 28800 a 3600 segundos baseado na resposta do par, o ASA está mudando determinados atributos do IPSEC. Neste caso o intervalo do rekey [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, carregando todo o sas de IPSec [IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, gerando a chave do Quick Mode!
Crypto map de harmonização “MAPA” Found e entrada 10 e combinado lhe contra a lista de acesso “VPN.”	[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, NP cifram a regra olham acima para o MAPA 10 do crypto map que combina ACL VPN: cs_id=53f11198 retornado; rule=53f11a90
O dispositivo gerou o tráfego de entrada e de saída 0xfd2d851f e 0xdde50931for SPI respectivamente.	[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, gerando a chave do Quick Mode! IPSEC: @ 0x53FC3698 criado SA embrionário novo, SCB: 0x53F910F0, Direção: saída SPI: 0xDDE50931 ID de sessão: 0x00006000 VPIF numérico: 0x00000003 Tipo de túnel: l2l Protocolo: esp Duração: 240 segundos IPSEC: Atualização terminada do host OBSA, SPI 0xDDE50931 IPSEC: Criando o contexto de partida VPN, SPI 0xDDE50931 Bandeiras: 0x00000005 SA: 0x53FC3698 SPI: 0xDDE50931 MTU: 1500 bytes VCID: 0x00000000 Correspondente: 0x00000000 SCB: 0x01CF218F Canal: 0x4C69CB80 IPSEC: Contexto de partida terminado VPN, SPI 0xDDE50931 Punho VPN: 0x000161A4 IPSEC: De partida novos cifram a regra, SPI 0xDDE50931 ADDR de Src: 192.168.1.0 Máscara de Src: 255.255.255.0 ADDR de Dst: 192.168.2.0 Máscara de Dst: 255.255.255.0 Portas de Src Parte superior: 0 Abaixe: 0 Op: ignore Portas de Dst Parte superior: 0

Abaixe: 0
Op: ignore
Protocolo: 1
Protocolo do uso: verdadeiro
SPI: 0x00000000
Uso SPI: falso
IPSEC: De partida terminados cifram a regra, SPI 0xDDE50931
Regra ID: 0x53FC3AD8
IPSEC: Regra de partida nova da licença, SPI 0xDDE50931
ADDR de Src: 10.0.0.1
Máscara de Src: 255.255.255.255
ADDR de Dst: 10.0.0.2
Máscara de Dst: 255.255.255.255
Portas de Src
Parte superior: 0
Abaixe: 0
Op: ignore
Portas de Dst
Parte superior: 0
Abaixe: 0
Op: ignore
Protocolo: 50
Protocolo do uso: verdadeiro
SPI: 0xDDE50931
Uso SPI: verdadeiro
IPSEC: Regra de partida terminada da licença, SPI 0xDDE50931
Regra ID: 0x53F91538
[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, NP cifram a regra olham acima para o MAPA 10 do crypto map que combina ACL VPN: cs_id=53f11198 retornado; rule=53f11a90
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, negociação de segurança completa para o iniciador do grupo do LAN para LAN (10.0.0.2), de entrada SPI = 0xfd2d851f, de partida SPI = 0xdde50931
IPSEC: Atualização terminada do host IBSA, SPI 0xFD2D851F
IPSEC: Criando o contexto de entrada VPN, SPI 0xFD2D851F
Bandeiras: 0x00000006
SA: 0x53FC3C00
SPI: 0xFD2D851F
MTU: bytes 0
VCID: 0x00000000
Correspondente: 0x000161A4
SCB: 0x01CEA8EF
Canal: 0x4C69CB80
IPSEC: Contexto de entrada terminado VPN, SPI 0xFD2D851F
Punho VPN: 0x00018BBC
IPSEC: Atualizando o contexto de partida 0x000161A4 VPN, SPI 0xDDE50931
Bandeiras: 0x00000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 bytes
VCID: 0x00000000
Correspondente: 0x00018BBC
SCB: 0x01CF218F
Canal: 0x4C69CB80
IPSEC: Contexto de partida terminado VPN, SPI 0xDDE50931
Punho VPN: 0x000161A4
IPSEC: Regra interna de partida terminada, SPI 0xDDE50931
Regra ID: 0x53FC3AD8
IPSEC: Regra exterior de partida terminada SPD, SPI 0xDDE50931
Regra ID: 0x53F91538
IPSEC: Regra de entrada nova do fluxo do túnel, SPI 0xFD2D851F
ADDR de Src: 192.168.2.0
Máscara de Src: 255.255.255.0

Construção QM3. Confirme todos os SPI criados ao peer remoto.

	ADDR de Dst: 192.168.1.0 Máscara de Dst: 255.255.255.0 Portas de Src Parte superior: 0 Abaixe: 0 Op: ignore Portas de Dst Parte superior: 0 Abaixe: 0 Op: ignore Protocolo: 1 Protocolo do uso: verdadeiro SPI: 0x00000000 Uso SPI: falso IPSEC: Regra de entrada terminada do fluxo do túnel, SPI 0xFD2D851F Regra ID: 0x53F91970 IPSEC: Regra de entrada nova do decrypt, SPI 0xFD2D851F ADDR de Src: 10.0.0.2 Máscara de Src: 255.255.255.255 ADDR de Dst: 10.0.0.1 Máscara de Dst: 255.255.255.255 Portas de Src Parte superior: 0 Abaixe: 0 Op: ignore Portas de Dst Parte superior: 0 Abaixe: 0 Op: ignore Protocolo: 50 Protocolo do uso: verdadeiro SPI: 0xFD2D851F Uso SPI: verdadeiro IPSEC: Regra de entrada terminada do decrypt, SPI 0xFD2D851F Regra ID: 0x53F91A08 IPSEC: Regra de entrada nova da licença, SPI 0xFD2D851F ADDR de Src: 10.0.0.2 Máscara de Src: 255.255.255.255 ADDR de Dst: 10.0.0.1 Máscara de Dst: 255.255.255.255 Portas de Src Parte superior: 0 Abaixe: 0 Op: ignore Portas de Dst Parte superior: 0 Abaixe: 0 Op: ignore Protocolo: 50 Protocolo do uso: verdadeiro SPI: 0xFD2D851F Uso SPI: verdadeiro IPSEC: Regra de entrada terminada da licença, SPI 0xFD2D851F Regra ID: 0x53F91AA0	
Envie QM3.	[IKEv1 DESCODIFICAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, iniciador IKE que envia o ó pkt QM: msg identificação = 7b80c2b0 ==========QM3==========>	
Fase 2 completa. O iniciador está agora pronto para cifrar e decifrar pacotes usando estes valores SPI.	[IKEv1]: IP= 10.0.0.2, IKE_DECODE que ENVIA a mensagem (msgid=7b80c2b0) com cargas úteis: HDR + MISTURA (8) + NENHUNS (0) comprimentos total: 76 [IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, IKE obtiveram um msg KEY_ADD para o SA: SPI = 0xdde50931	[IKEv1]: O IP= 10.0.0.2, IKE_DECODE RECEBEU a mensagem (msgid=52481cf5) Iniciador do fom do receivd QM3.

[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, com cargas úteis:
jarro: KEY_UPDATE recebido, spi 0xfd2d851f HDR +
[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, MISTURA (8) +
começando o P2 rekey o temporizador: 3060 segundos. NENHUNS (0)
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, FASE 2 comprimentos
TERMINADA (msgid=7b80c2b0) total: 52
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, processando o
payload da mistura
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, carregando todo o
sas de IPSec
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, gerando a chave do
Quick Mode!
[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, NP cifram a regra
olham acima para o MAPA 10 do crypto map que combina ACL VPN:
cs_id=53f11198 retornado; rule=53f11a90
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, gerando a chave do
Quick Mode!
IPSEC: @ 0x53F18B00 criado SA embrionário novo,
SCB: 0x53F8A1C0,
Direção: saída
SPI: 0xDB680406
ID de sessão: 0x00004000
VPIF numérico: 0x00000003
Tipo de túnel: l2l
Protocolo: esp
Duração: 240 segundos
IPSEC: Atualização terminada do host OBSA, SPI 0xDB680406
IPSEC: Criando o contexto de partida VPN, SPI 0xDB680406
Bandeiras: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 bytes Processo QM3.
VCID: 0x00000000 As chaves de
Correspondente: 0x00000000 criptografia são
SCB: 0x005E4849 geradas para os dados
Canal: 0x4C69CB80 SA.
IPSEC: Contexto de partida terminado VPN, SPI 0xDB680406 Durante este processo,
Punho VPN: 0x0000E9B4 Os SPI são ajustados a
IPSEC: De partida novos cifram a regra, SPI 0xDB680406 fim passar o tráfego.
ADDR de Src: 192.168.1.0
Máscara de Src: 255.255.255.0
ADDR de Dst: 192.168.2.0
Máscara de Dst: 255.255.255.0
Portas de Src
Parte superior: 0
Abaixe: 0
Op: ignore
Portas de Dst
Parte superior: 0
Abaixe: 0
Op: ignore
Protocolo: 1
Protocolo do uso: verdadeiro
SPI: 0x00000000
Uso SPI: falso
IPSEC: De partida terminados cifram a regra, SPI 0xDB680406
Regra ID: 0x53F89160
IPSEC: Regra de partida nova da licença, SPI 0xDB680406
ADDR de Src: 10.0.0.1
Máscara de Src: 255.255.255.255
ADDR de Dst: 10.0.0.2
Máscara de Dst: 255.255.255.255
Portas de Src
Parte superior: 0

Abaixe: 0
Op: ignore
Portas de Dst
Parte superior: 0
Abaixe: 0
Op: ignore
Protocolo: 50
Protocolo do uso: verdadeiro
SPI: 0xDB680406
Uso SPI: verdadeiro
IPSEC: Regra de partida terminada da licença, SPI 0xDB680406
Regra ID: 0x53E47E88
[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, NP cifram a regra olham acima para o MAPA 10 do crypto map que combina ACL VPN: cs_id=53f11198 retornado; rule=53f11a90
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, negociação de segurança completa para o que responde do grupo do LAN para LAN (10.0.0.2), de entrada SPI = 0x1698cac7, de partida SPI = 0xdb680406
[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, IKE obtiveram um msg KEY_ADD para o SA: SPI = 0xdb680406
IPSEC: Atualização terminada do host IBSA, SPI 0x1698CAC7
IPSEC: Criando o contexto de entrada VPN, SPI 0x1698CAC7
Bandeiras: 0x00000006
SA: 0x53FC3698
SPI: 0x1698CAC7
MTU: bytes 0
VCID: 0x00000000
Correspondente: 0x0000E9B4
SCB: 0x005DAE51
Canal: 0x4C69CB80
IPSEC: Contexto de entrada terminado VPN, SPI 0x1698CAC7
Punho VPN: 0x00011A8C
IPSEC: Atualizando o contexto de partida 0x0000E9B4 VPN, SPI 0xDB680406
Bandeiras: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 bytes
VCID: 0x00000000
Correspondente: 0x00011A8C
SCB: 0x005E4849
Canal: 0x4C69CB80
IPSEC: Contexto de partida terminado VPN, SPI 0xDB680406
Punho VPN: 0x0000E9B4
IPSEC: Regra interna de partida terminada, SPI 0xDB680406
Regra ID: 0x53F89160
IPSEC: Regra exterior de partida terminada SPD, SPI 0xDB680406
Regra ID: 0x53E47E88
IPSEC: Regra de entrada nova do fluxo do túnel, SPI 0x1698CAC7
ADDR de Src: 192.168.2.0
Máscara de Src: 255.255.255.0
ADDR de Dst: 192.168.1.0
Máscara de Dst: 255.255.255.0
Portas de Src
Parte superior: 0
Abaixe: 0
Op: ignore
Portas de Dst
Parte superior: 0
Abaixe: 0
Op: ignore
Protocolo: 1
Protocolo do uso: verdadeiro
SPI: 0x00000000

Os SPI são atribuídos aos dados SA.

Uso SPI: falso IPSEC: Regra de entrada terminada do fluxo do túnel, SPI 0x1698CAC7 Regra ID: 0x53FC3E80 IPSEC: Regra de entrada nova do decrypt, SPI 0x1698CAC7 ADDR de Src: 10.0.0.2 Máscara de Src: 255.255.255.255 ADDR de Dst: 10.0.0.1 Máscara de Dst: 255.255.255.255 Portas de Src Parte superior: 0 Abaixe: 0 Op: ignore Portas de Dst Parte superior: 0 Abaixe: 0 Op: ignore Protocolo: 50 Protocolo do uso: verdadeiro SPI: 0x1698CAC7 Uso SPI: verdadeiro IPSEC: Regra de entrada terminada do decrypt, SPI 0x1698CAC7 Regra ID: 0x53FC3F18 IPSEC: Regra de entrada nova da licença, SPI 0x1698CAC7 ADDR de Src: 10.0.0.2 Máscara de Src: 255.255.255.255 ADDR de Dst: 10.0.0.1 Máscara de Dst: 255.255.255.255 Portas de Src Parte superior: 0 Abaixe: 0 Op: ignore Portas de Dst Parte superior: 0 Abaixe: 0 Op: ignore Protocolo: 50 Protocolo do uso: verdadeiro SPI: 0x1698CAC7 Uso SPI: verdadeiro IPSEC: Regra de entrada terminada da licença, SPI 0x1698CAC7 Regra ID: 0x53F8AEA8	
[IKEv1 DEBUGAM]: Grupo = 10.0.0.2, IP= 10.0.0.2, jarro: KEY_UPDATE recebido, spi 0x1698cac7	
[IKEv1 DEBUGAM]: O grupo = 10.0.0.2, IP= 10.0.0.2, começando o P2 rekey o temporizador: 3060 segundos.	O IPsec do começo rekey épocas.
[IKEv1]: Grupo = 10.0.0.2, IP= 10.0.0.2, FASE 2 TERMINADA (msgid=52481cf5)	Fase 2 completa. O que responde e o iniciador podem cifrar/tráfego do decrypt.

Verificação do túnel

Nota: Desde que o ICMP é usado para provocar o túnel, simplesmente um IPsec SA está acima. 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
```

Informações Relacionadas

- Um bom lugar a começar é artigo do wikipedia no IPsec. O padrão e as referências contêm muita informação util
- Troubleshooting de IPSec: Compreendendo e usando comandos debug
- **Suporte Técnico e Documentação - Cisco Systems**