Os IO IKEv2 debugam para o VPN de Site-para-Site com os PSK que pesquisam defeitos TechNote

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Edição de núcleo
Configuração do roteador
Troubleshooting
Depurações de roteador
CHILD_SA debuga
Verificação do túnel
ISAKMP
IPsec
Informações Relacionadas

Introdução

Este documento descreve a versão 2 do intercâmbio de chave de Internet (IKEv2) debuga no ® do Cisco IOS quando uma chave pré-compartilhada (PSK) é usada. Além, este documento fornece a informação em como traduzir certo debuga linhas em uma configuração.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do intercâmbio de pacotes para IKEv2. Para mais informação, refira a eliminação de erros do intercâmbio de pacotes IKEv2 e do nível de protocolo.

Componentes Utilizados

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

- Versão 2 do intercâmbio de chave de Internet (IKEv2)
- Cisco IOS 15.1(1)T ou mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Edição de núcleo

O intercâmbio de pacotes em IKEv2 é radicalmente diferente do intercâmbio de pacotes em IKEv1. Em IKEv1 havia uma troca phase1 claramente delimitada que consistisse em seis (6) pacotes seguidos por uma troca da fase 2 que consistisse em três (3) pacotes; a troca IKEv2 é variável. Para obter mais informações sobre das diferenças e de uma explicação do intercâmbio de pacotes, refira a eliminação de erros do intercâmbio de pacotes IKEv2 e do nível de protocolo.

Configuração do roteador

Esta seção alista 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
```

Troubleshooting

Depurações de roteador

Estes comandos debug são usados neste documento:

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

Descrição de mensagem do roteador1 (iniciador)	Debugs	Descrição de mensagem do roteador2 (que responde)
O roteador1 recebe um pacote que combine o acl cripto para o par ASA 10.0.0.2. Criação novatos SA	* 11 de novembro 20:28:34.003: IKEv2:Got um pacote do expedidor * 11 de novembro 20:28:34.003: IKEv2: Processando um artigo fora da fila de pak * 11 de novembro 19:30:34.811: Chave preshared de obtenção de IKEv2:% pelo endereço 10.0.0.2 * 11 de novembro 19:30:34.811: Proposta PHASE1-prop IKEv2:Adding ao policyle do conjunto de ferramentas * 11 de novembro 19:30:34.811: IKEv2:(1): Escolhendo o perfil IKEV2-SETUP IKE * 11 de novembro 19:30:34.811: Pedido ikev2 sa IKEv2:New admitido * 11 de novembro 19:30:34.811: Contagem de negócio que parte sa IKEv2:Incrementing por uma	
O primeiro par de mensagens é a troca IKE_SA_INIT. Estas mensagens negociam algoritmos criptográficos, nonces da troca, e fazem um intercâmbio Diffie-Hellman. **Configuração relevante:** `telecontrole local Cisco da chave pré-compartilhada de Cisco ikev2 da chave pré-compartilhada cripto cripto do hostname host1 de 10.0.0.2 255.255.255.0 do endereço do par peer1 do keyring ikev2 KEYRNG do grupo2 da integridade sha1 da`	* 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento INATIVO: EV_INIT_SA * 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento I_BLD_INIT: EV_GET_IKE_POLICY * 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento I_BLD_INIT: **EV_SET_POLICY** * 11 de novembro 19:30:34.811: Políticas configuradas 1):Setting IKEv2:(SA ID= * 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento I_BLD_INIT: EV_CHK_AUTH4PKI * 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento I_BLD_INIT: **EV_GEN_DH_KEY** * 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000	

CurState: Evento I_BLD_INIT: EV_NO_EVENT
* 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000
CurState: Evento I_BLD_INIT: EV_OK_RECD_DH_PUBKEY_RESP
* 11 de novembro 19:30:34.811: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000
CurState: Evento I_BLD_INIT: EV_GET_CONFIG_MODE

`criptografia 3des aes-cbc-128 da proposta PHASE1-prop`

* 11 de novembro 19:30:34.811: Iniciador IKEv2:IKEv2 - nenhuns dados da configuração a enviar na troca IKE_SA_INIT
* 11 de novembro 19:30:34.811: Dados da configuração IKEv2:No a enviar ao conjunto de ferramentas:
* 11 de novembro 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000
CurState: Evento I_BLD_INIT: EV_BLD_MSG
* 11 de novembro 19:30:34.811: Payload específico do vendedor IKEv2:Construct: DELETE-REASON
* 11 de novembro 19:30:34.811: Payload específico do vendedor IKEv2:Construct: (COSTUME)
* 11 de novembro 19:30:34.811: IKEv2:Construct notificam o payload: NAT_DETECTION_SOURCE_IP
* 11 de novembro 19:30:34.811: IKEv2:Construct notificam o payload: NAT_DETECTION_DESTINATION_IP
* 11 de novembro 19:30:34.811: Payload **IKEv2:(SA ID= 1):Next**: SA, versão: 2.0 Tipo da troca: **IKE_SA_INIT,** bandeiras: ID de mensagem do **INICIADOR**: 0, comprimento: 344
Índices do payload:
Payload seguinte **SA**: KE, reservado: 0x0, comprimento: 56
última proposta: 0x0, reservado: 0x0, comprimento: 52
Proposta: 1, ID de protocolo: IKE, tamanho SPI: 0, #trans: o último 5 transforma: 0x3, reservado: 0x0: comprimento: 8
tipo: 1, reservado: 0x0, identificação: 3DES
último transforme: 0x3, reservado: 0x0: comprimento: 12
tipo: 1, reservado: 0x0, identificação: AES-CBC
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 2, reservado: 0x0, identificação: SHA1
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA96
último transforme: 0x0, reservado: 0x0: comprimento: 8
tipo: 4, reservado: 0x0, identificação: DH_GROUP_1024_MODP/Group 2
Payload seguinte **KE**: N, reservado: 0x0, comprimento: 136
Grupo DH: 2, reservado: 0x0
Payload seguinte N: VID, reservado: 0x0, comprimento: 24

Iniciador que constrói o pacote IKE_INIT_SA. Contém: Encabeçamento ISAKMP (SPI/version/flags), SAi1 (algoritmo criptográfico que apoios do iniciador IKE), KEi (valor de chave pública DH do iniciador), e N (nonce do iniciador).

Payload seguinte VID: VID, reservado: 0x0, comprimento: 23
Payload seguinte VID: NOTIFIQUE, reservou: 0x0, comprimento: 21
Payload seguinte NOTIFY(NAT_DETECTION_SOURCE_IP): NOTIFIQUE, reservou: 0x0, comprimento: 28
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_SOURCE_IP
Payload seguinte NOTIFY(NAT_DETECTION_DESTINATION_IP): NENHUNS, reservado: 0x0, comprimento: 28
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_DESTINATION_IP
* 11 de novembro 19:30:34.814: IKEv2:Got um pacote do expedidor
* 11 de novembro 19:30:34.814: IKEv2:Processing um artigo fora da fila de pak
* 11 de novembro 19:30:34.814: Pedido ikev2 sa IKEv2:New admitido
* 11 de novembro 19:30:34.814: Contagem de negócio entrante sa IKEv2:Incrementing por uma
* 11 de novembro 19:30:34.814: Payload IKEv2:Next: SA, versão: 2.0 Tipo da troca: IKE_SA_INIT, bandeiras: ID de mensagem do INICIADOR: 0, comprimento: 344
Índices do payload:
Payload seguinte SA: KE, reservado: 0x0, comprimento: 56
última proposta: 0x0, reservado: 0x0, comprimento: 52
Proposta: 1, ID de protocolo: IKE, tamanho SPI: 0, #trans: o último 5 transforma: 0x3, reservado: 0x0: comprimento: 8
tipo: 1, reservado: 0x0, identificação: 3DES
último transforme: 0x3, reservado: 0x0: comprimento: 12
tipo: 1, reservado: 0x0, identificação: AES-CBC
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 2, reservado: 0x0, identificação: SHA1
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA96
último transforme: 0x0, reservado: 0x0: comprimento: 8
tipo: 4, reservado: 0x0, identificação: DH_GROUP_1024_MODP/Group 2
Payload seguinte KE: N, reservado: 0x0, comprimento: 136
Grupo DH: 2, reservado: 0x0
Payload seguinte N: VID, reservado: 0x0, comprimento: 24

* 11 de novembro 19:30:34.814: Payload específico do vendedor IKEv2:Parse: Payload seguinte CISCO-DELETE-REASON VID: VID, reservado: 0x0, comprimento: 23
* 11 de novembro 19:30:34.814: Payload específico do vendedor IKEv2:Parse: (COSTUME) payload seguinte VID: NOTIFIQUE, reservou: 0x0, comprimento: 21
* 11 de novembro 19:30:34.814: IKEv2:Parse notificam o

O que responde recebe IKE_INIT_SA.

O que responde inicia a criação SA para esse par.

payload: Payload
seguinte NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_SOURCE_IP): NOTIFIQUE,
reservou: 0x0, comprimento: 28
   Identificação do protocolo de segurança: IKE, tamanho
do spi: 0, tipo: NAT_DETECTION_SOURCE_IP
* 11 de novembro 19:30:34.814: IKEv2:Parse notificam o
payload: Payload
seguinte NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP):
NENHUNS, reservado: 0x0, comprimento: 28
   Identificação do protocolo de segurança: IKE, tamanho
do spi: 0, tipo: NAT_DETECTION_DESTINATION_IP
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento INATIVO: **EV_RECV_INIT**
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_INIT: **EV_VERIFY_MSG**
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_INIT: **EV_INSERT_SA**
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_INIT: **EV_GET_IKE_POLICY**
* 11 de novembro 19:30:34.814: Padrão da proposta
IKEv2:Adding à política do conjunto de ferramentas
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_INIT: **EV_PROC_MSG**
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_INIT: EV_DETECT_NAT
* 11 de novembro 19:30:34.814: A descoberta IKEv2:(SA
ID= 1):Process NAT notifica
* 11 de novembro 19:30:34.814: IKEv2:(SA ID=
1):Processing nat detectam o src para notificar
* 11 de novembro 19:30:34.814: Endereço IKEv2:(SA ID=
1):Remote combinado
* 11 de novembro 19:30:34.814: IKEv2:(SA ID=
1):Processing nat detectam o dst para notificar
* 11 de novembro 19:30:34.814: Endereço IKEv2:(SA ID=
1):Local combinado
* 11 de novembro 19:30:34.814: IKEv2:(SA ID= 1):No NAT
encontrado
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B

O que responde verifica e processa a mensagem IKE_INIT: (1) escolhem a série cripto daquelas oferecidas pelo iniciador, (2) computam sua própria chave secreta DH, e (3) computa um valor do skeyid, de que todas as chaves podem ser derivadas para este IKE_SA. Todos mas os encabeçamentos de todas as mensagens que seguem são cifrados e autenticados. As chaves usadas para a proteção da criptografia e da integridade são derivadas de SKEYID e sabidas como: SK_e (criptografia), SK_a (autenticação), SK_d é derivado e usado para a derivação de um material de ajuste mais adicional para CHILD_SAs, e um SK_e e um SK_a

R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_INIT: EV_CHK_CONFIG_MODE
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT: EV_SET_POLICY
* 11 de novembro 19:30:34.814: IKEv2:(SA ID= 1):
Ajustando políticas configuradas
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT: EV_CHK_AUTH4PKI
* 11 de novembro 19:30:34.814: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT: EV_PKI_SESH_OPEN
* 11 de novembro 19:30:34.814: IKEv2:(SA ID= 1):Opening uma sessão PKI
* 11 de novembro 19:30:34.815: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT: **EV_GEN_DH_KEY**
* 11 de novembro 19:30:34.815: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT: EV_NO_EVENT
* 11 de novembro 19:30:34.815: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT:
EV_OK_RECD_DH_PUBKEY_RESP
* 11 de novembro 19:30:34.815: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de novembro 19:30:34.815: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT: **EV_GEN_DH_SECRET**
* 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT: EV_NO_EVENT
* 11 de novembro 19:30:34.822: **Chave preshared de obtenção de** IKEv2:% pelo **endereço 10.0.0.1**
* 11 de novembro 19:30:34.822: Padrão da proposta IKEv2:Adding à política do conjunto de ferramentas
* 11 de novembro 19:30:34.822: IKEv2:(2): Escolhendo o perfil IKEV2-SETUP IKE
* 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Evento R_BLD_INIT:
EV_OK_RECD_DH_SECRET_RESP
* 11 de novembro 19:30:34.822: IKEv2:(SA ID= 1):Action:

separados são computados para cada sentido.
Configuração relevante: `telecontrole local Cisco da chave pré-compartilhada de Cisco ikev2 da chave pré-compartilhada cripto cripto do hostname host2 de 10.0.0.1 255.255.255.0 do endereço do par peer2 do keyring ikev2 KEYRNG do grupo2 da integridade sha1 da criptografia 3des aes-cbc-128 da proposta PHASE1-prop`

Action_Null
* 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: **EV_GEN_SKEYID**
* 11 de novembro 19:30:34.822: IKEv2:(SA ID= 1): **Gerencia o skeyid**
* 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GET_CONFIG_MODE
* 11 de novembro 19:30:34.822: Que responde IKEv2:IKEv2 - nenhuns dados da configuração a enviar na troca IKE_SA_INIT
* 11 de novembro 19:30:34.822: Dados da configuração IKEv2:No a enviar ao conjunto de ferramentas:
* 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_BLD_MSG
* 11 de novembro 19:30:34.822: Payload específico do vendedor IKEv2:Construct: DELETE-REASON
* 11 de novembro 19:30:34.822: Payload específico do vendedor IKEv2:Construct: (COSTUME)
* 11 de novembro 19:30:34.822: IKEv2:Construct notificam o payload: NAT_DETECTION_SOURCE_IP
* 11 de novembro 19:30:34.822: IKEv2:Construct notificam o payload: NAT_DETECTION_DESTINATION_IP
* 11 de novembro 19:30:34.822: IKEv2:Construct notificam o payload: HTTP_CERT_LOOKUP_SUPPORTED
* 11 de novembro 19:30:34.822: Payload IKEv2:(SA ID= 1):Next: SA, versão: 2.0 Tipo da troca: **IKE_SA_INIT,** bandeiras: ID de mensagem do **QUE RESPONDE MSG-RESPONSE**: 0, comprimento: 449
Índices do payload:
 Payload seguinte **SA**: KE, reservado: 0x0, comprimento: 48
  última proposta: 0x0, reservado: 0x0, comprimento: 44
  Proposta: 1, ID de protocolo: IKE, tamanho SPI: 0, #trans: o último 4 transforma: 0x3, reservado: 0x0: comprimento: 12
    tipo: 1, reservado: 0x0, identificação: AES-CBC
    último transforme: 0x3, reservado: 0x0: comprimento: 8
    tipo: 2, reservado: 0x0, identificação: SHA1
    último transforme: 0x3, reservado: 0x0: comprimento: 8
    tipo: 3, reservado: 0x0, identificação: SHA96
    último transforme: 0x0, reservado: 0x0: comprimento: 8
    tipo: 4, reservado: 0x0, identificação: DH_GROUP_1024_MODP/Group 2
 Payload seguinte **KE**: N, reservado: 0x0, comprimento: 136
    Grupo DH: 2, reservado: 0x0
 Payload seguinte **N**: VID, reservado: 0x0, comprimento: 24

O roteador2 constrói a mensagem do que responde para a troca IKE_SA_INIT, que é recebida por ASA1. Este pacote contém: Encabeçamento ISAKMP (versão/bandeiras SPI/), algoritmo SAr1(cryptographic que o que responde IKE escolhe), KEr (valor de chave pública DH do que responde), e nonce do que responde.

	Payload seguinte VID: VID, reservado: 0x0, comprimento: 23 Payload seguinte VID: NOTIFIQUE, reservou: 0x0, comprimento: 21 Payload seguinte NOTIFY(NAT_DETECTION_SOURCE_IP): NOTIFIQUE, reservou: 0x0, comprimento: 28 Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_SOURCE_IP Payload seguinte NOTIFY(NAT_DETECTION_DESTINATION_IP): CERTREQ, reservado: 0x0, comprimento: 28 Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_DESTINATION_IP Payload seguinte CERTREQ: NOTIFIQUE, reservou: 0x0, comprimento: 105 Mistura da codificação CERT e URL de PKIX Payload seguinte NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED): NENHUNS, reservado: 0x0, comprimento: 8 Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: HTTP_CERT_LOOKUP_SUPPORTED * 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento INIT_DONE: EV_DONE * 11 de novembro 19:30:34.822: IKEv2:(SA ID= 1):Cisco DeleteReason Notify é permitido * 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento INIT_DONE: EV_CHK4_ROLE * 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento INIT_DONE: **EV_START_TMR** * 11 de novembro 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento R_WAIT_AUTH: EV_NO_EVENT * 11 de novembro 19:30:34.822: IKEv2: **Pedido novo ikev2 sa admitido** * 11 de novembro 19:30:34.822: IKEv2: **Incrementando contagem de negócio que parte sa por uma**		O roteador2 manda a mensagem do que responde ao roteador1.
O roteador1 recebe o pacote de resposta IKE_SA_INIT do roteador2.	* 11 de novembro 19:30:34.823: IKEv2:Got um pacote do expedidor * 11 de novembro 19:30:34.823: IKEv2:Got um pacote do expedidor * 11 de novembro	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento INIT_DONE: **EV_START_TMR**	O que responde começa o temporizador para o processo do AUTH.

19:30:34.823:
IKEv2:Processing um artigo
fora da fila de pak
* 11 de novembro 19:30:34.823: Payload IKEv2:(SA ID=
1):Next: SA, versão: 2.0 Tipo da troca: IKE_SA_INIT,
bandeiras: ID de mensagem do **QUE RESPONDE MSG-RESPONSE**: 0, comprimento: 449
Índices do payload:
Payload seguinte **SA**: KE, reservado: 0x0, comprimento:
48
última proposta: 0x0, reservado: 0x0, comprimento: 44
Proposta: 1, ID de protocolo: IKE, tamanho SPI: 0, #trans:
o último 4 transforma: 0x3, reservado: 0x0: comprimento:
12
tipo: 1, reservado: 0x0, identificação: AES-CBC
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 2, reservado: 0x0, identificação: SHA1
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA96
último transforme: 0x0, reservado: 0x0: comprimento: 8
tipo: 4, reservado: 0x0, identificação:
DH_GROUP_1024_MODP/Group 2
Payload seguinte **KE**: N, reservado: 0x0, comprimento:
136
Grupo DH: 2, reservado: 0x0
Payload seguinte **N**: VID, reservado: 0x0, comprimento: 24

O roteador1 verifica e processa a resposta: (1) a chave secreta do iniciador DH é computada, e (2) o skeyid do iniciador é gerado igualmente.

* 11 de novembro 19:30:34.823: Payload específico do vendedor IKEv2:Parse: Payload seguinte CISCO-DELETE-REASON VID: VID, reservado: 0x0, comprimento: 23

* 11 de novembro 19:30:34.823: Payload específico do vendedor IKEv2:Parse: (COSTUME) payload seguinte VID: NOTIFIQUE, reservou: 0x0, comprimento: 21

* 11 de novembro 19:30:34.823: IKEv2:Parse notificam o payload: Payload
seguinte NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_SOURCE_IP): NOTIFIQUE,
reservou: 0x0, comprimento: 28
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_SOURCE_IP

* 11 de novembro 19:30:34.824: IKEv2:Parse notificam o payload: Payload
seguinte NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP):
CERTREQ, reservado: 0x0, comprimento: 28
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NAT_DETECTION_DESTINATION_IP
Payload seguinte CERTREQ: NOTIFIQUE, reservou: 0x0, comprimento: 105
Mistura da codificação CERT e URL de PKIX

* 11 de novembro 19:30:34.824: IKEv2:Parse notificam o payload: Payload
seguinte HTTP_CERT_LOOKUP_SUPPORTED
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED):
NENHUNS, reservado: 0x0, comprimento: 8
    Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: HTTP_CERT_LOOKUP_SUPPORTED
* 11 de novembro 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_WAIT_INIT: EV_RECV_INIT
* 11 de novembro 19:30:34.824: Mensagem IKEv2:(SA ID= 1):Processing IKE_SA_INIT
* 11 de novembro 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_CHK4_NOTIFY
* 11 de novembro 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_VERIFY_MSG
* 11 de novembro 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_PROC_MSG
* 11 de novembro 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_DETECT_NAT
* 11 de novembro 19:30:34.824: A descoberta IKEv2:(SA ID= 1):Process NAT notifica
* 11 de novembro 19:30:34.824: IKEv2:(SA ID= 1):Processing nat detectam o src para notificar
* 11 de novembro 19:30:34.824: Endereço IKEv2:(SA ID= 1):Remote combinado
* 11 de novembro 19:30:34.824: IKEv2:(SA ID= 1):Processing nat detectam o dst para notificar
* 11 de novembro 19:30:34.824: Endereço IKEv2:(SA ID= 1):Local combinado
* 11 de novembro 19:30:34.824: IKEv2:(SA ID= 1):No NAT encontrado
* 11 de novembro 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_CHK_NAT_T
* 11 de novembro 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_CHK_CONFIG_MODE
* 11 de novembro 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000

	CurState: Evento INIT_DONE: **EV_GEN_DH_SECRET** * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: EV_NO_EVENT * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: EV_OK_RECD_DH_SECRET_RESP * 11 de novembro 19:30:34.831: IKEv2:(SA ID= 1):Action: Action_Null * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: **EV_GEN_SKEYID** * 11 de novembro 19:30:34.831: IKEv2:(SA ID= 1): **Gerencia o skeyid** * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: EV_DONE * 11 de novembro 19:30:34.831: IKEv2:(SA ID= 1):Cisco DeleteReason Notify é permitido * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: EV_CHK4_ROLE * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_GET_CONFIG_MODE * 11 de novembro 19:30:34.831: Dados da configuração IKEv2:Sending ao conjunto de ferramentas * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_CHK_EAP
A troca dos começos IKE_AUTH do iniciador e gerencie o payload da autenticação. O pacote IKE_AUTH contém: O encabeçamento ISAKMP (versão/bandeiras SPI/), IDi (a identidade do iniciador), payload do AUTH,	* 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: **EV_GEN_AUTH** * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_CHK_AUTH_TYPE * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_OK_AUTH_GEN * 11 de novembro 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000

SAi2(initiates o SA-similar à fase 2 transforma a troca do grupo em IKEv1), e o TSi e o TSr (o iniciador e o que responde traficam os seletores): Contêm o endereço de rementente e destinatário do iniciador e do que responde respectivamente para enviar/que recebe o tráfego criptografado. A escala de endereço especifica que todo o tráfego a e dessa escala está escavado um túnel. Se a proposta é aceitável ao que responde, envia cargas úteis idênticas TS para trás. O primeiro CHILD_SA é criado para o par do proxy_ID que combina o pacote do disparador.

Configuração relevante:

```
conjunto de transformação ajustado cripto TS
ikev2-profile ajustado IKEV2-SETUP do perfil
IPSec phse2-prof do esp-sha-hmac cripto do esp-3des do
conjunto de transformação TS do IPsec
```

CurState: Evento I_BLD_AUTH: EV_SEND_AUTH
* 11 de novembro 19:30:34.831: Payload específico do vendedor IKEv2:Construct: CISCO-GRANITE
* 11 de novembro 19:30:34.831: IKEv2:Construct notificam o payload: INITIAL_CONTACT
* 11 de novembro 19:30:34.831: IKEv2:Construct notificam o payload: SET_WINDOW_SIZE
* 11 de novembro 19:30:34.831: IKEv2:Construct notificam o payload: ESP_TFC_NO_SUPPORT
* 11 de novembro 19:30:34.831: IKEv2:Construct notificam o payload: NON_FIRST_FRAGS
Índices do payload:
Payload seguinte VID: IDi, reservado: 0x0, comprimento: 20
Payload seguinte **IDi**: AUTH, reservado: 0x0, comprimento: 12
Tipo identificação: Endereço do IPv4, reservado: 0x0 0x0
Payload seguinte do **AUTH**: CFG, reservado: 0x0, comprimento: 28
Método PSK do AUTH, reservado: 0x0, 0x0 reservado
Payload seguinte **CFG**: SA, reservado: 0x0, comprimento: 309
tipo do cfg: CFG_REQUEST, reservado: 0x0, reservado: 0x0
* 11 de novembro 19:30:34.831: Payload seguinte SA: **TSi**, reservado: 0x0, comprimento: 40
última proposta: 0x0, reservado: 0x0, comprimento: 36
Proposta: 1, ID de protocolo: ESP, tamanho SPI: 4, #trans: o último 3 transforma: 0x3, reservado: 0x0: comprimento: 8
tipo: 1, reservado: 0x0, identificação: 3DES
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA96
último transforme: 0x0, reservado: 0x0: comprimento: 8
tipo: 5, reservado: 0x0, identificação: Não use ESN
Payload seguinte de **TSi**: TSr, reservado: 0x0, comprimento: 24
Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento: 16
porta do começo: 0, porta da extremidade: 65535
ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255
Payload seguinte de **TSr**: NOTIFIQUE, reservou: 0x0, comprimento: 24
Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento: 16
porta do começo: 0, porta da extremidade: 65535
ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255
Payload seguinte NOTIFY(INITIAL_CONTACT): NOTIFIQUE, reservou: 0x0, comprimento: 8
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: INITIAL_CONTACT

Payload seguinte NOTIFY(SET_WINDOW_SIZE): NOTIFIQUE, reservou: 0x0, comprimento: 12
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: SET_WINDOW_SIZE
Payload seguinte NOTIFY(ESP_TFC_NO_SUPPORT): NOTIFIQUE, reservou: 0x0, comprimento: 8
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: ESP_TFC_NO_SUPPORT
Payload seguinte NOTIFY(NON_FIRST_FRAGS): NENHUNS, reservado: 0x0, comprimento: 8
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NON_FIRST_FRAGS

* 11 de novembro 19:30:34.832: Payload IKEv2:(SA ID= 1):Next: ENCR, versão: 2.0 Tipo da troca: **IKE_AUTH**, bandeiras: ID de mensagem do **INICIADOR**: 1, comprimento: 556
Índices do payload:
Payload seguinte ENCR: VID, reservado: 0x0, comprimento: 528

* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 **CurState:** Evento **I_WAIT_AUTH**: EV_NO_EVENT
* 11 de novembro 19:30:34.832: IKEv2:Got um pacote do expedidor
* 11 de novembro 19:30:34.832: IKEv2:Processing um artigo fora da fila de pak
* 11 de novembro 19:30:34.832: IKEv2:(SA ID= 1):Request tem o mess_id 1; 1 previsto a 1
* 11 de novembro 19:30:34.832: Payload **IKEv2:(SA ID= 1):Next**: ENCR, versão: 2.0 Tipo da troca: **IKE_AUTH**, bandeiras: ID de mensagem do **INICIADOR**: 1, comprimento: 556
Índices do payload:
* 11 de novembro 19:30:34.832: Payload específico do vendedor IKEv2:Parse: (COSTUME) payload seguinte VID: IDi, reservado: 0x0, comprimento: 20
Payload seguinte **IDi**: AUTH, reservado: 0x0, comprimento: 12
Tipo identificação: Endereço do IPv4, reservado: 0x0 0x0
Payload seguinte do **AUTH**: CFG, reservado: 0x0, comprimento: 28
Método PSK do AUTH, reservado: 0x0, 0x0 reservado
Payload seguinte **CFG**: SA, reservado: 0x0, comprimento: 309
tipo do cfg: CFG_REQUEST, reservado: 0x0, reservado: 0x0
* 11 de novembro 19:30:34.832: tipo do attrib: IP4 interno DNS, comprimento: 0

O roteador2 recebe e verifica os dados de autenticação recebidos do roteador1.
Configuração relevante: `do IPsec ikev2 da IPsec-proposta AES256 do protocolo esp da criptografia do aes-256 do protocolo integridade cripto sha-1 md5 esp`

* 11 de novembro 19:30:34.832: tipo do attrib: IP4 interno DNS, comprimento: 0
* 11 de novembro 19:30:34.832: tipo do attrib: IP4 interno NBNS, comprimento: 0
* 11 de novembro 19:30:34.832: tipo do attrib: IP4 interno NBNS, comprimento: 0
* 11 de novembro 19:30:34.832: tipo do attrib: sub-rede IP4 interna, comprimento: 0
* 11 de novembro 19:30:34.832: tipo do attrib: versão de aplicativo, comprimento: 257
tipo do attrib: Desconhecido - 28675, comprimento: 0
* 11 de novembro 19:30:34.832: tipo do attrib: Desconhecido - 28672, comprimento: 0
* 11 de novembro 19:30:34.832: tipo do attrib: Desconhecido - 28692, comprimento: 0
* 11 de novembro 19:30:34.832: tipo do attrib: Desconhecido - 28681, comprimento: 0
* 11 de novembro 19:30:34.832: tipo do attrib: Desconhecido - 28674, comprimento: 0
* 11 de novembro 19:30:34.832: Payload seguinte **SA**: TSi, reservado: 0x0, comprimento: 40
última proposta: 0x0, reservado: 0x0, comprimento: 36
Proposta: 1, ID de protocolo: ESP, tamanho SPI: 4, #trans: o último 3 transforma: 0x3, reservado: 0x0: comprimento: 8
tipo: 1, reservado: 0x0, identificação: 3DES
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA96
último transforme: 0x0, reservado: 0x0: comprimento: 8
tipo: 5, reservado: 0x0, identificação: Não use ESN
Payload seguinte de **TSi**: TSr, reservado: 0x0, comprimento: 24
Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento: 16
porta do começo: 0, porta da extremidade: 65535
ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255
Payload seguinte de **TSr**: NOTIFIQUE, reservou: 0x0, comprimento: 24
Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento: 16
porta do começo: 0, porta da extremidade: 65535
ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255
* 11 de novembro 19:30:34.832: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_RECV_AUTH
* 11 de novembro 19:30:34.832: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001

O roteador2 constrói a resposta ao pacote IKE_AUTH que recebeu do roteador1. Este pacote de resposta

CurState: Evento R_WAIT_AUTH: EV_CHK_NAT_T
* 11 de novembro 19:30:34.832: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_PROC_ID
* 11 de novembro 19:30:34.832: Parameteres válidos IKEv2:(SA ID= 1):Received na identificação de processo
* 11 de novembro 19:30:34.832: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
* 11 de novembro 19:30:34.832: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_GET_POLICY_BY_PEERID
* 11 de novembro 19:30:34.833: IKEv2:(1): Escolhendo o perfil IKEV2-SETUP IKE
* 11 de novembro 19:30:34.833: Chave preshared de obtenção de IKEv2:% pelo endereço 10.0.0.1
* 11 de novembro 19:30:34.833: Chave preshared de obtenção de IKEv2:% pelo endereço 10.0.0.1
* 11 de novembro 19:30:34.833: Padrão da proposta IKEv2:Adding à política do conjunto de ferramentas
* 11 de novembro 19:30:34.833: Perfil 'IKEV2-SETUP IKEv2:(SA ID= 1):Using IKEv2
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_SET_POLICY
* 11 de novembro 19:30:34.833: Políticas configuradas 1):Setting IKEv2:(SA ID=
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_VERIFY_POLICY_BY_PEERID
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_CHK_AUTH4EAP
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_CHK_POLREQEAP
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_CHK_AUTH_TYPE
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA

contém: O encabeçamento ISAKMP (versão/bandeiras SPI/), IDr (a identidade do que responde), payload do AUTH, SAr2(initiates o SA-similar à fase 2 transforma a troca do grupo em IKEv1), e o TSi e o TSr (o iniciador e o que responde traficam os seletores). Contêm o endereço de rementente e destinatário do iniciador e do que responde respectivamente para enviar/que recebe o tráfego criptografado. A escala de endereço especifica que todo o tráfego a e dessa escala está escavado um túnel. Estes parâmetros são idênticos a esse que foi recebido de ASA1.

ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_GET_PRESHR_KEY
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_VERIFY_AUTH
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_CHK4_IC
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_CHK_REDIRECT
* 11 de novembro 19:30:34.833: A verificação IKEv2:(SA
ID= 1):Redirect não é precisada, saltando o
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_NOTIFY_AUTH_DONE
* 11 de novembro 19:30:34.833: A autorização do grupo
IKEv2:AAA não é configurada
* 11 de novembro 19:30:34.833: A autorização de usuário
IKEv2:AAA não é configurada
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_CHK_CONFIG_MODE
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_SET_RECD_CONFIG_MODE
* 11 de novembro 19:30:34.833: Dados da configuração
IKEv2:Received do conjunto de ferramentas:
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_PROC_SA_TS
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_GET_CONFIG_MODE
* 11 de novembro 19:30:34.833: IKEv2:Error que constrói a
resposta da configuração
* 11 de novembro 19:30:34.833: Dados da configuração
IKEv2:No a enviar ao conjunto de ferramentas:
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA

ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_MY_AUTH_METHOD
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_GET_PRESHR_KEY
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_GEN_AUTH
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_CHK4_SIGN
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_OK_AUTH_GEN
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_SEND_AUTH
* 11 de novembro 19:30:34.833: Payload específico do
vendedor IKEv2:Construct: CISCO-GRANITE
* 11 de novembro 19:30:34.833: IKEv2:Construct notificam
o payload: SET_WINDOW_SIZE
* 11 de novembro 19:30:34.833: IKEv2:Construct notificam
o payload: ESP_TFC_NO_SUPPORT
* 11 de novembro 19:30:34.833:
IKEv2:Construct notificam o payload: NON_FIRST_FRAGS
* 11 de novembro 19:30:34.833: Payload IKEv2:(SA ID=
1):Next: ENCR, versão: 2.0 Tipo da
troca: **IKE_AUTHENTIC**, bandeiras: ID de mensagem do
QUE RESPONDE MSG-RESPONSE: 1, comprimento:
252
Índices do payload:
Payload seguinte **ENCR**: VID, reservado: 0x0,
comprimento: 224
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento AUTH_DONE: EV_OK
* 11 de novembro 19:30:34.833: IKEv2:(SA ID= 1):Action:
Action_Null
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Evento AUTH_DONE: EV_PKI_SESH_CLOSE
* 11 de novembro 19:30:34.833: IKEv2:(SA ID= 1):Closing
a sessão PKI
* 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B

O que responde envia a resposta para IKE_AUTH.

	R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_UPDATE_CAC_STATS * 11 de novembro 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento AUTH_DONE: **EV_INSERT_IKE** * 11 de novembro 19:30:34.834: Deslocamento predeterminado ikev2 1 MIB IKEv2:Store, plataforma 60 * 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_GEN_LOAD_IPSEC * 11 de novembro 19:30:34.834: Pedido IKEv2:(SA ID= 1):Asynchronous enfileirado * 11 de novembro 19:30:34.834: IKEv2:(SA ID= 1): * 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento **AUTH_DONE**: EV_NO_EVENT		
		* 11 de novembro 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_OK_RECD_LOAD_IPSEC * 11 de novembro 19:30:34.840: IKEv2:(SA ID= 1):Action: Action_Null	
O iniciador recebe a resposta do que responde.	* 11 de novembro 19:30:34.834: IKEv2:Got um pacote do expedidor * 11 de novembro 19:30:34.834: IKEv2:Processing um artigo fora da fila de pak	* 11 de novembro 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_START_ACCT * 11 de novembro 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_CHECK_DUPE * 11 de novembro 19:30:34.840: Trace-> SA	O que responde introduz uma entrada no TRISTE.

IKEv2:(SA ID= 1):SM:
I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C
4 (R) MsgID = 00000001
CurState: Evento
AUTH_DONE:
EV_CHK4_ROLE

* 11 de novembro 19:30:34.834: Payload IKEv2:(SA ID= 1):Next: ENCR, versão: 2.0 Tipo da troca: **IKE_AUTH**, bandeiras: ID de mensagem do **QUE RESPONDE MSG-RESPONSE**: 1, comprimento: 252
Índices do payload:

* 11 de novembro 19:30:34.834: Payload específico do vendedor IKEv2:Parse: (COSTUME) payload seguinte VID: IDr, reservado: 0x0, comprimento: 20
Payload seguinte **IDr**: AUTH, reservado: 0x0, comprimento: 12
Tipo identificação: Endereço do IPv4, reservado: 0x0 0x0
Payload seguinte do **AUTH**: SA, reservado: 0x0, comprimento: 28
Método PSK do AUTH, reservado: 0x0, 0x0 reservado
Payload seguinte **SA**: TSi, reservado: 0x0, comprimento: 40
última proposta: 0x0, reservado: 0x0, comprimento: 36
Proposta: 1, ID de protocolo: ESP, tamanho SPI: 4, #trans: o último 3 transforma: 0x3, reservado: 0x0: comprimento: 8
tipo: 1, reservado: 0x0, identificação: 3DES
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA96
último transforme: 0x0, reservado: 0x0: comprimento: 8
tipo: 5, reservado: 0x0, identificação: Não use ESN
Payload seguinte de **TSi**: TSr, reservado: 0x0, comprimento: 24
Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento: 16
porta do começo: 0, porta da extremidade: 65535
ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255
Payload seguinte de **TSr**: NOTIFIQUE, reservou: 0x0, comprimento: 24
Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento: 16
porta do começo: 0, porta da extremidade: 65535
ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255

O roteador1 verifica e processa os dados de autenticação neste pacote. O roteador1 introduz então este SA no seu TRISTE.

* 11 de novembro 19:30:34.834: IKEv2:Parse notificam o payload: Payload seguinte SET_WINDOW_SIZE

NOTIFY(SET_WINDOW_SIZE): NOTIFIQUE, reservou: 0x0, comprimento: 12
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: SET_WINDOW_SIZE

* 11 de novembro 19:30:34.834: IKEv2:Parse notificam o payload: Payload seguinte ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT): NOTIFIQUE, reservou: 0x0, comprimento: 8
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: ESP_TFC_NO_SUPPORT

* 11 de novembro 19:30:34.834: IKEv2:Parse notificam o payload: Payload seguinte NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS): NENHUNS, reservado: 0x0, comprimento: 8
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: NON_FIRST_FRAGS

* 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_WAIT_AUTH: EV_RECV_AUTH
* 11 de novembro 19:30:34.834: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK4_NOTIFY
* 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_PROC_MSG
* 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
* 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_GET_POLICY_BY_PEERID
* 11 de novembro 19:30:34.834: Proposta PHASE1-prop IKEv2:Adding à política do conjunto de ferramentas
* 11 de novembro 19:30:34.834: Perfil 'IKEV2-SETUP IKEv2:(SA ID= 1):Using IKEv2
* 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_VERIFY_POLICY_BY_PEERID

* 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH: EV_CHK_AUTH_TYPE
* 11 de novembro 19:30:34.834: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH: EV_GET_PRESHR_KEY
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH: EV_VERIFY_AUTH
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH: EV_CHK_EAP
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH:
EV_NOTIFY_AUTH_DONE
* 11 de novembro 19:30:34.835: A autorização do grupo
IKEv2:AAA não é configurada
* 11 de novembro 19:30:34.835: A autorização de usuário
IKEv2:AAA não é configurada
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH:
EV_CHK_CONFIG_MODE
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH: EV_CHK4_IC
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH: EV_CHK_IKE_ONLY
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento I_PROC_AUTH: EV_PROC_SA_TS
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento AUTH_DONE: EV_OK
* 11 de novembro 19:30:34.835: IKEv2:(SA ID= 1):Action:
Action_Null
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState: Evento AUTH_DONE: EV_PKI_SESH_CLOSE
* 11 de novembro 19:30:34.835: IKEv2:(SA ID= 1):Closing

a sessão PKI
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_UPDATE_CAC_STATS
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_INSERT_IKE
* 11 de novembro 19:30:34.835: Deslocamento predeterminado ikev2 1 MIB IKEv2:Store, plataforma 60
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_GEN_LOAD_IPSEC
* 11 de novembro 19:30:34.835: Pedido IKEv2:(SA ID= 1):Asynchronous enfileirado

* 11 de novembro 19:30:34.835: IKEv2:(SA ID= 1):
* 11 de novembro 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_NO_EVENT
* 11 de novembro 19:30:34.835: Mensagem 8 IKEv2:KMI consumida. Nenhuma ação tomada.
* 11 de novembro 19:30:34.835: Mensagem 12 IKEv2:KMI consumida. Nenhuma ação tomada.
* 11 de novembro 19:30:34.835: Dados IKEv2:No a enviar no grupo do config de modo.
* 11 de novembro 19:30:34.841: Punho 0x80000002 identificação IKEv2:Adding associado com o SPI 0x9506D414 para a sessão 8

* 11 de novembro 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_OK_RECD_LOAD_IPSEC
* 11 de novembro 19:30:34.841: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de novembro 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_START_ACCT
* 11 de novembro 19:30:34.841: IKEv2:(SA ID= 1):Accounting não exigido
* 11 de novembro 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_CHECK_DUPE
* 11 de novembro 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B

	R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento **AUTH_DONE**: EV_CHK4_ROLE		
O túnel está acima no iniciador e no showsREADY do estado.	* 11 de novembro 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C 4 (i) MsgID = 00000001 CurState: **READYEvent**: EV_CHK_IKE_ONLY * 11 de novembro 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C 4 (i) MsgID = 00000001 CurState: Evento PRONTO: EV_I_OK	***** 11 de novembro 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C 4 (R) MsgID = 00000001 CurState: Evento **PRONTO**: EV_R_OK * 11 de novembro 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C 4 (R) MsgID = 00000001 CurState: Evento PRONTO: EV_NO_EVENT	O túnel está acima no que responde. O túnel do que responde vem geralmente acima antes do iniciador.

CHILD_SA debuga

Esta troca consiste em um único par do pedido/resposta e foi referida como uma troca da fase 2 em IKEv1. Pôde ser iniciada por um ou outro fim do IKE_SA depois que as trocas iniciais são terminadas.

Descrição de mensagem do roteador1 CHILD_SA	**Debugs**	**Descrição de mensagem do roteador2 CHILD_SA**
O roteador1 inicia a troca CHILD_SA. Este é o pedido CREATE_CHILD_SA. O pacote CHILD_SA contém tipicamente: • SA HDR (version.flags/tipo da troca) • Ni do nonce (opcional): Se o CHILD_SA é criado como parte da troca inicial, um segundo payload e o nonce KE não devem ser enviados)	* 11 de novembro 19:31:35.873: IKEv2:Got um pacote do expedidor * 11 de novembro 19:31:35.873: IKEv2:Processing um artigo fora da fila de pak * 11 de novembro 19:31:35.873: IKEv2:(SA ID= 2):Request tem o mess_id 3; 3 previstos com 7 * 11 de novembro 19:31:35.873: Payload IKEv2:(SA ID= 2):Next: ENCR, versão: 2.0 **Tipo da troca: CREATE_CHILD_SA**, bandeiras: ID de mensagem do **INICIADOR**: 3, comprimento: 396 Índices do payload: Payload seguinte **SA**: N, reservado: 0x0, comprimento: 152 última proposta: 0x0, reservado: 0x0, comprimento: 148 Proposta: 1, ID de protocolo: IKE, tamanho SPI: 8, #trans: o último 15 transforma: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, identificação: AES-CBC último transforme: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, identificação: AES-CBC	

- Payload SA
- KEi (Chave-opcional): O pedido CREATE_CHILD_SA pôde opcionalmente conter um payload KE para que uma troca adicional DH permita umas garantias mais fortes do secretismo dianteiro para o CHILD_SA. Se as ofertas SA incluem grupos diferentes DH, KEi deve ser um elemento do grupo que o iniciador espera o que responde aceitar. Se supõe erradamente, a troca CREATE_CHILD_SA falha, e terá que experimentar de novo com um KEi diferente
- N (notifique payload-opcional). O payload da notificação, é usado para transmitir dados informativos,

último transforme: 0x3, reservado: 0x0: comprimento: 12
tipo: 1, reservado: 0x0, identificação: AES-CBC
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 2, reservado: 0x0, identificação: SHA512
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 2, reservado: 0x0, identificação: SHA384
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 2, reservado: 0x0, identificação: SHA256
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 2, reservado: 0x0, identificação: SHA1
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 2, reservado: 0x0, identificação: MD5
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA512
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA384
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA256
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: SHA96
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 3, reservado: 0x0, identificação: MD596
último transforme: 0x3, reservado: 0x0: comprimento: 8
tipo: 4, reservado: 0x0, identificação: DH_GROUP_1536_MODP/Group 5
último transforme: 0x0, reservado: 0x0: comprimento: 8
tipo: 4, reservado: 0x0, identificação: DH_GROUP_1024_MODP/Group 2
Payload seguinte **N**: KE, reservado: 0x0, comprimento: 24
Payload seguinte **KE**: NOTIFIQUE, reservou: 0x0, comprimento: 136
Grupo DH: 2, reservado: 0x0

* 11 de novembro 19:31:35.874: IKEv2:Parse notificam o payload: Payload seguinte SET_WINDOW_SIZE **NOTIFY(SET_WINDOW_SIZE)**: NENHUNS, reservado: 0x0, comprimento: 12
Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: SET_WINDOW_SIZE

* 11 de novembro 19:31:35.874: IKEv2: (Trace-> SA **SA ID= 2):SM**: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento PRONTO: **EV_RECV_CREATE_CHILD**
* 11 de novembro 19:31:35.874: IKEv2:(SA ID= 2):Action: Action_Null
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_INIT: EV_RECV_CREATE_CHILD
* 11 de novembro 19:31:35.874: IKEv2:(SA ID= 2):Action: Action_Null

tais como condições de erro e transições de estado, a um par IKE. Um payload da notificação pode aparecer em um mensagem de resposta (que especifica geralmente porque um pedido foi rejeitado), em uma troca INFORMATIVA (para relatar um erro não em um pedido IKE), ou em toda a outra mensagem para indicar capacidades do remetente ou para alterar o significado do pedido. Se esta troca CREATE_CHILD_SA rekeying um SA existente a não ser o IKE_SA, o payload principal N do tipo REKEY_SA DEVE identificar o SA que está sendo rekeyed. Se esta troca CREATE_CHIL

* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_INIT: EV_VERIFY_MSG
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_INIT: EV_CHK_CC_TYPE
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_IKE: **EV_REKEY_IKESA**
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_IKE: EV_GET_IKE_POLICY
* 11 de novembro 19:31:35.874: **Chave preshared de obtenção de** IKEv2:% pelo **endereço 10.0.0.2**
* 11 de novembro 19:31:35.874: Chave preshared de obtenção de IKEv2:% pelo endereço 10.0.0.2
* 11 de novembro 19:31:35.874: Proposta PHASE1-prop IKEv2:Adding à política do conjunto de ferramentas
* 11 de novembro 19:31:35.874: Perfil 'IKEV2-SETUP IKEv2:(SA ID= 2):Using IKEv2
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_IKE: EV_PROC_MSG
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_IKE: EV_SET_POLICY
* 11 de novembro 19:31:35.874: IKEv2:(SA ID= 2): **Ajustando políticas configuradas**
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: EV_GEN_DH_KEY
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: EV_NO_EVENT
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: EV_OK_RECD_DH_PUBKEY_RESP
* 11 de novembro 19:31:35.874: IKEv2:(SA ID= 2):Action: Action_Null
* 11 de novembro 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003

	CurState: Evento CHILD_R_BLD_MSG: **EV_GEN_DH_SECRET** * 11 de novembro 19:31:35.881: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: EV_NO_EVENT * 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: EV_OK_RECD_DH_SECRET_RESP * 11 de novembro 19:31:35.882: IKEv2:(SA ID= 2):Action: Action_Null * 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: EV_BLD_MSG * 11 de novembro 19:31:35.882: **IKEv2:Construct notificam o payload**: SET_WINDOW_SIZE Índices do payload: Payload seguinte **SA**: N, reservado: 0x0, comprimento: 56 última proposta: 0x0, reservado: 0x0, comprimento: 52 Proposta: 1, ID de protocolo: IKE, tamanho SPI: 8, #trans: o último 4 transforma: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, identificação: AES-CBC último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, identificação: SHA1 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, identificação: SHA96 último transforme: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, identificação: DH_GROUP_1024_MODP/Group 2 Payload seguinte **N**: KE, reservado: 0x0, comprimento: 24 Payload seguinte **KE**: NOTIFIQUE, reservou: 0x0, comprimento: 136 Grupo DH: 2, reservado: 0x0 Payload seguinte **NOTIFY(SET_WINDOW_SIZE)**: NENHUNS, reservado: 0x0, comprimento: 12 Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: SET_WINDOW_SIZE
D_SA não rekeying um SA existente, o payload N DEVE ser omitido.	
	* 11 de novembro 19:31:35.869: IKEv2: (Payload **SA ID= 2):Next**: ENCR, versão: 2.0 Tipo da troca: **CREATE_CHILD_SA**, bandeiras: ID de mensagem do **INICIADOR**: 2, comprimento: 460 Índices do payload: Payload seguinte ENCR: SA, reservado: 0x0, comprimento: 432 * 11 de novembro 19:31:35.873: IKEv2:Construct notificam o payload: SET_WINDOW_SIZE Índices do payload: Payload seguinte **SA**: N, reservado: 0x0, comprimento: 152
	Este pacote é recebido pelo roteador2.

última proposta: 0x0, reservado: 0x0, comprimento: 148 Proposta: 1, ID de protocolo: IKE, tamanho SPI: 8, #trans: o último 15 transforma: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, identificação: AES-CBC último transforme: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, identificação: AES-CBC último transforme: 0x3, reservado: 0x0: comprimento: 12 tipo: 1, reservado: 0x0, identificação: AES-CBC último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, identificação: SHA512 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, identificação: SHA384 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, identificação: SHA256 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, identificação: SHA1 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 2, reservado: 0x0, identificação: MD5 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, identificação: SHA512 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, identificação: SHA384 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, identificação: SHA256 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, identificação: SHA96 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 3, reservado: 0x0, identificação: MD596 último transforme: 0x3, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, identificação: DH_GROUP_1536_MODP/Group 5 último transforme: 0x0, reservado: 0x0: comprimento: 8 tipo: 4, reservado: 0x0, identificação: DH_GROUP_1024_MODP/Group 2 Payload seguinte **N**: KE, reservado: 0x0, comprimento: 24 Payload seguinte **KE**: NOTIFIQUE, reservou: 0x0, comprimento: 136 Grupo DH: 2, reservado: 0x0 Payload seguinte **NOTIFY(SET_WINDOW_SIZE)**: NENHUNS, reservado: 0x0, comprimento: 12 Identificação do protocolo de segurança: IKE, tamanho do spi: 0, tipo: SET_WINDOW_SIZE	
* 11 de novembro 19:31:35.882: IKEv2: (Payload **SA ID= 2):Next**: ENCR, versão: 2.0 Tipo da troca: **CREATE_CHILD_SA,** bandeiras: ID de mensagem do **QUE RESPONDE MSG-RESPONSE**: 3, comprimento: 300 Índices do payload: Payload seguinte **SA**: N, reservado: 0x0, comprimento: 56 última proposta: 0x0, reservado: 0x0, comprimento: 52 Proposta: 1, ID de protocolo: IKE, tamanho SPI: 8, #trans: o último 4 transforma: 0x3, reservado: 0x0: comprimento:	O roteador2 constrói agora a resposta para a troca CHILD_SA. Esta é a resposta CREATE_CHILD_SA. O pacote CHILD_SA contém tipicamente: • SA HDR

```
    tipo: 1, reservado: 0x0, identificação: AES-CBC
    último transforme: 0x3, reservado: 0x0: comprimento: 8
    tipo: 2, reservado: 0x0, identificação: SHA1
    último transforme: 0x3, reservado: 0x0: comprimento: 8
    tipo: 3, reservado: 0x0, identificação: SHA96
    último transforme: 0x0, reservado: 0x0: comprimento: 8
    tipo: 4, reservado: 0x0, identificação:
DH_GROUP_1024_MODP/Group 2
 Payload seguinte N: KE, reservado: 0x0, comprimento: 24
 Payload seguinte KE: NOTIFIQUE, reservou: 0x0,
comprimento: 136
    Grupo DH: 2, reservado: 0x0

* 11 de novembro 19:31:35.882: IKEv2:Parse notificam o
payload: Payload seguinte SET_WINDOW_SIZE
NOTIFY(SET_WINDOW_SIZE): NENHUNS, reservado:
0x0, comprimento: 12
    Identificação do protocolo de segurança: IKE, tamanho
do spi: 0, tipo: SET_WINDOW_SIZE

* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_WAIT: EV_RECV_CREATE_C
HILD
* 11 de novembro 19:31:35.882: IKEv2:(SA ID= 2):Action:
Action_Null
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC: EV_CHK4_NOTIFY
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC: EV_VERIFY_MSG
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC: EV_PROC_MSG
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC: EV_CHK4_PFS
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC: EV_GEN_DH_SECRET
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC: EV_NO_EVENT
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
```

(version.flags/tipo da troca)

- Nonce Ni(optional): Se o CHILD_SA é criado como parte da troca inicial, um segundo payload e o nonce KE não devem ser enviados.
- Payload SA
- KEi (Chave-opcional): O pedido CREATE_CHILD_SA pôde opcionalmente conter um payload KE para que uma troca adicional DH permita umas garantias mais fortes do secretismo dianteiro para o CHILD_SA. Se as ofertas SA incluem grupos diferentes DH, KEi deve ser um elemento do grupo que o iniciador espera o que responde aceitar. Se supõe erradamente, a troca CREATE_CHILD_SA falha, e

ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC:
EV_OK_RECD_DH_SECRET_RESP
* 11 de novembro 19:31:35.890: IKEv2:(SA ID= 2):Action:
Action_Null
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC: EV_CHK_IKE_REKEY
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_PROC: EV_GEN_SKEYID
* 11 de novembro 19:31:35.890: Skeyid IKEv2:(SA ID=
2):Generate
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento **CHILD_I_DONE**: **EV_ACTIVATE_NEW_
SA**
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_DONE:
EV_UPDATE_CAC_STATS
* 11 de novembro 19:31:35.890: Pedido ikev2 sa
IKEv2:New ativado
* 11 de novembro 19:31:35.890: IKEv2:Failed para
decrescer a contagem para negócio que parte
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_DONE: EV_CHECK_DUPE
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento CHILD_I_DONE: EV_OK
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState: Evento da SAÍDA: EV_CHK_PENDING
* 11 de novembro 19:31:35.890: A resposta IKEv2:(SA ID=
2):Processed com ID de mensagem 3, pedidos pode ser
enviada da escala 4 a 8
* 11 de novembro 19:31:35.890: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID =
00000003 **CurState:** Evento da **SAÍDA**: EV_NO_EVENT

deve experimentar de novo com um KEi diferente.

- N (notifique payload-opcional): O payload da notificação é usado para transmitir dados informativos, tais como condições de erro e transições de estado, a um par IKE. Um payload da notificação pôde aparecer em um mensagem de resposta (que especifica geralmente porque um pedido foi rejeitado), em uma troca informativa (para relatar um erro não em um pedido IKE), ou em toda a outra mensagem para indicar capacidades do remetente ou para alterar o significado do pedido. Se esta troca CREATE_CHIL

		D_SA rekeying um SA existente a não ser o IKE_SA, o payload principal N do tipo REKEY_SA deve identificar o SA que está sendo rekeyed. Se esta troca CREATE_CHILD_SA não rekeying um SA existente, o payload N deve ser omitido.
		O roteador2 envia a resposta para fora e termina a ativação CRIANÇA nova SA.
O roteador1 recebe o pacote de resposta do roteador2 e termina a ativação do CHILD_SA.	* 11 de novembro 19:31:35.882: Payload IKEv2:(SA ID= 2):Next: ENCR, versão: 2.0 Tipo da troca: **CREATE_CHILD_SA**, bandeiras: ID de mensagem do **QUE RESPONDE MSG-RESPONSE**: 3, comprimento: 300 Índices do payload: Payload seguinte ENCR: SA, reservado: 0x0, comprimento: 272 * 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: **EV_CHK_IKE_REKEY** * 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: EV_GEN_SKEYID * 11 de novembro 19:31:35.882: IKEv2:(SA ID= 2): **Gerencia o skeyid** * 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_DONE: **EV_ACTIVATE_NEW_SA** * 11 de novembro 19:31:35.882: Deslocamento predeterminado ikev2 3 MIB IKEv2:Store, plataforma 62	

* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_DONE: EV_UPDATE_CAC_STATS
* 11 de novembro 19:31:35.882: Pedido ikev2 sa IKEv2:New ativado
* 11 de novembro 19:31:35.882: IKEv2:Failed para decrescer a contagem para o negócio entrante
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento **CHILD_R_DONE**: EV_CHECK_DUPE
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_DONE: EV_OK
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento CHILD_R_DONE: EV_START_DEL_NEG_TMR
* 11 de novembro 19:31:35.882: IKEv2:(SA ID= 2):Action: Action_Null
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Evento da SAÍDA: EV_CHK_PENDING
* 11 de novembro 19:31:35.882: A resposta IKEv2:(SA ID= 2):Sent com ID de mensagem 3, pedidos pode ser a escala aceitada 4 8
* 11 de novembro 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 **CurState:** Evento da **SAÍDA**: EV_NO_EVENT

Verificação do túnel

ISAKMP

Comando

show crypto ikev2 sa detailed

Saída do roteador1

```
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 roteador2

```
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

```
show crypto ipsec sa
```

> Nota: Nesta saída, ao contrário em IKEv1, o valor de grupo PFS DH aparece como o “PFS (Y/N): N, grupo DH: nenhuns” durante a primeira negociação do túnel, mas, depois que um rekey ocorre, os valores direitos aparecem. Este não é um erro, mesmo que o comportamento seja descrito na identificação de bug Cisco CSCug67056.
>
> A diferença entre IKEv1 e IKEv2 é que, nos últimos, a criança SA está criada como parte da troca própria do AUTH. O grupo DH configurado sob o crypto map seria usado somente durante rekey. Daqui, você veria o “PFS (Y/N): N, grupo DH: nenhuns” até os primeiros rekey.
>
> Com IKEv1, você vê um comportamento diferente, porque a criação criança SA acontece durante o Quick Mode, e a mensagem CREATE_CHILD_SA tem uma disposição levar o payload das trocas de chave que especifique os parâmetros DH para derivar um segredo

compartilhado novo.

Saída do roteador1

```
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 roteador2

```
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 pode igualmente verificar a saída do comando de **sessão de criptografia da mostra em** ambo o Roteadores; esta saída mostra o estado da sessão de túnel como UP-ATIVE.

```
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

- Eliminação de erros do intercâmbio de pacotes IKEv2 e do nível de protocolo
- Suporte Técnico e Documentação - Cisco Systems