Solucionar problemas de depuração do IOS IKEv2 para VPN site a site com PSKs

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Informações de Apoio](#)
[Problema principal](#)
[Configuração do roteador](#)
[Troubleshoot](#)
[Depurações de roteador](#)
[Depurações CHILD_SA](#)
[Verificação de túnel](#)
[ISAKMP](#)
[IPsec](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve as depurações do Internet Key Exchange versão 2 (IKEv2) no Cisco IOS® quando uma chave não compartilhada (PSK) é usada.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento da troca de pacotes para IKEv2. Para obter mais informações, consulte Intercâmbio de Pacotes IKEv2 e Depuração no Nível de Protocolo.

Componentes Utilizados

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

- Internet Key Exchange versão 2 (IKEv2)
- Cisco IOS 15.1(1)T ou posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Este documento fornece informações sobre como traduzir determinadas linhas de depuração em uma configuração.

Problema principal

A troca de pacotes em IKEv2 é radicalmente diferente da troca de pacotes em IKEv1. No IKEv1 houve uma troca de fase1 claramente demarcada que consistia em seis (6) pacotes com uma troca de fase 2 depois que consistia em três (3) pacotes; a troca de IKEv2 é variável. Para obter mais informações sobre as diferenças e uma explicação da troca de pacotes, consulte Intercâmbio de Pacotes IKEv2 e Depuração no Nível de Protocolo.

Configuração do roteador

Esta seção lista as configurações usadas neste documento.

Roteador 1

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy site-pol
 proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
 peer peer1
  address 10.0.0.2 255.255.255.0
  hostname host1
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
```

```
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

Roteador 2

```
crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 keyring KEYRNG
 peer peer2
  address 10.0.0.1 255.255.255.0
  hostname host2
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.102 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

Troubleshoot

Depurações de roteador

Estes comandos de depuração são usados neste documento:

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Descrição da Mensagem do Roteador 1 (Iniciador)	Debugs	Descrição da Mensagem do Roteador 2 (Respondente)
O roteador 1 recebe um pacote que corresponde à ACL criptografada para o ASA 10.0.0.2 correspondente. Inicia a criação de SA	*11 de novembro 20:28:34.003: IKEv2: Um pacote foi recebido do despachante *11 de novembro 20:28:34.003: IKEv2:Processando um item fora da fila de pacotes *Nov 11 19:30:34.811: IKEv2:% Obtendo chave pré-compartilhada pelo endereço 10.0.0.2 *11 de novembro 19:30:34.811: IKEv2:Adicionando proposta PHASE1-prop para o estilo de política do kit de ferramentas *11 de novembro 19:30:34.811: IKEv2:(1): Escolhendo o perfil IKE IKEV2-SETUP *11 de novembro 19:30:34.811: IKEv2:Nova solicitação ikev2 sa admitida *11 de novembro 19:30:34.811: IKEv2:Incrementando negociação de saída como contagem em um	
O primeiro par de mensagens é a troca IKE_SA_INIT. Essas mensagens negociam algoritmos criptográficos, trocam momentos e fazem uma troca Diffie-Hellman. **Configuração relevante:** `proposta crypto ikev2 PHASE1-prop encryption 3des aes-cbc-128 integrity sha1 group 2crypto ikev2 keyring KEYRNG peer1 address 10.0.0.2 255.255.255.0`	*11 de novembro 19:30:34.811: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: IDLE Evento: EV_INIT_SA *11 de novembro 19:30:34.811: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_GET_IKE_POLICY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento:**EV_SET_POLICY** *11 de novembro, 19:30:34.811: IKEv2:(SA ID = 1):Definindo políticas configuradas *11 de novembro 19:30:34.811: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_CHK_AUTH4PKI *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento:**EV_GEN_DH_KEY** *11 de novembro 19:30:34.811: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B	

`hostname host1` `pre-shared-key local cisco pre-shared-key remote cisco`	R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_NO_EVENT *11 de novembro 19:30:34.811: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_OK_RED_DH_PUBKEY_RESP *11 de novembro 19:30:34.811: IKEv2:(ID da AS = 1):Ação: Action_Null *11 de novembro 19:30:34.811: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_GET_CONFIG_MODE *11 de novembro 19:30:34.811: IKEv2:IKEv2 iniciador - nenhum dado de configuração para enviar no exch IKE_SA_INIT *11 de novembro, 19:30:34.811: IKEv2:Sem dados de configuração para enviar ao kit de ferramentas: *11 de novembro 19:30:34.811: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_BLD_MSG *11 de novembro, 19:30:34.811: IKEv2: Criar carga específica do fornecedor: DELETE-REASON *11 de novembro, 19:30:34.811: IKEv2: Criar carga específica do fornecedor: (PERSONALIZADO) *11 de novembro 19:30:34.811: IKEv2:Criar Carga de Notificação: NAT_DETECTION_SOURCE_IP *11 de novembro 19:30:34.811: IKEv2:Criar Carga de Notificação: NAT_DETECTION_DESTINATION_IP	
Iniciador criando pacote IKE_INIT_SA. Ele contém: Cabeçalho ISAKMP (SPI/versão/flags), SAi1 (algoritmo criptográfico suportado pelo iniciador IKE), KEi (valor de chave pública DH do iniciador) e N (Iniciador Nonce).	*11 de novembro 19:30:34.811: **IKEv2:(SA ID = 1)**:Próxima carga: SA, versão: 2.0 Tipo de troca: **IKE_SA_INIT,** sinalizadores: **INITIATOR** ID da mensagem: 0, comprimento: 344 Conteúdo da carga: **SA** Próxima carga: KE, reservado: 0x0, comprimento: 56 última proposta: 0x0, reservado: 0x0, comprimento: 52 Proposta: 1, ID do protocolo: IKE, tamanho SPI: 0, #trans: 5 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 1, reservado: 0x0, id: 3DES última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **KE** Próxima carga: N, reservado: 0x0, comprimento: 136 Grupo DH: 2, Reservado: 0x0 N Próxima carga: VID, reservado: 0x0, comprimento: 24 VID Próxima carga: VID, reservado: 0x0, comprimento: 23 Próxima carga útil de VID: NOTIFY, reservado: 0x0, comprimento: 21	

	NOTIFY(NAT_DETECTION_SOURCE_IP) Próxima carga: NOTIFY, reservado: 0x0, comprimento: 28 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Próxima carga: NONE, reservado: 0x0, comprimento: 28 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_DESTINATION_IP	
----------Iniciador enviou IKE_INIT_SA ---------->		
	*11 de novembro 19:30:34.814: IKEv2: Um pacote foi recebido do despachante *11 de novembro 19:30:34.814: IKEv2:Processando um item fora da fila de pacotes *11 de novembro 19:30:34.814: IKEv2:Nova solicitação ikev2 sa admitida *11 de novembro 19:30:34.814: IKEv2:Incrementando a negociação de entrada como contagem em um	O respondente recebe IKE_INIT_SA.
	*11 de novembro 19:30:34.814: IKEv2:Próxima carga: SA, versão: 2.0 Tipo de troca: IKE_SA_INIT, sinalizadores: INITIATOR ID da mensagem: 0, comprimento: 344 Conteúdo da carga: Próximo payload de SA: KE, reservado: 0x0, comprimento: 56 última proposta: 0x0, reservado: 0x0, comprimento: 52 Proposta: 1, ID do protocolo: IKE, tamanho SPI: 0, #trans: 5 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 1, reservado: 0x0, id: 3DES última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 Próxima carga útil de KE: N, reservada: 0x0, comprimento: 136 Grupo DH: 2, Reservado: 0x0 N Próxima carga: VID, reservado: 0x0, comprimento: 24 *11 de novembro 19:30:34.814: IKEv2:Analisar Carga Específica do Fornecedor: CISCO-DELETE-REASON VID Próxima carga: VID, reservado: 0x0, comprimento: 23 *11 de novembro 19:30:34.814: IKEv2:Analisar Carga Específica do Fornecedor: (PERSONALIZADO) VID Próxima carga: NOTIFY, reservado: 0x0, comprimento: 21 *11 de novembro 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Próxima carga: NOTIFY, reservada: 0x0, extensão: 28 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo:	O respondente inicia a criação de SA para esse par.

	NAT_DETECTION_SOURCE_IP *11 de novembro 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Próxima carga: NONE, reservada: 0x0, comprimento: 28 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_DESTINATION_IP	
	*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: IDLE Event:**EV_RECV_INIT** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento:**EV_VERIFY_MSG** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento:**EV_INSERT_SA** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento:**EV_GET_IKE_POLICY** *11 de novembro, 19:30:34.814: IKEv2:Adicionando o padrão da proposta à política do kit de ferramentas *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento:**EV_PROC_MSG** *11 de novembro 19:30:34.814: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento: EV_DETECT_NAT *11 de novembro, 19:30:34.814: IKEv2:(SA ID = 1):Processar notificação de descoberta de NAT *11 de novembro, 19:30:34.814: IKEv2:(SA ID = 1):Processando notificação src de detecção de nat *11 de novembro 19:30:34.814: IKEv2:(ID da AS = 1):Endereço remoto correspondente *11 de novembro 19:30:34.814: IKEv2:(SA ID = 1):Processando notificação dst de detecção nat *11 de novembro 19:30:34.814: IKEv2:(ID da AS = 1):Endereço local correspondente *11 de novembro 19:30:34.814: IKEv2:(ID da AS = 1):Nenhum NAT encontrado *11 de novembro 19:30:34.814: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento: EV_CHK_CONFIG_MODE *11 de novembro 19:30:34.814: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_SET_POLICY *11 de novembro 19:30:34.814: IKEv2:(SA ID = 1):**Definindo**	O respondente verifica e processa a mensagem IKE_INIT: (1) Escolhe o conjunto de criptografia dentre os oferecidos pelo iniciador, (2) calcula sua própria chave secreta DH e (3) calcula um valor skeyid, a partir do qual todas as chaves podem ser derivadas para este IKE_SA. Todos, exceto os cabeçalhos de todas as mensagens que vêm depois, são criptografados e autenticados. As chaves usadas para a criptografia e proteção da integridade são derivadas do SKEYID e são conhecidas como: SK_e (criptografia), SK_a (autenticação), SK_d é derivada e usada para derivação de mais material de chaveamento para CHILD_SAs, e uma SK_e e SK_a separadas são calculadas para cada direção. **Configuração relevante:** `crypto ikev2 proposal PHASE1-prop`

	políticas configuradas *11 de novembro 19:30:34.814: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_CHK_AUTH4PKI *11 de novembro 19:30:34.814: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_PKI_SESH_OPEN *11 de novembro, 19:30:34.814: IKEv2:(SA ID = 1):Abrindo uma sessão PKI *Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento:**EV_GEN_DH_KEY** *11 de novembro 19:30:34.815: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_NO_EVENT *Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento:**EV_OK_RECD_DH_PUBKEY_RESP** *11 de novembro 19:30:34.815: IKEv2:(ID da AS = 1):Ação: Action_Null *Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento:**EV_GEN_DH_SECRET** *11 de novembro 19:30:34.822: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_NO_EVENT *Nov 11 19:30:34.822: IKEv2:% **Obtendo chave pré-compartilhada pelo endereço 10.0.0.1** *11 de novembro, 19:30:34.822: IKEv2:Adicionando o padrão da proposta à política do kit de ferramentas *11 de novembro 19:30:34.822: IKEv2:(2): Escolhendo o perfil IKE IKEV2-SETUP *11 de novembro 19:30:34.822: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_OK_RECD_DH_SECRET_RESP *11 de novembro 19:30:34.822: IKEv2:(ID da AS = 1):Ação: Action_Null *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento:**EV_GEN_SKEYID** *11 de novembro 19:30:34.822: IKEv2:(SA ID = 1):**Gerar skeyid** *11 de novembro 19:30:34.822: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B	`encryption 3des aes-cbc-128 integrity sha1 group 2 crypto ikev2 keyring KEYRNG peer peer2 address 10.0.0.1 255.255.255.0 hostname host2 pre-shared-key local cisco pre-shared-key remote cisco`

	R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_GET_CONFIG_MODE *11 de novembro, 19:30:34.822: IKEv2:IKEv2 Respondente - nenhum dado de configuração para enviar no intercâmbio IKE_SA_INIT *11 de novembro, 19:30:34.822: IKEv2:Nenhum dado de configuração para enviar ao kit de ferramentas: *11 de novembro 19:30:34.822: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_BLD_MSG *11 de novembro, 19:30:34.822: IKEv2: Criar Carga Específica do Fornecedor: DELETE-REASON *11 de novembro, 19:30:34.822: IKEv2: Criar Carga Específica do Fornecedor: (PERSONALIZADO) *11 de novembro 19:30:34.822: IKEv2:Criar Carga de Notificação: NAT_DETECTION_SOURCE_IP *11 de novembro 19:30:34.822: IKEv2:Criar Carga de Notificação: NAT_DETECTION_DESTINATION_IP *11 de novembro 19:30:34.822: IKEv2:Criar Carga de Notificação: HTTP_CERT_LOOKUP_SUPPORTED	
	*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Próxima carga: SA, versão: 2.0 Tipo de troca: **IKE_SA_INIT,** sinalizadores: **RESPONDER MSG-RESPONSE** ID da mensagem: 0, comprimento: 449 Conteúdo da carga: **SA** Próxima carga: KE, reservado: 0x0, comprimento: 48 última proposta: 0x0, reservado: 0x0, comprimento: 44 Proposta: 1, ID do protocolo: IKE, tamanho SPI: 0, #trans: 4 última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **KE** Próxima carga: N, reservado: 0x0, comprimento: 136 Grupo DH: 2, Reservado: 0x0 **N** Próxima carga: VID, reservado: 0x0, comprimento: 24 VID Próxima carga: VID, reservado: 0x0, comprimento: 23 Próxima carga útil de VID: NOTIFY, reservado: 0x0, comprimento: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Próxima carga: NOTIFY, reservado: 0x0, comprimento: 28 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Próxima carga: CERTREQ, reservado: 0x0, comprimento: 28 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo:	O roteador 2 cria a mensagem do respondente para troca IKE_SA_INIT, que é recebida pelo ASA1. Este pacote contém: Cabeçalho ISAKMP (SPI/ versão/sinalizadores), SAr1 (algoritmo criptográfico escolhido pelo respondente IKE), KEr (valor da chave pública DH do respondente) e Respondente Nonce.

	NAT_DETECTION_DESTINATION_IP Carga útil seguinte de CERTREQ: NOTIFY, reservado: 0x0, comprimento: 105 Hash de codificação de certificado e URL de PKIX NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Próxima carga: NENHUMA, reservada: 0x0, comprimento: 8 ID do protocolo de segurança: IKE, tamanho spi: 0, tipo: HTTP_CERT_LOOKUP_SUPPORTED		
	*11 de novembro 19:30:34.822: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Evento: EV_DONE *11 de novembro 19:30:34.822: IKEv2:(ID da AS = 1):Cisco DeleteReason Notify está habilitado *11 de novembro 19:30:34.822: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Evento: EV_CHK4_ROLE *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Evento:**EV_START_TMR** *11 de novembro 19:30:34.822: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_WAIT_AUTH Evento: EV_NO_EVENT *11 de novembro 19:30:34.822: IKEv2:**Nova solicitação ikev2 sa admitida** *11 de novembro 19:30:34.822: IKEv2:**Incrementando negociação de saída como contagem em um**		O Roteador 2 envia a mensagem do respondente ao Roteador 1.
<----------Respondente enviou ---------- IKE_INIT_SA			
O roteador 1 recebe o pacote de resposta IKE_SA_INIT do roteador 2.	*11 de novembro 19:30:34.823: IKEv2: Um pacote foi recebido do despachante *11 de novembro 19:30:34.823: IKEv2: Um pacote foi recebido do despachante *11 de novembro 19:30:34.823: IKEv2:Processando um item fora da fila de pacotes	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = Estado 00000000: Evento INIT_DONE:**EV_START_TMR**	O respondente inicia o timer do processo de Autenticação.
O Roteador 1 verifica e processa a resposta: (1) a	*Nov 11 19:30:34.823: IKEv2:(SA ID = 1):Próxima carga: SA, versão: 2.0 Tipo de troca: IKE_SA_INIT, sinalizadores:		

chave secreta DH do iniciador é computada e (2) a ID de interface do iniciador também é gerada.	**RESPONDER MSG-RESPONSE** ID da mensagem: 0, comprimento: 449 Conteúdo da carga: **SA** Próxima carga: KE, reservado: 0x0, comprimento: 48 última proposta: 0x0, reservado: 0x0, comprimento: 44 Proposta: 1, ID do protocolo: IKE, tamanho SPI: 0, #trans: 4 última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **KE** Próxima carga: N, reservado: 0x0, comprimento: 136 Grupo DH: 2, Reservado: 0x0 **N** Próxima carga: VID, reservado: 0x0, comprimento: 24 *11 de novembro 19:30:34.823: IKEv2:Analisar Carga Específica do Fornecedor: CISCO-DELETE-REASON VID Próxima carga: VID, reservado: 0x0, comprimento: 23 *11 de novembro 19:30:34.823: IKEv2:Analisar Carga Específica do Fornecedor: (PERSONALIZADO) VID Próxima carga: NOTIFY, reservado: 0x0, comprimento: 21 *11 de novembro 19:30:34.823: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Próxima carga: NOTIFY, reservada: 0x0, extensão: 28 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_SOURCE_IP *11 de novembro 19:30:34.824: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Próxima carga: CERTREQ, reservado: 0x0, comprimento: 28 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_DESTINATION_IP Carga útil seguinte de CERTREQ: NOTIFY, reservado: 0x0, comprimento: 105 Hash de codificação de certificado e URL de PKIX *11 de novembro 19:30:34.824: IKEv2:Parse Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Próxima carga: NONE, reservada: 0x0, comprimento: 8 ID do protocolo de segurança: IKE, tamanho spi: 0, tipo: HTTP_CERT_LOOKUP_SUPPORTED *11 de novembro 19:30:34.824: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B	

R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_WAIT_INIT Evento: EV_RECV_INIT
*11 de novembro 19:30:34.824: IKEv2:(ID da AS = 1):Processando mensagem IKE_SA_INIT
*11 de novembro 19:30:34.824: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_CHK4_NOTIFY
*11 de novembro 19:30:34.824: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_VERIFY_MSG
*11 de novembro 19:30:34.824: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_PROC_MSG
*11 de novembro 19:30:34.824: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_DETECT_NAT
*11 de novembro, 19:30:34.824: IKEv2:(SA ID = 1):Processar notificação de descoberta de NAT
*11 de novembro 19:30:34.824: IKEv2:(SA ID = 1):Processando notificação src de detecção de nat
*11 de novembro 19:30:34.824: IKEv2:(ID da AS = 1):Endereço remoto correspondente
*11 de novembro 19:30:34.824: IKEv2:(SA ID = 1):Processando notificação dst de detecção nat
*11 de novembro 19:30:34.824: IKEv2:(ID da AS = 1):Endereço local correspondente
*11 de novembro 19:30:34.824: IKEv2:(ID da AS = 1):Nenhum NAT encontrado
*11 de novembro 19:30:34.824: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_CHK_NAT_T
*11 de novembro 19:30:34.824: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento:**EV_GEN_DH_SECRET**
*11 de novembro 19:30:34.831: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_NO_EVENT
*11 de novembro 19:30:34.831: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_OK_RECD_DH_SECRET_RESP
*11 de novembro 19:30:34.831: IKEv2:(ID da AS = 1):Ação:

	Action_Null *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento:**EV_GEN_SKEYID** *11 de novembro 19:30:34.831: IKEv2:(SA ID = 1):**Gerar skeyid** *11 de novembro 19:30:34.831: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_DONE *11 de novembro 19:30:34.831: IKEv2:(ID da AS = 1):Cisco DeleteReason Notify está habilitado *11 de novembro 19:30:34.831: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_CHK4_ROLE *11 de novembro 19:30:34.831: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_GET_CONFIG_MODE *11 de novembro, 19:30:34.831: IKEv2:Enviando dados de configuração para o kit de ferramentas *11 de novembro 19:30:34.831: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_CHK_EAP	
O iniciador inicia a troca IKE_AUTH e gera o payload de autenticação. O pacote IKE_ AUTH contém: Cabeçalho ISAKMP (SPI/ versão/ flags), IDi (identidade do iniciador), payload AUTH, SAi2 (inicia o SA- semelhante à troca do conjunto de transformação da fase 2 em IKEv1), e TSi e TSr (seletores de Tráfego do Iniciador e do Respondente). Eles contêm os endereços de origem e destino do iniciador e do	*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento:**EV_GEN_AUTH** *11 de novembro 19:30:34.831: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_CHK_AUTH_TYPE *11 de novembro 19:30:34.831: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_OK_AUTH_GEN *11 de novembro 19:30:34.831: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_SEND_AUTH *11 de novembro, 19:30:34.831: IKEv2: Criar carga específica do fornecedor: CISCO-GRANITE *11 de novembro 19:30:34.831: IKEv2:Criar Carga de Notificação: INITIAL_CONTACT *11 de novembro 19:30:34.831: IKEv2:Criar Carga de Notificação: SET_WINDOW_SIZE *11 de novembro, 19:30:34.831: IKEv2: Criar Notificação de Payload: ESP_TFC_NO_SUPPORT	

respondente respectivamente para encaminhar/receber tráfego criptografado. O intervalo de endereços especifica que todo o tráfego de e para esse intervalo é encapsulado. Se a proposta for aceitável para o respondente, ele enviará payloads TS idênticos de volta. O primeiro CHILD_SA é criado para o par proxy_ID que corresponde ao pacote de acionamento. **Configuração relevante:** `crypto ipsec transform-set TS esp-3des esp-sha-hmac crypto ipsec profile phse2-prof set transform-set TS set ikev2-profile IKEV2-SETUP`	*11 de novembro 19:30:34.831: IKEv2:Criar Carga de Notificação: NON_FIRST_FRAGS **Conteúdo da carga:** VID Próxima carga: IDi, reservado: 0x0, comprimento: 20 **IDi** Próxima carga útil: AUTH, reservado: 0x0, comprimento: 12 Tipo de ID: endereço IPv4, Reservado: 0x0 0x0 **AUTH** Próxima carga útil: CFG, reservado: 0x0, comprimento: 28 Método de autenticação PSK, reservado: 0x0, reservado 0x0 **CFG** Próxima carga útil: SA, reservado: 0x0, comprimento: 309 tipo de cfg: CFG_REQUEST, reservado: 0x0, reservado: 0x0 *Nov 11 19:30:34.831: SA Próxima carga: **TSi**, reservado: 0x0, comprimento: 40 última proposta: 0x0, reservado: 0x0, comprimento: 36 Proposta: 1, ID do protocolo: ESP, tamanho SPI: 4, #trans: 3 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 1, reservado: 0x0, id: 3DES última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 5, reservado: 0x0, id: Não usar ESN **TSi** Próxima carga útil: TSr, reservado: 0x0, comprimento: 24 Número de TSs: 1, 0x0 reservado, 0x0 reservado Tipo de TS: TS_IPV4_ADDR_RANGE, id do proto: 0, comprimento: 16 porta inicial: 0, porta final: 65535 end. inicial: 0.0.0.0, end. final: 255.255.255.255 **TSr** Próxima carga útil: NOTIFY, reservado: 0x0, comprimento: 24 Número de TSs: 1, 0x0 reservado, 0x0 reservado Tipo de TS: TS_IPV4_ADDR_RANGE, id do proto: 0, comprimento: 16 porta inicial: 0, porta final: 65535 end. inicial: 0.0.0.0, end. final: 255.255.255.255 NOTIFY(INITIAL_CONTACT) Próxima carga: NOTIFY, reservado: 0x0, comprimento: 8 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: INITIAL_CONTACT NOTIFY(SET_WINDOW_SIZE) Próxima carga: NOTIFY, reservado: 0x0, comprimento: 12 ID do protocolo de segurança: IKE, tamanho spi: 0, tipo: SET_WINDOW_SIZE NOTIFY(ESP_TFC_NO_SUPPORT) Próxima carga: NOTIFY, reservado: 0x0, comprimento: 8 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: ESP_TFC_NO_SUPPORT NOTIFY(NON_FIRST_FRAGS) Próxima carga: NONE, reservado: 0x0, comprimento: 8 ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NON_FIRST_FRAGS	

	*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Próxima carga útil: ENCR, versão: 2.0 Tipo de troca: **IKE_AUTH**, sinalizadores: **INITIATOR** ID da mensagem: 1, comprimento: 556 Conteúdo da carga: Próximo payload de ENCR: VID, reservado: 0x0, comprimento: 528 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 **CurState: I_WAIT_AUTH** Evento: EV_NO_EVENT	
----------Iniciador enviou IKE_AUTH ---------->		
	*11 de novembro 19:30:34.832: IKEv2: Um pacote foi recebido do despachante *11 de novembro 19:30:34.832: IKEv2:Processando um item fora da fila de pacotes *11 de novembro 19:30:34.832: IKEv2:(ID da AS = 1):A solicitação tem messe_id 1; esperada de 1 a 1 *11 de novembro 19:30:34.832: **IKEv2:(SA ID = 1)**:Próxima carga útil: ENCR, versão: 2.0 Tipo de troca: **IKE_AUTH**, sinalizadores: **INITIATOR** ID da mensagem: 1, comprimento: 556 Conteúdo da carga: *11 de novembro 19:30:34.832: IKEv2:Analisar Carga Específica do Fornecedor: (PERSONALIZADO) VID Próxima carga: IDi, reservado: 0x0, comprimento: 20 **IDi** Próxima carga útil: AUTH, reservado: 0x0, comprimento: 12 Tipo de ID: endereço IPv4, Reservado: 0x0 0x0 **AUTH** Próxima carga útil: CFG, reservado: 0x0, comprimento: 28 Método de autenticação PSK, reservado: 0x0, reservado 0x0 **CFG** Próxima carga útil: SA, reservado: 0x0, comprimento: 309 tipo de cfg: CFG_REQUEST, reservado: 0x0, reservado: 0x0 *11 de novembro 19:30:34.832: tipo de atributo: DNS IP4 interno, comprimento: 0 *11 de novembro 19:30:34.832: tipo de atributo: DNS IP4 interno, comprimento: 0 *11 de novembro 19:30:34.832: tipo de atributo: IP interno4 NBNS, comprimento: 0 *11 de novembro 19:30:34.832: tipo de atributo: IP interno4 NBNS, comprimento: 0 *11 de novembro 19:30:34.832: tipo de atributo: sub-rede IP4 interna, comprimento: 0 *Nov 11 19:30:34.832: tipo de atributo: versão do aplicativo, comprimento: 257 tipo de atributo: Desconhecido - 28675, comprimento: 0 *11 de novembro 19:30:34.832: tipo de atributo: Desconhecido - 28672, comprimento: 0 *11 de novembro 19:30:34.832: tipo de atributo: Desconhecido - 28692, comprimento: 0	O roteador 2 recebe e verifica os dados de autenticação recebidos do roteador 1. **Configuração relevante**: `crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-1 md5`

	*11 de novembro 19:30:34.832: tipo de atributo: Desconhecido - 28681, comprimento: 0 *11 de novembro 19:30:34.832: tipo de atributo: Desconhecido - 28674, comprimento: 0 *Nov 11 19:30:34.832: **SA** Próximo payload: TSi, reservado: 0x0, comprimento: 40 última proposta: 0x0, reservado: 0x0, comprimento: 36 Proposta: 1, ID do protocolo: ESP, tamanho SPI: 4, #trans: 3 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 1, reservado: 0x0, id: 3DES última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 5, reservado: 0x0, id: Não usar ESN **TSi** Próxima carga útil: TSr, reservado: 0x0, comprimento: 24 Número de TSs: 1, 0x0 reservado, 0x0 reservado Tipo de TS: TS_IPV4_ADDR_RANGE, id do proto: 0, comprimento: 16 porta inicial: 0, porta final: 65535 end. inicial: 0.0.0.0, end. final: 255.255.255.255 **TSr** Próxima carga útil: NOTIFY, reservado: 0x0, comprimento: 24 Número de TSs: 1, 0x0 reservado, 0x0 reservado Tipo de TS: TS_IPV4_ADDR_RANGE, id do proto: 0, comprimento: 16 porta inicial: 0, porta final: 65535 end. inicial: 0.0.0.0, end. final: 255.255.255.255	
	*11 de novembro 19:30:34.832: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_RECV_AUTH *11 de novembro 19:30:34.832: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_NAT_T *11 de novembro 19:30:34.832: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_PROC_ID *11 de novembro 19:30:34.832: IKEv2:(ID da AS = 1):Parâmetros válidos recebidos no ID do processo *11 de novembro 19:30:34.832: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR PROF_SEL *11 de novembro 19:30:34.832: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_GET_POLICY_BY_PEERID	O Roteador 2 cria a resposta para o pacote IKE_AUTH recebido do Roteador 1. Este pacote de resposta contém: Cabeçalho ISAKMP (SPI/ versão/sinalizadores), IDr. (identidade do respondente), payload AUTH, SAr2 (inicia o SA-similar à troca do conjunto de transformação da fase 2 em IKEv1) e TSi e TSr (seletores de Tráfego do Iniciador e do Respondente). Eles contêm os endereços de origem e destino do iniciador e do respondente respectivamente para

	*11 de novembro 19:30:34.833: IKEv2:(1): Escolhendo o perfil IKE IKEV2-SETUP *11 de novembro 19:30:34.833: IKEv2:% Obtendo chave pré-compartilhada pelo endereço 10.0.0.1 *11 de novembro 19:30:34.833: IKEv2:% Obtendo chave pré-compartilhada pelo endereço 10.0.0.1 *11 de novembro, 19:30:34.833: IKEv2:Adicionando o padrão da proposta à política do kit de ferramentas *11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):Usando o perfil IKEv2 'IKEV2-SETUP' *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_SET_POLICY *11 de novembro, 19:30:34.833: IKEv2:(SA ID = 1):Definindo políticas configuradas *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_VERIFY_POLICY_BY_PEERID *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_AUTH4EAP *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_POLREQEAP *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK_AUTH_TYPE *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_GET_PRESHR_KEY *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_VERIFY_AUTH *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK4_IC *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK_REDIRECT *11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):Não é necessária verificação de redirecionamento, ignorando-a *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState:	encaminhar/receber tráfego criptografado. O intervalo de endereços especifica que todo o tráfego de e para esse intervalo é encapsulado. Esses parâmetros são idênticos àquele que foi recebido do ASA1.

R_VERIFY_AUTH Evento: EV_NOTIFY_AUTH_DONE
*11 de novembro 19:30:34.833: IKEv2:AAA group authorization não is configured
*11 de novembro 19:30:34.833: IKEv2:AAA autorização do usuário não configurada
*11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK_CONFIG_MODE
*11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_SET_RECD_CONFIG_MODE
*11 de novembro 19:30:34.833: IKEv2:Dados de configuração recebidos do kit de ferramentas:
*11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_PROC_SA_TS
*11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_GET_CONFIG_MODE
*11 de novembro 19:30:34.833: IKEv2:Erro ao criar resposta de configuração
*11 de novembro, 19:30:34.833: IKEv2:Sem dados de configuração para enviar ao kit de ferramentas:
*11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_MY_AUTH_METHOD
*11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_GET_PRESHR_KEY
*11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_GEN_AUTH
*11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_CHK4_SIGN
*11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_OK_AUTH_GEN
*11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_SEND_AUTH
*11 de novembro, 19:30:34.833: IKEv2: Criar carga específica do fornecedor: CISCO-GRANITE

	*11 de novembro 19:30:34.833: IKEv2:Criar Carga de Notificação: SET_WINDOW_SIZE *11 de novembro 19:30:34.833: IKEv2:Criar Carga de Notificação: ESP_TFC_NO_SUPPORT *11 de novembro 19:30:34.833: IKEv2:Criar Carga de Notificação: NON_FIRST_FRAGS		
	*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Próxima carga útil: ENCR, versão: 2.0 Tipo de troca: **IKE_AUTH**, sinalizadores: **RESPONDER MSG-RESPONSE** ID da mensagem: 1, comprimento: 252 Conteúdo da carga: **ENCR** Próxima carga útil: VID, reservado: 0x0, comprimento: 224 *11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_OK *11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):Ação: Action_Null *11 de novembro 19:30:34.833: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_PKI_SESH_CLOSE *11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):Fechando a sessão PKI *11 de novembro 19:30:34.833: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_UPDATE_CAC_STATS *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento:**EV_INSERT_IKE** *11 de novembro 19:30:34.834: IKEv2:Índice MIB de loja ikev2 1, plataforma 60 *11 de novembro 19:30:34.834: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_GEN_LOAD_IPSEC *11 de novembro 19:30:34.834: IKEv2:(ID da AS = 1):Solicitação assíncrona na fila *11 de novembro 19:30:34.834: IKEv2:(ID da AS = 1): *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **AUTH_DONE** Evento: EV_NO_EVENT		O respondente envia a resposta para IKE_AUTH.
<----------Responder enviou IKE_AUTH----------			
O iniciador recebe a resposta do Respondente.	*11 de novembro 19:30:34.834: IKEv2: Um	*11 de novembro 19:30:34.840: IKEv2:(ID da AS = 1):SM Trace-	O respondente insere uma entrada no SAD.

	pacote foi recebido do despachante *11 de novembro 19:30:34.834: IKEv2:Processando um item fora da fila de pacotes	> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_OK_RECD_LOAD_IPSEC *11 de novembro 19:30:34.840: IKEv2:(ID da AS = 1):Ação: Action_Null *11 de novembro 19:30:34.840: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_START_ACCT *11 de novembro 19:30:34.840: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHECK_DUPE *11 de novembro 19:30:34.840: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHK4_ROLE	
O roteador 1 verifica e processa os dados de autenticação nesse pacote. O roteador 1 insere essa AS em seu SAD.	*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Próxima carga útil: ENCR, versão: 2.0 Tipo de troca: **IKE_AUTH**, sinalizadores: **RESPONDER MSG-RESPONSE** ID da mensagem: 1, comprimento: 252 **Conteúdo da carga:** *11 de novembro 19:30:34.834: IKEv2:Analisar Carga Específica do Fornecedor: (PERSONALIZADO) VID Próxima carga: IDr., reservado: 0x0, comprimento: 20 **IDr. Próxima** carga: AUTH, reservado: 0x0, comprimento: 12 Tipo de ID: endereço IPv4, Reservado: 0x0 0x0 **AUTH** Próxima carga: SA, reservado: 0x0, comprimento: 28 Método de autenticação PSK, reservado: 0x0, reservado 0x0 **SA** Próxima carga: TSi, reservado: 0x0, comprimento: 40 última proposta: 0x0, reservado: 0x0, comprimento: 36 Proposta: 1, ID do protocolo: ESP, tamanho SPI: 4, #trans: 3 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 1, reservado: 0x0, id: 3DES		

última transformação: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, id: SHA96
última transformação: 0x0, reservado: 0x0: comprimento: 8
tipo: 5, reservado: 0x0, id: Não usar ESN
TSi Próxima carga útil: TSr, reservado: 0x0, comprimento: 24
Número de TSs: 1, 0x0 reservado, 0x0 reservado
Tipo de TS: TS_IPV4_ADDR_RANGE, id do proto: 0, comprimento: 16
porta inicial: 0, porta final: 65535
end. inicial: 0.0.0.0, end. final: 255.255.255.255
TSr Próxima carga útil: NOTIFY, reservado: 0x0, comprimento: 24
Número de TSs: 1, 0x0 reservado, 0x0 reservado
Tipo de TS: TS_IPV4_ADDR_RANGE, id do proto: 0, comprimento: 16
porta inicial: 0, porta final: 65535
end. inicial: 0.0.0.0, end. final: 255.255.255.255

*11 de novembro 19:30:34.834: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Próxima carga: NOTIFY, reservado: 0x0, comprimento: 12
ID do protocolo de segurança: IKE, tamanho spi: 0, tipo: SET_WINDOW_SIZE

*11 de novembro 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) Próxima carga: NOTIFY, reservado: 0x0, comprimento: 8
ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: ESP_TFC_NO_SUPPORT

*11 de novembro 19:30:34.834: IKEv2:Parse Notify Payload: NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) Próxima carga: NONE, reservada: 0x0, comprimento: 8
ID do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NON_FIRST_FRAGS

*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_WAIT_AUTH Evento:**EV_RECV_AUTH**
*11 de novembro 19:30:34.834: IKEv2:(ID da AS = 1):Ação: Action_Null
*11 de novembro 19:30:34.834: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK4_NOTIFY
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento:**EV_PROC_MSG**
*11 de novembro 19:30:34.834: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B

R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR PROF_SEL
*11 de novembro 19:30:34.834: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_GET_POLICY_BY_PEERID
*11 de novembro 19:30:34.834: IKEv2:Adicionando proposta PHASE1-prop à política de kit de ferramentas
*11 de novembro 19:30:34.834: IKEv2:(ID da AS = 1):Usando o perfil IKEv2 'IKEV2-SETUP'
*11 de novembro 19:30:34.834: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_VERIFY_POLICY_BY_PEERID
*11 de novembro 19:30:34.834: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_AUTH_TYPE
*11 de novembro 19:30:34.834: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_GET_PRESHR_KEY
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento:**EV_VERIFY_AUTH**
*11 de novembro 19:30:34.835: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_EAP
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento:**EV_NOTIFY_AUTH_DONE**
*11 de novembro 19:30:34.835: IKEv2:AAA group authorization não is configured
*11 de novembro 19:30:34.835: IKEv2:AAA autorização do usuário não configurada
*11 de novembro 19:30:34.835: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_CONFIG_MODE
*11 de novembro 19:30:34.835: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK4_IC
*11 de novembro 19:30:34.835: IKEv2:(ID da SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_IKE_ONLY
*11 de novembro 19:30:34.835: IKEv2:(ID da AS = 1):SM

Trace-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState:
I_PROC_AUTH Evento: EV_PROC_SA_TS
*11 de novembro 19:30:34.835: IKEv2:(ID da AS = 1):SM
Trace-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState:
AUTH_DONE Evento: EV_OK
*11 de novembro 19:30:34.835: IKEv2:(ID da AS = 1):Ação:
Action_Null
*11 de novembro 19:30:34.835: IKEv2:(ID da SA = 1):SM
Trace-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState:
AUTH_DONE Evento: EV_PKI_SESH_CLOSE
*11 de novembro 19:30:34.835: IKEv2:(ID da AS = 1):Fechando
a sessão PKI
*11 de novembro 19:30:34.835: IKEv2:(ID da SA = 1):SM
Trace-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState:
AUTH_DONE Evento: EV_UPDATE_CAC_STATS
*11 de novembro 19:30:34.835: IKEv2:(ID da SA = 1):SM
Trace-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState:
AUTH_DONE Evento: EV_INSERT_IKE
*11 de novembro 19:30:34.835: IKEv2:Índice MIB de loja ikev2
1, plataforma 60
*11 de novembro 19:30:34.835: IKEv2:(ID da AS = 1):SM
Trace-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState:
AUTH_DONE Evento: EV_GEN_LOAD_IPSEC
*11 de novembro 19:30:34.835: IKEv2:(ID da AS =
1):Solicitação assíncrona na fila

*11 de novembro 19:30:34.835: IKEv2:(ID da AS = 1):
*11 de novembro 19:30:34.835: IKEv2:(ID da SA = 1):SM
Trace-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState:
AUTH_DONE Evento: EV_NO_EVENT
*11 de novembro 19:30:34.835: mensagem 8 de IKEv2:KMI
consumida. Nenhuma ação executada.
*11 de novembro 19:30:34.835: mensagem 12 de IKEv2:KMI
consumida. Nenhuma ação executada.
*11 de novembro, 19:30:34.835: IKEv2: nenhum dado para
enviar no conjunto de configurações do modo.
*11 de novembro 19:30:34.841: IKEv2:Adicionando
identificador de identificação 0x80000002 associado a SPI
0x9506D414 para a sessão 8

*11 de novembro 19:30:34.841: IKEv2:(ID da AS = 1):SM
Trace-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState:
AUTH_DONE Evento: EV_OK_RECD_LOAD_IPSEC
*11 de novembro 19:30:34.841: IKEv2:(ID da AS = 1):Ação:
Action_Null

	*11 de novembro 19:30:34.841: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_START_ACCT *11 de novembro 19:30:34.841: IKEv2:(ID da AS = 1):Contabilidade não necessária *11 de novembro 19:30:34.841: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHECK_DUPE *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: **AUTH_DONE** Evento: EV_CHK4_ROLE		
O túnel está ativo no iniciador e o status *mostraREADY*.	*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: READYEvent: EV_CHK_IKE_ONLY *11 de novembro 19:30:34.841: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: READY Evento: EV_I_OK	*****Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **READY** Evento: EV_R_OK *11 de novembro 19:30:34.840: IKEv2:(ID da AS = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: READY Evento: EV_NO_EVENT	O túnel está ativado no Respondente. O túnel do Respondente geralmente aparece antes do Iniciador.

Depurações CHILD_SA

Essa troca consiste em um único par de solicitação/resposta e foi chamada de troca de fase 2 em IKEv1. Ele pode ser iniciado por qualquer extremidade do IKE_SA após a conclusão das trocas iniciais.

Descrição da mensagem do roteador 1 CHILD_SA	Debugs	Descrição da mensagem do roteador 2 CHILD_SA
O roteador 1 inicia a troca CHILD_SA. Esta é a solicitação CREATE_CHILD_SA. O pacote CHILD_SA normalmente contém: • SA HDR (tipo version.flags/exchange) • Nonce Ni (opcional): se CHILD_SA for	*11 de novembro 19:31:35.873: IKEv2: Um pacote foi recebido do despachante *11 de novembro 19:31:35.873: IKEv2:Processando um item fora da fila de pacotes *11 de novembro, 19:31:35.873: IKEv2:(ID da AS = 2):A solicitação tem messe_id 3; esperada de 3 a 7	

criado como parte da troca inicial, um segundo payload de KE e nonce não deverão ser enviados) • Payload de SA • KEi (Chave opcional): A solicitação CREATE_CHILD_SA pode, opcionalmente, conter uma carga KE para uma troca DH adicional para permitir garantias mais fortes de sigilo de encaminhamento para CHILD_SA. Se as ofertas de SA incluírem diferentes grupos DH, o KEi deverá ser um elemento do grupo que o iniciador espera que o respondente aceite. Se ele achar errado, a troca CREATE_CHILD_SA falhará e poderá tentar novamente com um KEi diferente • N(Notify payload-optional). O Payload de Notificação, é usado para transmitir dados informativos, como condições de erro e transições de estado, para um peer IKE. Uma Carga Útil de Notificação pode aparecer em uma mensagem de resposta (geralmente ela especifica por que uma solicitação foi rejeitada), em uma Troca INFORMATIVA (para relatar um erro que não seja em uma solicitação IKE) ou em qualquer outra mensagem para indicar	*Nov 11 19:31:35.873: IKEv2:(SA ID = 2):Próxima carga útil: ENCR, versão: 2.0 **Tipo de troca: CREATE_CHILD_SA**, sinalizadores: **INITIATOR** ID da mensagem: 3, comprimento: 396 Conteúdo da carga: **SA** Próxima carga: N, reservado: 0x0, comprimento: 152 última proposta: 0x0, reservado: 0x0, comprimento: 148 Proposta: 1, ID do protocolo: IKE, tamanho SPI: 8, #trans: 15 última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA512 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA384 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA256 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: MD5 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA512 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA384 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA256 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: MD596 última transformação: 0x3, reservado: 0x0: comprimento: 8	

recursos do remetente ou para modificar o significado da solicitação. Se essa troca CREATE_CHILD_SA estiver reinserindo uma SA existente diferente de IKE_SA, a carga útil N principal do tipo REKEY_SA DEVERÁ identificar a SA que está sendo reinserida. Se essa troca CREATE_CHILD_SA não estiver rechaveando uma SA existente, o payload N DEVERÁ ser omitido.	tipo: 4, reservado: 0x0, id: DH_GROUP_1536_MODP/Grupo 5 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **N** Próxima carga útil: KE, reservado: 0x0, comprimento: 24 Próxima carga útil do **KE**: NOTIFY, reservado: 0x0, comprimento: 136 Grupo DH: 2, Reservado: 0x0 *Nov 11 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) Próximo payload: NONE, reservado: 0x0, length: 12 ID do protocolo de segurança: IKE, tamanho spi: 0, tipo: SET_WINDOW_SIZE *11 de novembro 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: READY Evento: **EV_RECV_CREATE_CHILD** *11 de novembro 19:31:35.874: IKEv2:(ID da AS = 2):Ação: Action_Null *11 de novembro, 19:31:35.874: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Evento: EV_RECV_CREATE_CHILD *11 de novembro 19:31:35.874: IKEv2:(ID da AS = 2):Ação: Action_Null *11 de novembro, 19:31:35.874: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Evento: EV_VERIFY_MSG *11 de novembro, 19:31:35.874: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Evento: EV_CHK_CC_TYPE *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Evento: **EV_REKEY_IKESA**	

	*11 de novembro, 19:31:35.874: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Evento: EV_GET_IKE_POLICY *Nov 11 19:31:35.874: IKEv2:% **Obtendo chave pré-compartilhada pelo endereço 10.0.0.2** *Nov 11 19:31:35.874: IKEv2:% Obtendo chave pré-compartilhada pelo endereço 10.0.0.2 *11 de novembro 19:31:35.874: IKEv2:Adicionando proposta PHASE1-prop à política de kit de ferramentas *11 de novembro 19:31:35.874: IKEv2:(ID da AS = 2):Usando o perfil IKEv2 'IKEV2-SETUP' *11 de novembro, 19:31:35.874: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Evento: EV_PROC_MSG *11 de novembro, 19:31:35.874: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Evento: EV_SET_POLICY *11 de novembro 19:31:35.874: IKEv2:(SA ID = 2):**Definindo políticas configuradas** *11 de novembro, 19:31:35.874: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento: EV_GEN_DH_KEY *11 de novembro, 19:31:35.874: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento: EV_NO_EVENT *11 de novembro, 19:31:35.874: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento: EV_OK_RECD_DH_PUBKEY_RESP *11 de novembro 19:31:35.874: IKEv2:(ID da AS = 2):Ação: Action_Null	

	*11 de novembro 19:31:35.874: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento:**EV_GEN_DH_SECRET** *11 de novembro, 19:31:35.881: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento: EV_NO_EVENT *11 de novembro, 19:31:35.882: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento: EV_OK_RECD_DH_SECRET_RESP *11 de novembro 19:31:35.882: IKEv2:(ID da AS = 2):Ação: Action_Null *11 de novembro, 19:31:35.882: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento: EV_BLD_MSG *11 de novembro 19:31:35.882: **IKEv2:ConstructNotify Payload**: SET_WINDOW_SIZE Conteúdo da carga: **SA** Próxima carga: N, reservado: 0x0, comprimento: 56 última proposta: 0x0, reservado: 0x0, comprimento: 52 Proposta: 1, ID do protocolo: IKE, tamanho SPI: 8, #trans: 4 última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **N** Próxima carga útil: KE, reservado: 0x0, comprimento: 24 Próxima carga útil do **KE**: NOTIFY, reservado: 0x0, comprimento: 136	

	Grupo DH: 2, Reservado: 0x0 **NOTIFY**(SET_WINDOW_SIZE) Próxima carga: NONE, reservada: 0x0, comprimento: 12 ID do protocolo de segurança: IKE, tamanho spi: 0, tipo: SET_WINDOW_SIZE	
	*Nov 11 19:31:35.869: IKEv2:(**SA ID = 2**):Próxima carga útil: ENCR, versão: 2.0 Tipo de troca: **CREATE_CHILD_SA**, sinalizadores: **INITIATOR** ID da mensagem: 2, comprimento: 460 Conteúdo da carga: Próximo payload de ENCR: SA, reservado: 0x0, comprimento: 432 *11 de novembro 19:31:35.873: IKEv2:Criar Carga de Notificação: SET_WINDOW_SIZE Conteúdo da carga: **SA** Próxima carga: N, reservado: 0x0, comprimento: 152 última proposta: 0x0, reservado: 0x0, comprimento: 148 Proposta: 1, ID do protocolo: IKE, tamanho SPI: 8, #trans: 15 última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA512 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA384 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA256 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: MD5 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA512	Esse pacote é recebido pelo Roteador 2.

	última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA384 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA256 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: MD596 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1536_MODP/Grupo 5 última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **N** Próxima carga útil: KE, reservado: 0x0, comprimento: 24 Próxima carga útil do **KE**: NOTIFY, reservado: 0x0, comprimento: 136 Grupo DH: 2, Reservado: 0x0 **NOTIFY**(SET_WINDOW_SIZE) Próxima carga: NONE, reservada: 0x0, comprimento: 12 ID do protocolo de segurança: IKE, tamanho spi: 0, tipo: SET_WINDOW_SIZE	
	*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):Próxima carga útil: ENCR, versão: 2.0 Tipo de troca: **CREATE_CHILD_SA,** sinalizadores: **RESPONDER MSG-RESPONSE** ID da mensagem: 3, comprimento: 300 Conteúdo da carga: **SA** Próxima carga: N, reservado: 0x0, comprimento: 56 última proposta: 0x0, reservado: 0x0, comprimento: 52 Proposta: 1, ID do protocolo: IKE, tamanho SPI: 8, #trans: 4 última transformação: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformação: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, id: SHA96	O roteador 2 agora cria a resposta para a troca CHILD_SA. Esta é a resposta CREATE_CHILD_SA. O pacote CHILD_SA normalmente contém: • SA HDR (tipo version.flags/exchange) • Nonce Ni(opcional): se CHILD_SA for criado como parte da troca inicial, um segundo payload de KE e nonce não deverão ser enviados. • Payload de SA • KEi (Chave opcional): A solicitação CREATE_CHILD_SA pode, opcionalmente, conter uma carga KE

	última transformação: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **N** Próxima carga útil: KE, reservado: 0x0, comprimento: 24 Próxima carga útil do **KE**: NOTIFY, reservado: 0x0, comprimento: 136 Grupo DH: 2, Reservado: 0x0 *Nov 11 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) Próximo payload: NONE, reservado: 0x0, length: 12 ID do protocolo de segurança: IKE, tamanho spi: 0, tipo: SET_WINDOW_SIZE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_WAIT** Evento: **EV_RECV_CREATE_CHILD** *11 de novembro 19:31:35.882: IKEv2:(ID da AS = 2):Ação: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_PROC** Evento: EV_CHK4_NOTIFY *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: **EV_VERIFY_MSG** *11 de novembro, 19:31:35.882: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_PROC_MSG *11 de novembro, 19:31:35.882: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_CHK4_PFS *11 de novembro, 19:31:35.882: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID =	para uma troca DH adicional para permitir garantias mais fortes de sigilo de encaminhamento para CHILD_SA. Se as ofertas de SA incluírem diferentes grupos DH, o KEi deverá ser um elemento do grupo que o iniciador espera que o respondente aceite. Se ele achar errado, a troca CREATE_CHILD_SA falhará e deverá tentar novamente com um KEi diferente. • N (Notify payload-optional): A carga útil de notificação é usada para transmitir dados informativos, como condições de erro e transições de estado, para um peer IKE. Um Payload de Notificação pode aparecer em uma mensagem de resposta (geralmente ele especifica por que uma solicitação foi rejeitada), em uma troca de informações (para relatar um erro que não seja em uma solicitação IKE) ou em qualquer outra mensagem para indicar as capacidades do remetente ou para modificar o significado da solicitação. Se essa troca CREATE_CHILD_SA estiver rechaveando uma SA existente diferente de IKE_SA, a carga N principal do tipo REKEY_SA deverá identificar a SA que está sendo

	00000003 CurState: CHILD_I_PROC Evento: EV_GEN_DH_SECRET *11 de novembro, 19:31:35.890: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_NO_EVENT *11 de novembro, 19:31:35.890: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_OK_RECD_DH_SECRET_RESP *11 de novembro 19:31:35.890: IKEv2:(ID da AS = 2):Ação: Action_Null *11 de novembro, 19:31:35.890: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_CHK_IKE_REKEY *11 de novembro, 19:31:35.890: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_GEN_SKEYID *11 de novembro 19:31:35.890: IKEv2:(ID da AS = 2):Gerar skeyid *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_DONE** Evento: **EV_ATIVATE_NEW_SA** *11 de novembro, 19:31:35.890: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Evento: EV_UPDATE_CAC_STATS *11 de novembro 19:31:35.890: IKEv2:Nova solicitação sa ikev2 ativada *11 de novembro 19:31:35.890: IKEv2:Falha ao diminuir a contagem para negociação de saída *11 de novembro, 19:31:35.890: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE	rechaveada. Se essa troca CREATE_CHILD_SA não estiver recolocando uma SA existente, a carga útil N deverá ser omitida. O roteador 2 envia a resposta e conclui a ativação da nova SA FILHO.

	Evento: EV_CHECK_DUPE *11 de novembro, 19:31:35.890: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Evento: EV_OK *11 de novembro, 19:31:35.890: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: Evento de SAÍDA: EV_CHK_PENDING *11 de novembro 19:31:35.890: IKEv2:(ID da AS = 2):Resposta processada com ID de mensagem 3, as solicitações podem ser enviadas do intervalo 4 a 8 *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 **CurState: EXIT** Evento: EV_NO_EVENT	
O Roteador 1 recebe o pacote de resposta do Roteador 2 e conclui a ativação de CHILD_SA.	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Próxima carga útil: ENCR, versão: 2.0 Tipo de troca: **CREATE_CHILD_SA**, sinalizadores: **RESPONDER MSG-RESPONSE** ID da mensagem: 3, comprimento: 300 Conteúdo da carga: Próximo payload de ENCR: SA, reservado: 0x0, comprimento: 272 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento:**EV_CHK_IKE_REKEY** *11 de novembro, 19:31:35.882: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Evento: EV_GEN_SKEYID *11 de novembro 19:31:35.882: IKEv2:(SA ID = 2):**Gerar skeyid** *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID =	

	00000003 CurState: CHILD_R_DONE Evento:**EV_ATIVATE_NEW_SA** *11 de novembro 19:31:35.882: IKEv2:Índice MIB de loja ikev2 3, plataforma 62 *11 de novembro, 19:31:35.882: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Evento: EV_UPDATE_CAC_STATS *11 de novembro 19:31:35.882: IKEv2:Nova solicitação sa ikev2 ativada *11 de novembro 19:31:35.882: IKEv2:Falha ao diminuir a contagem para negociação de entrada *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: **CHILD_R_DONE** Evento: EV_CHECK_DUPE *11 de novembro, 19:31:35.882: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Evento: EV_OK *11 de novembro 19:31:35.882: IKEv2:(ID da SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Evento: EV_START_DEL_NEG_TMR *11 de novembro 19:31:35.882: IKEv2:(ID da AS = 2):Ação: Action_Null *11 de novembro, 19:31:35.882: IKEv2:(ID da AS = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento de SAÍDA: EV_CHK_PENDING *11 de novembro 19:31:35.882: IKEv2:(ID da AS = 2):Resposta enviada com ID de mensagem 3, as solicitações podem ser aceitas do intervalo 4 a 8 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 **CurState: EXIT** Evento: EV_NO_EVENT	

Verificação de túnel

ISAKMP

Comando

<#root>

show crypto ikev2 sa detailed

Saída do roteador 1

<#root>

```
Router1#
```

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote             fvrf/ivrf         Status
1         10.0.0.1/500          10.0.0.2/500       none/none         READY
      Encr: AES-CBC, keysize: 128,
         Hash: SHA96, DH Grp:2,
         Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/10 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: E58F925107F8B73F     Remote spi: AFD098F4147869DA
      Local id: 10.0.0.1
      Remote id: 10.0.0.2
      Local req msg id:  2       Remote req msg id:  0
      Local next msg id: 2       Remote next msg id: 0
      Local req queued:  2       Remote req queued:  0
      Local window:      5       Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
```

Saída do roteador 2

<#root>

```
Router2#
```

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA
```

```
Tunnel-id Local           Remote              fvrf/ivrf         Status
2         10.0.0.2/500    10.0.0.1/500        none/none         READY
      Encr: AES-CBC, keysize: 128, Hash: SHA96,
         DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/37 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: AFD098F4147869DA       Remote spi: E58F925107F8B73F
      Local id: 10.0.0.2
      Remote id: 10.0.0.1
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
```

IPsec

Comando

<#root>

show crypto ipsec sa

> **Observação**: nesta saída, ao contrário de IKEv1, o valor do grupo DH do PFS aparece como "PFS (Y/N): N, grupo DH: nenhum" durante a primeira negociação de túnel, mas, após uma nova chave ocorrer, os valores corretos aparecem. Isso não é um bug, embora o comportamento esteja descrito na ID de bug Cisco CSCug67056. (Somente usuários registrados da Cisco podem acessar ferramentas ou informações internas da Cisco.)
> A diferença entre IKEv1 e IKEv2 é que, neste último, as SAs Filho são criadas como parte da própria troca AUTH. O Grupo DH configurado no mapa de criptografia seria usado somente durante a rechave. Assim, você veria 'PFS (Y/N): N, DH group: none' até o primeiro rechaveamento.
> Com IKEv1, você vê um comportamento diferente, porque a criação de SA Filho acontece durante o Modo Rápido, e a mensagem CREATE_CHILD_SA tem uma provisão para transportar a carga útil de Troca de Chaves que especifica os parâmetros DH para derivar um novo segredo compartilhado.

Saída do roteador 1

<#root>

```
Router1#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0,
         local addr 10.0.0.1
```

```
protected vrf: (none)
local  ident (addr/mask/prot/port):
      (0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port):
      (0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.2 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 10, #pkts encrypt:
      10, #pkts digest: 10
 #pkts decaps: 10, #pkts decrypt:
      10, #pkts verify: 10
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 10.0.0.1,
      remote crypto endpt.: 10.0.0.2
  path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
  current outbound spi: 0xF6083ADD(4127734493)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0x6B74CB79(1802816377)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 18, flow_id: SW:18,
      sibling_flags 80000040,
      crypto map: Tunnel0-head-0
     sa timing: remaining key lifetime (k/sec):
      (4276853/3592)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0xF6083ADD(4127734493)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 17, flow_id: SW:17,
      sibling_flags 80000040,
      crypto map: Tunnel0-head-0
     sa timing: remaining key
      lifetime (k/sec): (4276853/3592)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  outbound ah sas:

  outbound pcp sas:
```

Saída do roteador 2

```
<#root>
```

```
Router2#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.2,
         remote crypto endpt.: 10.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x6B74CB79(1802816377)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime
         (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Você também pode verificar a saída do comando **show crypto session** em ambos os roteadores; essa saída mostra o status da sessão do túnel como UP-ATIVE.

<#root>

```
Router1#
```

show crypto session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
  IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Router2#
```

show cry session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
  IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Informações Relacionadas

- **Intercâmbio de pacotes IKEv2 e depuração de nível de protocolo**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.