Nota técnica de solução de problemas de depurações de ASA IPsec e IKE (modo principal IKEv1)

Contents

Introduction

Este documento descreve as depurações no Adaptive Security Appliance (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 tópicos não discutidos neste documento incluem tráfego de passagem após o túnel ter sido estabelecido e conceitos básicos de IPsec ou Internet Key Exchange (IKE).

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos.

- PSK
- IKE

Componentes Utilizados

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

- Cisco ASA 9.3.2
- Roteadores que executam o Cisco IOS® 12.4T

Problema principal

Às vezes, as depurações de IKE e IPsec são criptografadas, mas você pode usá-las para entender onde um problema de estabelecimento de túnel IPsec VPN está localizado.

Cenário

O modo principal é normalmente usado entre túneis LAN a LAN ou, no caso de acesso remoto (EzVPN), quando os certificados são usados para autenticação.

As depurações são de dois ASAs 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 iniciador de IKE
- ASA como respondente para IKE

Comandos de depuração usados

debug crypto ikev1 127

debug crypto ipsec 127

Configuração do ASA

Configuração de 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 do 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 da mensagem do iniciador	Debugs	Descrição da mensagem do respondedor
Início da troca do modo principal; nenhuma política foi compartilhada e os correspondentes estão ainda em MM_NO_STATE.	[DEPURAÇÃO IKEv1]: Argumento: recebeu uma mensagem de aquisição de chave, spi 0x0 IPSEC(crypto_map_check)-3: Procurando um mapa de criptografia correspondente a 5 tuplas: Prot=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3: Verificando o mapa de criptografia MAP 10: correspondente.	
Como iniciador, o ASA começa a construir o payload.	[IKEv1]: IP = 10.0.0.2, Iniciador IKE: Nova Fase 1, Intf inside, IKE Peer 10.0.0.2 Endereço Proxy local 192.168.1.0, Endereço Proxy remoto 192.168.2.0, Mapa de Criptografia (MAP) [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o **payload SA ISAKMP** [DEBUG IKEv1]: IP = 10.0.0.2, construindo o NAT-Traversal VID ver 02 payload	
Construir MM1 Este processoinclui iProposta inicial para IKE e sfornecedores de NAT-T suportados.	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o NAT-Traversal VID ver 03 payload [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o payload de RFC de VID de passagem de NAT [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo VID de fragmentação + payload de recursos estendidos	
Enviar MM1.	[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=0) com payloads : HDR + SA (1) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + NENHUM (0) comprimento total: 168	
	==========MM1==========>	
	[IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=0) com payloads : HDR + SA (1) + FORNECEDOR (13) +FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + NENHUM (0) comprimento total: 164	MM1 recebido do iniciador.
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando o payload SA	Processo MM1.
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, a proposta Oakley é aceitável	A comparação das
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID	políticas
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, NAT-Traversal RFC VID recebido	ISAKMP/IKE é
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID	iniciada.
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID	O peer remoto anuncia
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, NAT-Traversal ver 03 VID recebido	que pode usar NAT-T.
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID	Configuração
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, NAT-Traversal ver 02 VID recebido	relacionada:
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando o payload SA do IKE	*crypto isakmp policy*
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, IKE SA Proposta nº 1,	*10*

	Transformação nº 1 aceita corresponde à entrada global IKE nº 2	*Pré-compartilhamento de autenticação* *criptografia 3des* *hash sha* *grupo 2* *duração 86400*
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o payload SA de ISAKMP [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o NAT-Traversal VID ver 02 payload [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo VID de fragmentação + payload de recursos estendidos	Construir MM2. Nesta mensagem, o respondente seleciona quais configurações de política isakmp usar. Ele também anuncia as versões NAT-T que pode usar.
	[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=0) com payloads : HDR + SA (1) + FORNECEDOR (13) + FORNECEDOR (13) + NONE(0) comprimento total : 128	Envie MM2.
	<==========	
MM2 recebido do respondente.	[IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=0) com payloads : HDR + SA (1) + FORNECEDOR (13) + NENHUM (0) comprimento total : 104	
Processo MM2.	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando o payload SA [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, a proposta Oakley é aceitável [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, NAT-Traversal RFC VID recebido	
Construa MM3. Este processoncludespayloads de descoberta de NAT, Diffie- Cargas úteis do Exchange de chave (KE) Hellman (DH) (i)o nitator inclui g, p e A para o respondedor), e Suporte DPD.	30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, construindo o payload de ke 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, construindo payload nonce 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, construindo o payload do VID do Cisco Unity 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, construindo o payload V6 VID 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, Enviar VID do IOS 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, Construindo o payload de ID de fornecedor do IOS para spoofing do ASA (versão: 1.0.0, recursos: 20000001) 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, construindo o payload VID 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, Enviar Altiga/Cisco VPN3000/Cisco ASA GW VID 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, construindo o payload NAT-Discovery 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, computação de hash de descoberta de NAT 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, construindo o payload NAT-Discovery 30 de novembro 10:38:29 [DEBUG IKEv1]: IP = 10.0.0.2, computação de hash de descoberta de NAT	
Enviar MM3.	[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=0) com payloads : HDR + KE (4) + NONCE (10) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) comprimento total : 304	
	==========MM3==========>	
	[IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=0) com payloads : HDR + KE (4) + NONCE (10) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) comprimento total : 284	MM3 recebido do iniciador.
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload ke	Processo MM3.
	[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload ISA_KE [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando nonce payload	Do respondedor de cargas úteis do NAT-

[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, DPD VID recebido [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, Processando payload de ID de fornecedor do IOS/PIX (versão: 1.0.0, recursos: 00000f6f) [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, xauth V6 VID recebido [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando a carga útil NAT-Discovery [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, computação de hash de descoberta de NAT [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando a carga útil NAT-Discovery [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, computação de hash de descoberta de NAT [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo payload ke [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo payload nonce [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o payload do VID do Cisco Unity [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo xauth V6 VID payload [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, Enviar VID do IOS [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, Construindo o payload de ID de fornecedor do IOS para spoofing do ASA (versão: 1.0.0, recursos: 20000001) [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, Enviar Altiga/Cisco VPN3000/Cisco ASA GW VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o payload NAT-Discovery [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, computação de hash de descoberta de NAT [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, construindo o payload NAT-Discovery [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, computação de hash de descoberta de NAT	D é capaz de determinar se o o iniciador está por trás do NAT e se o o respondente está por trás do NAT. Do DH KE, o respondente da carga útil obtém valores de p, g e A. Construa MM4. Este processoncludes carga útil de descoberta de NAT, DH KE ro respondedor gera "B" e "s" (envia "B" de volta para o iniciador), e DPD VID.
[IKEv1]: IP = 10.0.0.2, Conexão aterrisada em tunnel_group 10.0.0.2 [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Gerando chaves para o Respondedor...	O peer está associado ao grupo de túnel L2L 10.0.0.2 e as chaves de criptografia e hash são geradas dos "s" acima e da chave pré-compartilhada.
[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=0) com payloads : HDR + KE (4) + NONCE (10) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) comprimento total: 304 <========== =======	Enviar MM4.
[IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=0) com payloads : HDR + KE (4) + NONCE (10) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) comprimento total : 304	MM4 recebido do respondente.
[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando como payload [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload ISA_KE [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando nonce payload [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, VID do cliente Cisco Unity recebido [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, DPD VID recebido [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, Processando payload de ID de fornecedor do IOS/PIX (versão: 1.0.0, recursos: 00000f7f) [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando payload VID [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, xauth V6 VID recebido	Processar MM4. Nas cargas úteis do NAT-D, o iniciador agora pode determinar se o o iniciador está atrás do NAT e se o o respondente está por trás do NAT. Do DH KE, eu...O iniciador recebe "B" e agora pode gerar "s".

[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando a carga útil NAT-Discovery
[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, computação de hash de descoberta de NAT
[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, processando a carga útil NAT-Discovery
[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, computação de hash de descoberta de NAT

O peer está associado ao grupo de túnel L2L 10.0.0.2 e o iniciador gera chaves de criptografia e de hash usando "s" acima e a chave pré-compartilhada.

[IKEv1]: IP = 10.0.0.2, Conexão aterrisada em tunnel_group 10.0.0.2
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Gerando chaves para o iniciador...

Construa o MM5. Configuração relacionada:
crypto isakmp identity auto

[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo payload de ID
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo o payload de hash
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Hash de computação para ISAKMP
[DEPURAÇÃO IKEv1]: IP = 10.0.0.2, Construindo o payload de manutenção de atividade do IOS: proposta=32767/32767 seg.
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo o payload dpd vid

Enviar MM5.

[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=0) com payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +FORNECEDOR (13) + NENHUM (0) comprimento total : 96
==========MM5==========>

O respondedor não está por trás de nenhum NAT. Não é necessário NAT-T.

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Status de detecção automática de NAT: A extremidade remota NÃO está atrás de um dispositivo NAT. Essa extremidade NÃO está atrás de um dispositivo NAT

[IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=0) com payloads : HDR + ID (5) + HASH (8) + NONE (0) comprimento total : 64

MM5 recebido do iniciador. Este processoinclui rRemote peer identity (ID) e cdestino da conexão em um grupo de túneis específico.

[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, payload de ID de processamento
[DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID recebida 10.0.0.2
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processamento de payload de hash
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Hash de computação para ISAKMP
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processando payload de notificação
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2,NAT automático
[IKEv1]: IP = 10.0.0.2, Conexão aterrisada em tunnel_group 10.0.0.2

Processar MM5.
A autenticação com chaves pré-compartilhadas começa agora.
A autenticação ocorre em ambos os pares; portanto, você verá dois conjuntos de processos de autenticação correspondentes.
Configuração relacionada:
tunnel group 10.0.0.2 type ipsec-l2l

Status da detecção: A extremidade remota NÃO está atrás de um dispositivo NAT. Essa extremidade NÃO está atrás de um dispositivo NAT

No NAT-T necessário neste caso.

[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo

Construa o MM6.

		payload de ID [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo o payload de hash [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Hash de computação para ISAKMP [DEPURAÇÃO IKEv1]: IP = 10.0.0.2, Construindo o payload de manutenção de atividade do IOS: proposta=32767/32767 seg. [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo o payload dpd vid	Enviar identidade inclui tempos de rechaveamento iniciados e identidade enviada ao peer remoto.
		[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=0) com payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +FORNECEDOR (13) + NENHUM (0) comprimento total : 96 <==========	Envie MM6.
			Fase 1 concluída. Inicie o temporizador de rechave isakmp. Configuração relacionada: crypto isakmp policy 10 Pré-compartilhamento de autenticação criptografia 3des hash sha grupo 2 duração 86400 ciscoasa# sh run all crypto isakmp crypto isakmp identity auto
MM6 recebido do respondente.	[IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=0) com payloads : HDR + ID (5) + HASH (8) + NONE (0) comprimento total : 64	[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, FASE 1 CONCLUÍDA [IKEv1]: IP = 10.0.0.2, tipo Keep-alive para esta conexão: DPD [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, iniciando o temporizador de chave P1: 64800 segundos.	
Processar MM6. Este processoinclui ridentidade remota enviada de peer e fdecisão final sobre o grupo de túneis a escolher.	[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, payload de ID de processamento [DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID recebida 10.0.0.2 [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processamento de payload de hash [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Hash de computação para ISAKMP [IKEv1]: IP = 10.0.0.2, Conexão aterrisada em tunnel_group 10.0.0.2 [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, início rápido de Oakley [DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Iniciador IKE iniciando QM: msg id = 7b80c2b0		
Fase 1 concluída. Inicie o temporizador de rechaveamento ISAKMP. Relacionado cConfiguração: tunnel group 10.0.0.2 type ipsec-l2l tunnel group 10.0.0.2 ipsec-attribute chave pré-compartilhada da cisco	[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, FASE 1 CONCLUÍDA [IKEv1]: IP = 10.0.0.2, tipo Keep-alive para esta conexão: DPD DPD foi negociado e a fase 1 está completa. [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, iniciando o temporizador de chave P1: 82080 segundos.		
A fase 2 (modo rápido) é iniciada.	IPSEC: Nova SA embrionária criada a 0x53FC3C00, SCB: 0x53F90A00, Direção: entrada SPI: 0xFD2D851F ID da sessão: 0x00006000 VPIF num : 0x00000003 Tipo de túnel: l2l		

	Protocolo: esp Duração: 240 segundos
	[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE obteve SPI do mecanismo de chave: SPI = 0xfd2d851f
	[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, oakley construindo modo rápido
Construir QM1. Esse processo inclui IDs de proxy e IPs políticas. Configuração relacionada: crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac licença estendida de VPN de lista de acesso icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0	[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo payload de hash em branco [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo o payload IPSec SA [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo payload IPSec nonce [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo ID de proxy [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Transmitindo ID do Proxy: Sub-rede local: 192.168.1.0 máscara 255.255.255.0 Protocolo 1 Porta 0 Sub-rede remota: 192.168.2.0 Máscara 255.255.255.0 Protocolo 1 Porta 0 A sub-rede local (192.168.1.0/24) e a sub-rede remota esperada (192.168.2.0/24) estão sendo enviadas [DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Iniciador IKE enviando contato inicial [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo o payload de hash qm [DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Iniciador IKE enviando o primeiro pacote QM: msg id = 7b80c2b0
Enviar QM1.	[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=7b80c2b0) com payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFICAÇÃO (11) + NENHUM (0) comprimento total : 200 ========== ===>
	[DECODE IKEv1]: IP = 10.0.0.2, IKE Responder iniciando QM: msg id = 52481cf5 [IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=52481cf5) com payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) comprimento total : 172
Processar QM1. Este processo compara proxies remotos com seleciona IP aceitáveis política. Configuração relacionada: crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac licença estendida de VPN de lista de acesso icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 crypto map MAP 10 match address VPN	[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processamento de payload de hash [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processando o payload SA [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processando nonce payload [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, payload de ID de processamento
As sub-redes remotas e locais (192.168.2.0/24 e 192.168.1.0/24) são recebidas.	[DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID recebido—192.168.2.0—255.255.255.0[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Dados da sub-rede do proxy IP remoto recebidos no payload do ID: Endereço 192.168.2.0, Máscara 255.255.255.0, Protocolo 1, Porta 0 [DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, payload de ID de processamento [DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID recebido—192.168.1.0—255.255.255.0
QM1 recebido do iniciador. O respondedor inicia a fase 2 (QM).	

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Dados da sub-rede do Proxy IP local recebido no payload do ID: Endereço 192.168.1.0, Máscara 255.255.255.0, Protocolo 1, Porta 0
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed old sa não encontrado por addr
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, verificação de mapa de criptografia estático, mapa de verificação = MAP, seq = 10...
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, verificação de mapa de criptografia estático, MAP de mapa, seq = 10 é uma correspondência bem-sucedida

Uma entrada de criptografia estática correspondente é procurada e encontrada.

[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Peer Remoto IKE configurado para mapa de criptografia: MAPA
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processando o payload IPSec SA
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IPSec SA Proposta nº 1, Transformação nº 1 aceitável corresponde à entrada SA IPSec global nº 10
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE: solicitando SPI!
IPSEC: Nova SA embrionária criada em 0x53FC3698,
SCB: 0x53FC2998,
Direção: entrada
SPI: 0x1698CAC7
ID da sessão: 0x00004000
VPIF num : 0x00000003
Tipo de túnel: l2l
Protocolo: esp
Duração: 240 segundos
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE obteve SPI do mecanismo de chave: SPI = 0x1698cac7
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Oakley construindo modo rápido

Construa o QM2. Este processoinclui cconfirmação de identidades de proxy, tipo de túnel e uma é realizada uma verificação para ACLs de criptografia espelhada.

[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo payload de hash em branco
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo o payload IPSec SA
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo payload IPSec nonce
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo ID de proxy
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Transmitindo ID do Proxy:
Sub-rede remota: 192.168.2.0 Máscara 255.255.255.0 Protocolo 1 Porta 0
Sub-rede local: 192.168.1.0 máscara 255.255.255.0 Protocolo 1 Porta 0
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, construindo o payload de hash qm
[DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Respondedor IKE enviando o segundo pacote QM: id da msg = 52481cf5
[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=52481cf5) com payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) comprimento total : 172

Enviar QM2.

<==========
=======

QM2 recebido do respondente.

[IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=7b80c2b0) com payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFICAÇÃO (11) + NENHUM (0) comprimento total : 200
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processamento de payload de hash
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processando o payload SA

Processar QM2. Nesse processo, ro final remoto envia parâmetros e a fase 2 de vida proposta mais curta é escolhida.

[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processando nonce payload
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, payload de ID de processamento

[DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2,
ID_IPV4_ADDR_SUBNET ID recebido—192.168.1.0—255.255.255.0
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, payload de ID de processamento
[DECODE IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2,
ID_IPV4_ADDR_SUBNET ID recebido—192.168.2.0—255.255.255.0
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processando payload de notificação
[DECODE IKEv1]: Decodificação da vida útil do respondedor a seguir (saída SPI[4]|atributos):
[DECODE IKEv1]: 0000 : DDE50931 80010001 00020004 00000E10
...1.....
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Respondente forçando a alteração da duração de rechaveamento de IPSec de 28800 para 3600 segundos
com base na resposta do peer, o ASA está alterando determinados atributos IPSEC. Nesse caso, o intervalo de rechaveamento
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carregando todas as SAs IPSEC
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, gerando chave de modo rápido!

Foi encontrado um mapa de criptografia correspondente "MAP" e a entrada 10 e correspondeu-o à lista de acesso "VPN".

[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, pesquisa de regra de criptografia NP para MAP 10 de mapa de criptografia correspondente à ACL VPN: retornado cs_id=53f11198; rule=53f11a90

[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, gerando chave de modo rápido!
IPSEC: Nova SA embrionária criada em 0x53FC3698,
SCB: 0x53F910F0,
Direção: saída
SPI: 0xDDE50931
ID da sessão: 0x00006000
VPIF num : 0x00000003
Tipo de túnel: l2l
Protocolo: esp
Duração: 240 segundos
IPSEC: Atualização de OBSA do host concluída, SPI 0xDDE50931
IPSEC: Criando contexto de VPN de saída, SPI 0xDDE50931
Flags: 0x00000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 bytes
VCID: 0x00000000

O dispositivo gerou os SPIs 0xfd2d851f e 0xdde50931para tráfego de entrada e saída respectivamente.

Correspondente: 0x00000000
SCB: 0x01CF218F
Canal: 0x4C69CB80
IPSEC: Contexto VPN de saída concluído, SPI 0xDDE50931
Identificador de VPN: 0x000161A4
IPSEC: Nova regra de criptografia de saída, 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
Portas Src
Superior: 0
Inferior: 0
Op: ignore
Portas Dst
Superior: 0
Inferior: 0
Op: ignore
Protocolo: 1
Usar protocolo: verdadeiro

SPI: 0x00000000
Usar SPI: falso
IPSEC: Regra de criptografia de saída concluída, SPI 0xDDE50931
ID da regra: 0x53FC3AD8
IPSEC: Nova regra de permissão de saída, 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
Portas Src
Superior: 0
Inferior: 0
Op: ignore
Portas Dst
Superior: 0
Inferior: 0
Op: ignore
Protocolo: 50
Usar protocolo: verdadeiro
SPI: 0xDDE50931
Usar SPI: verdadeiro
IPSEC: Regra de permissão de saída concluída, SPI 0xDDE50931
ID da regra: 0x53F91538
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, pesquisa de regra de criptografia NP para MAP 10 de mapa de criptografia correspondente à ACL VPN: retornado cs_id=53f11198; rule=53f11a90
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, negociação de segurança concluída para o iniciador de grupo LAN para LAN (10.0.0.2), SPI de entrada = 0xfd2d851f, SPI de saída = 0xdde50931
IPSEC: Atualização IBSA do host concluída, SPI 0xFD2D851F
IPSEC: Criando contexto de VPN de entrada, SPI 0xFD2D851F
Flags: 0x00000006
SA: 0x53FC3C00
SPI: 0xFD2D851F
MTU: 0 bytes
VCID: 0x00000000
Correspondente: 0x000161A4
SCB: 0x01CEA8EF
Canal: 0x4C69CB80
IPSEC: Contexto VPN de entrada concluído, SPI 0xFD2D851F
Identificador de VPN: 0x00018BBC
IPSEC: Atualização do contexto de VPN de saída 0x000161A4, SPI 0xDDE50931
Flags: 0x00000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 bytes
VCID: 0x00000000
Correspondente: 0x00018BBC
SCB: 0x01CF218F
Canal: 0x4C69CB80
IPSEC: Contexto VPN de saída concluído, SPI 0xDDE50931
Identificador de VPN: 0x000161A4
IPSEC: Regra interna de saída concluída, SPI 0xDDE50931
ID da regra: 0x53FC3AD8
IPSEC: Regra SPD externa de saída concluída, SPI 0xDDE50931
ID da regra: 0x53F91538
IPSEC: Nova regra de fluxo de túnel de entrada, 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
Portas Src
Superior: 0

Construa o QM3. Confirmar todos os SPIs criados para o peer remoto.

Inferior: 0
Op: ignore
Portas Dst
Superior: 0
Inferior: 0
Op: ignore
Protocolo: 1
Usar protocolo: verdadeiro
SPI: 0x00000000
Usar SPI: falso
IPSEC: Regra de fluxo de túnel de entrada concluída, SPI 0xFD2D851F
ID da regra: 0x53F91970
IPSEC: Nova regra de descriptografia de entrada, 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
Portas Src
Superior: 0
Inferior: 0
Op: ignore
Portas Dst
Superior: 0
Inferior: 0
Op: ignore
Protocolo: 50
Usar protocolo: verdadeiro
SPI: 0xFD2D851F
Usar SPI: verdadeiro
IPSEC: Regra de descriptografia de entrada concluída, SPI 0xFD2D851F
ID da regra: 0x53F91A08
IPSEC: Nova regra de permissão de entrada, 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
Portas Src
Superior: 0
Inferior: 0
Op: ignore
Portas Dst
Superior: 0
Inferior: 0
Op: ignore
Protocolo: 50
Usar protocolo: verdadeiro
SPI: 0xFD2D851F
Usar SPI: verdadeiro
IPSEC: Regra de permissão de entrada concluída, SPI 0xFD2D851F
ID da regra: 0x53F91AA0

Enviar QM3.

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

==========

[IKEv1]: IP = 10.0.0.2, mensagem de envio IKE_DECODE (msgid=7b80c2b0) com payloads : HDR + HASH (8) + NONE (0) comprimento total: 76

Fase 2 concluída. O iniciador agora está pronto para criptografar e descriptografar pacotes usando esses valores SPI.

[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE recebeu uma mensagem KEY_ADD para SA: SPI = 0xdde50931
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Pitcher: KEY_UPDATE recebido, spi 0xfd2d851f
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2,

[IKEv1]: IP = 10.0.0.2, Mensagem RECEBIDA IKE_DECODE (msgid=52481cf5) com payloads : HDR + HASH (8) + NONE (0)

QM3 recebido do iniciador.

iniciando o temporizador de rechave P2: 3060 segundos.
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, FASE 2 CONCLUÍDA (msgid=7b80c2b0)
comprimento total : 52
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, processamento de payload de hash
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, carregando todas as SAs IPSEC
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, gerando chave de modo rápido!
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, pesquisa de regra de criptografia NP para MAP 10 de mapa de criptografia correspondente à ACL VPN: retornado cs_id=53f11198; rule=53f11a90
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, gerando chave de modo rápido!
IPSEC: Nova SA embrionária criada a 0x53F18B00,
SCB: 0x53F8A1C0,
Direção: saída
SPI: 0xDB680406
ID da sessão: 0x00004000
VPIF num : 0x00000003
Tipo de túnel: l2l
Protocolo: esp
Duração: 240 segundos
IPSEC: Atualização de OBSA do host concluída, SPI 0xDB680406
IPSEC: Criando contexto de VPN de saída, SPI 0xDB680406
Flags: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 bytes
VCID: 0x00000000
Correspondente: 0x00000000
SCB: 0x005E4849
Canal: 0x4C69CB80
IPSEC: Contexto VPN de saída concluído, SPI 0xDB680406
Identificador de VPN: 0x0000E9B4
IPSEC: Nova regra de criptografia de saída, 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
Portas Src
Superior: 0
Inferior: 0
Op: ignore
Portas Dst
Superior: 0
Inferior: 0
Op: ignore
Protocolo: 1
Usar protocolo: verdadeiro
SPI: 0x00000000
Usar SPI: falso
IPSEC: Regra de criptografia de saída concluída, SPI 0xDB680406
ID da regra: 0x53F89160
IPSEC: Nova regra de permissão de saída, 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
Portas Src
Superior: 0
Inferior: 0
Op: ignore
Portas Dst

Processar QM3.
As chaves de criptografia são geradas para SAs de dados.
Durante esse processo, Os SPIs são definidos para passar o tráfego.

Superior: 0
Inferior: 0
Op: ignore
Protocolo: 50
Usar protocolo: verdadeiro
SPI: 0xDB680406
Usar SPI: verdadeiro
IPSEC: Regra de permissão de saída concluída, SPI 0xDB680406
ID da regra: 0x53E47E88
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, pesquisa de regra de criptografia NP para MAP 10 de mapa de criptografia correspondente à ACL VPN: retornado cs_id=53f11198; rule=53f11a90
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, negociação de segurança concluída para o respondedor de grupo LAN para LAN (10.0.0.2), SPI de entrada = 0x1698cac7, SPI de saída = 0xdb680406
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, IKE recebeu uma mensagem KEY_ADD para SA: SPI = 0xdb680406
IPSEC: Atualização IBSA do host concluída, SPI 0x1698CAC7
IPSEC: Criando contexto de VPN de entrada, SPI 0x1698CAC7
Flags: 0x00000006
SA: 0x53FC3698
SPI: 0x1698CAC7
MTU: 0 bytes
VCID: 0x00000000
Correspondente: 0x0000E9B4
SCB: 0x005DAE51
Canal: 0x4C69CB80
IPSEC: Contexto VPN de entrada concluído, SPI 0x1698CAC7
Identificador de VPN: 0x00011A8C
IPSEC: Atualização do contexto de VPN de saída 0x0000E9B4, SPI 0xDB680406
Flags: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 bytes
VCID: 0x00000000
Correspondente: 0x00011A8C
SCB: 0x005E4849
Canal: 0x4C69CB80
IPSEC: Contexto VPN de saída concluído, SPI 0xDB680406
Identificador de VPN: 0x0000E9B4
IPSEC: Regra interna de saída concluída, SPI 0xDB680406
ID da regra: 0x53F89160
IPSEC: Regra SPD externa de saída concluída, SPI 0xDB680406
ID da regra: 0x53E47E88
IPSEC: Nova regra de fluxo de túnel de entrada, 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
Portas Src
Superior: 0
Inferior: 0
Op: ignore
Portas Dst
Superior: 0
Inferior: 0
Op: ignore
Protocolo: 1
Usar protocolo: verdadeiro
SPI: 0x00000000
Usar SPI: falso
IPSEC: Regra de fluxo de túnel de entrada concluída, SPI 0x1698CAC7
ID da regra: 0x53FC3E80

Os SPIs são atribuídos aos SAs de dados.

IPSEC: Nova regra de descriptografia de entrada, 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 Portas Src Superior: 0 Inferior: 0 Op: ignore Portas Dst Superior: 0 Inferior: 0 Op: ignore Protocolo: 50 Usar protocolo: verdadeiro SPI: 0x1698CAC7 Usar SPI: verdadeiro	
IPSEC: Regra de descriptografia de entrada concluída, SPI 0x1698CAC7 ID da regra: 0x53FC3F18	
IPSEC: Nova regra de permissão de entrada, 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 Portas Src Superior: 0 Inferior: 0 Op: ignore Portas Dst Superior: 0 Inferior: 0 Op: ignore Protocolo: 50 Usar protocolo: verdadeiro SPI: 0x1698CAC7 Usar SPI: verdadeiro	
IPSEC: Regra de permissão de entrada concluída, SPI 0x1698CAC7 ID da regra: 0x53F8AEA8	
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, Pitcher: KEY_UPDATE recebido, spi 0x1698cac7	
[DEPURAÇÃO IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, iniciando o temporizador de rechave P2: 3060 segundos.	Iniciar tempos de rechave IPsec.
[IKEv1]: Grupo = 10.0.0.2, IP = 10.0.0.2, FASE 2 CONCLUÍDA (msgid=52481cf5)	Fase 2 concluída. Tanto o respondedor quanto o iniciador podem criptografar/descriptografar o tráfego.

Verificação de túnel

Note: Como o ICMP é usado para disparar o túnel, apenas uma SA IPSec está ativa. 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 para começar é artigo da wikipedia sobre IPSec. O padrão e as referências contêm muitas informações úteis
- Solução de problemas de IPsec: Entendendo e usando comandos debug
- Suporte Técnico e Documentação - Cisco Systems