# Отладки IOS IKEv2 для сквозного VPN-соединение с техническими примечаниями по поиску и устранению проблем PSK

## Содержание



## Введение

Когда предварительный общий ключ (PSK) используется, этот документ описывает отладки второй версии протокола Internet Key Exchange (IKEv2) на Cisco IOS®. Кроме того, этот документ предоставляет сведения о том, как преобразовать определенные линии отладки в конфигурации.

## Предварительные условия

### Требования

Cisco рекомендует ознакомиться с обменом пакетами для IKEv2. Для получения дополнительной информации обратитесь к Отладке Обмена пакетами и Уровня протокола IKEv2.

### Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Вторая версия протокола Internet Key Exchange (IKEv2)
- Cisco IOS 15.1 (1) T или позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

### Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

## Базовая проблема

Обмен пакетами в IKEv2 радикально отличается от обмена пакетами в IKEv1. В IKEv1 был ясно разграниченный обмен phase1, который состоял из шести (6) пакетов, придерживавшихся обменом фазы 2, который состоял из трех (3) пакетов; обмен IKEv2 является переменным. Для получения дополнительной информации о различиях и пояснении обмена пакетами, обратитесь к Отладке Обмена пакетами и Уровня протокола IKEv2.

## Настройка маршрутизатора

Этот раздел перечисляет конфигурации, используемые в этом документе.

### Маршрутизатор 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
```

## Маршрутизатор 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
```

# Устранение неполадок

## Отладочные данные маршрутизатора

Эти команды отладки используются в этом документе:

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

| Маршрутизатор 1 (инициатор) описание сообщения | Отладка | Маршрутизатор 2 (респондент) описание сообщения |
|---|---|---|
| Маршрутизатор 1 получает пакет, который совпадает с крипто-acl для однорангового ASA 10.0.0.2. Создание Initiates SA | *11 ноября 20:28:34.003: IKEv2:Got пакет от диспетчера<br>*11 ноября 20:28:34.003: IKEv2: Обработка элемента от очереди pak<br>*11 ноября 19:30:34.811: IKEv2: общий ключ Получения % адресом 10.0.0.2<br>*11 ноября 19:30:34.811: PHASE1-опора Предложения IKEv2:Adding к инструментарию policyle<br>*11 ноября 19:30:34.811: IKEv2: (1): Выбор IKE представляет IKEV2-НАСТРОЙКУ<br>*11 ноября 19:30:34.811: запрос IKEv2:New ikev2 sa признал<br>*11 ноября 19:30:34.811: выход IKEv2:Incrementing, выполняющий согласование sa, рассчитывает одним | |
| Первая пара сообщений является обменом IKE_SA_INIT. Эти сообщения выполняют согласование о криптографических алгоритмах, обмениваются параметрами и делают Обмен Диффи-Хеллмана. **Соответствующая конфигурация:** `crypto ikev2 proposal PHASE1-prop encryption 3des aes-cbc-128 integrity sha1 group 2 crypto ikev2 keyring KEYRNG peer peer1 address 10.0.0.2` | *11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: IDLE Event: EV_INIT_SA<br>*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: Событие I_BLD_INIT: EV_GET_IKE_POLICY<br>*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: **I_BLD_INIT Event:EV_SET_POLICY**<br>*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Установка настроенной политики<br>*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: Событие I_BLD_INIT: EV_CHK_AUTH4PKI<br>*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: **I_BLD_INIT Event:EV_GEN_DH_KEY**<br>*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): | |

255.255.255.0
hostname host1 pre-shared-key local cisco pre-shared-key remote cisco

Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: Событие I_BLD_INIT: EV_NO_EVENT
*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: Событие I_BLD_INIT: EV_OK_RECD_DH_PUBKEY_RESP
*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Действие: Action_Null
*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: Событие I_BLD_INIT: EV_GET_CONFIG_MODE
*11 ноября 19:30:34.811: инициатор IKEv2:IKEv2 - никакие данные config для передачи в обмене IKE_SA_INIT
*11 ноября 19:30:34.811: IKEv2:No конфигурируют данные для передачи к инструментарию:
*11 ноября 19:30:34.811: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: Событие I_BLD_INIT: EV_BLD_MSG
*11 ноября 19:30:34.811: IKEv2:Construct определяемое поставщиком информационное наполнение: УДАЛЯТЬ-ПРИЧИНА
*11 ноября 19:30:34.811: IKEv2:Construct определяемое поставщиком информационное наполнение: Специальный коммутатор
*11 ноября 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP
*11 ноября 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP
*11 ноября 19:30:34.811: **IKEv2: (ID SA = 1)**: Следующее информационное наполнение: SA, версия: 2.0 Exchange type : **IKE_SA_INIT,** флаги: Идентификатор сообщения **INITIATOR**: 0, длина: 344
Содержание информационного наполнения:
**SA** Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 56
последнее предложение: 0x0, зарезервированный: 0x0, длина: 52
Предложение: 1, Идентификатор протокола: IKE, размер SPI: 0, #trans: 5 последних преобразований: 0x3, зарезервированный: 0x0: длина: 8
введите : 1, зарезервированный: 0x0, идентификатор: 3DES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8

Инициатор, создающий пакет IKE_INIT_SA. Это содержит: Заголовок ISAKMP (SPI/версия/флаги), SAi1 (криптографический алгоритм, который инициатор IKE поддерживает), KEi (значение открытого ключа DH инициатора), и N (Параметр Инициатора).

введите : 2, зарезервированный: 0x0, идентификатор: SHA1
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1024_MODP/Group 2
KE Следующее информационное наполнение: N, зарезервированный: 0x0, длина: 136
Группа DH: 2, Зарезервированный: 0x0
N Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 24
VID Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 23
VID Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 21
УВЕДОМЬТЕ (NAT_DETECTION_SOURCE_IP) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 28
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NAT_DETECTION_SOURCE_IP
УВЕДОМЬТЕ (NAT_DETECTION_DESTINATION_IP) Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 28
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NAT_DETECTION_DESTINATION_IP
*11 ноября 19:30:34.814: IKEv2:Got пакет от диспетчера
*11 ноября 19:30:34.814: IKEv2:Processing элемент от очереди pak
*11 ноября 19:30:34.814: запрос IKEv2:New ikev2 sa признал
*11 ноября 19:30:34.814: поступление IKEv2:Incrementing, выполняющее согласование sa, рассчитывает одним
*11 ноября 19:30:34.814: информационное наполнение IKEv2:Next: SA, версия: 2.0 Exchange type: IKE_SA_INIT, флаги: Идентификатор сообщения INITIATOR: 0, длина: 344

Респондент получает IKE_INIT_SA.

Содержание информационного наполнения:
SA Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 56
последнее предложение: 0x0, зарезервированный: 0x0, длина: 52
Предложение: 1, Идентификатор протокола: IKE, размер SPI: 0, #trans: 5 последних преобразований: 0x3, зарезервированный: 0x0: длина: 8
введите : 1, зарезервированный: 0x0, идентификатор: 3DES

Респондент инициирует создание SA для того узла.

последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA1
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1024_MODP/Group 2
KE Следующее информационное наполнение: N, зарезервированный: 0x0, длина: 136
Группа DH: 2, Зарезервированный: 0x0
N Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 24

*11 ноября 19:30:34.814: IKEv2:Parse Определяемое поставщиком Информационное наполнение: VID СИСКО-ДЕЛЕТ-РИСОНА Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 23
*11 ноября 19:30:34.814: IKEv2:Parse Определяемое поставщиком Информационное наполнение: (ПОЛЬЗОВАТЕЛЬСКИЙ) VID Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 21
*11 ноября 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP УВЕДОМЛЯЮТ (NAT_DETECTION_SOURCE_IP) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 28
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NAT_DETECTION_SOURCE_IP
*11 ноября 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP УВЕДОМЛЯЮТ (NAT_DETECTION_DESTINATION_IP) Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 28
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NAT_DETECTION_DESTINATION_IP

| | |
|---|---|
| *11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: IDLE Event: **EV_RECV_INIT** | Респондент проверяет и обрабатывает сообщение IKE_INIT: (1) Выбирает крипто-комплект из предлагаемых |
| *11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: **R_INIT Event:EV_VERIFY_MSG** | |

*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: **R_INIT Event:EV_INSERT_SA**
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: **R_INIT Event:EV_GET_IKE_POLICY**
*11 ноября 19:30:34.814: по умолчанию Предложения IKEv2:Adding к политике инструментария
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: **R_INIT Event:EV_PROC_MSG**
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Событие R_INIT: EV_DETECT_NAT
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): обнаружение NAT Процесса уведомляет
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Обработка nat обнаруживает src, уведомляют
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Удаленный адрес совпал
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Обработка nat обнаруживает dst, уведомляют
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Локальный адрес совпал
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Никакой NAT не найден
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Событие R_INIT: EV_CHK_CONFIG_MODE
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Событие R_BLD_INIT: EV_SET_POLICY
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): **Установка настроенной политики**
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Событие R_BLD_INIT: EV_CHK_AUTH4PKI
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Событие R_BLD_INIT: EV_PKI_SESH_OPEN
*11 ноября 19:30:34.814: IKEv2: (ID SA = 1): Открытие сеанса PKI
*11 ноября 19:30:34.815: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000

инициатором, (2) вычисляет его собственный секретный ключ DH, и (3) он вычисляет значение skeyid, из которого все ключи могут быть получены для этого IKE_SA. Все кроме заголовков всех сообщений, которые придерживаются, шифруются и аутентифицируются. Ключи, используемые для шифрования и защиты целостности, получены из SKEYID и известны как: SK_e (шифрование), SK_a (аутентификация), SK_d получается и используется для деривации дальнейшего материала для кодирования для CHILD_SAs, и отдельный SK_e и SK_a вычислены для каждого направления.

**Соответствующая конфигурация:**

```
cry
pto 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-
```

CurState: **R_BLD_INIT Event:EV_GEN_DH_KEY**
*11 ноября 19:30:34.815: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Событие R_BLD_INIT: EV_NO_EVENT
*11 ноября 19:30:34.815: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: **R_BLD_INIT**
**Event:EV_OK_RECD_DH_PUBKEY_RESP**
*11 ноября 19:30:34.815: IKEv2: (ID SA = 1): Действие:
Action_Null
*11 ноября 19:30:34.815: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: **R_BLD_INIT Event:EV_GEN_DH_SECRET**
*11 ноября 19:30:34.822: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Событие R_BLD_INIT: EV_NO_EVENT
*11 ноября 19:30:34.822: IKEv2: **общий ключ Получения**
% **адресом 10.0.0.1**
*11 ноября 19:30:34.822: по умолчанию Предложения
IKEv2:Adding к политике инструментария
*11 ноября 19:30:34.822: IKEv2: (2): Выбор IKE
представляет IKEV2-НАСТРОЙКУ
*11 ноября 19:30:34.822: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Событие R_BLD_INIT:
EV_OK_RECD_DH_SECRET_RESP
*11 ноября 19:30:34.822: IKEv2: (ID SA = 1): Действие:
Action_Null
*11 ноября 19:30:34.822: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: **R_BLD_INIT Event:EV_GEN_SKEYID**
*11 ноября 19:30:34.822: IKEv2: (ID SA = 1):
**Генерируйте skeyid**
*11 ноября 19:30:34.822: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Событие R_BLD_INIT:
EV_GET_CONFIG_MODE
*11 ноября 19:30:34.822: респондент IKEv2:IKEv2 -
никакие данные config для передачи в обмене
IKE_SA_INIT
*11 ноября 19:30:34.822: IKEv2:No конфигурируют
данные для передачи к инструментарию:
*11 ноября 19:30:34.822: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000
CurState: Событие R_BLD_INIT: EV_BLD_MSG

```
key remote cisco
```

*11 ноября 19:30:34.822: IKEv2:Construct определяемое поставщиком информационное наполнение: УДАЛЯТЬ-ПРИЧИНА
*11 ноября 19:30:34.822: IKEv2:Construct определяемое поставщиком информационное наполнение: Специальный коммутатор
*11 ноября 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP
*11 ноября 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP
*11 ноября 19:30:34.822: IKEv2:Construct Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED
*11 ноября 19:30:34.822: IKEv2: (ID SA = 1): Следующее информационное наполнение: SA, версия: 2.0 Exchange type : **IKE_SA_INIT,** флаги : **RESPONDER MSG-RESPONSE Message id** : 0, длина: 449
Содержание информационного наполнения:
**SA** Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 48
последнее предложение: 0x0, зарезервированный: 0x0, длина: 44
Предложение: 1, Идентификатор протокола: IKE, размер SPI: 0, #trans: 4 последних преобразования: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA1
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1024_MODP/Group 2
**KE** Следующее информационное наполнение: N, зарезервированный: 0x0, длина: 136
Группа DH: 2, Зарезервированный: 0x0
**N** Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 24
VID Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 23
VID Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 21
УВЕДОМЬТЕ (NAT_DETECTION_SOURCE_IP) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 28
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NAT_DETECTION_SOURCE_IP

Маршрутизатор 2 создает сообщение респондента для обмена IKE_SA_INIT, который получен ASA1. Этот пакет содержит: Заголовок ISAKMP (SPI / версия/флаги), SAr1 (криптографический алгоритм, который респондент IKE выбирает), KEr (значение открытого ключа DH респондента), и Параметр Респондента.

| | | | |
|---|---|---|---|
| | УВЕДОМЬТЕ (NAT_DETECTION_DESTINATION_IP) Следующее информационное наполнение: CERTREQ, зарезервированный: 0x0, длина: 28<br>Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NAT_DETECTION_DESTINATION_IP<br>CERTREQ Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 105<br>Свидетельство, кодирующее Хэш и URL PKIX<br>УВЕДОМЬТЕ (HTTP_CERT_LOOKUP_SUPPORTED) Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 8<br>Идентификатор протокола безопасности: IKE, spi размер: 0, введите: HTTP_CERT_LOOKUP_SUPPORTED<br>*11 ноября 19:30:34.822: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Событие INIT_DONE: EV_DONE<br>*11 ноября 19:30:34.822: IKEv2: (ID SA = 1): Cisco DeleteReason Уведомляет, включен<br>*11 ноября 19:30:34.822: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Событие INIT_DONE: EV_CHK4_ROLE<br>*11 ноября 19:30:34.822: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE **Event:EV_START_TMR**<br>*11 ноября 19:30:34.822: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Событие R_WAIT_AUTH: EV_NO_EVENT<br>*11 ноября 19:30:34.822: **запрос IKEv2:New ikev2 sa признал**<br>*11 ноября 19:30:34.822: **выход IKEv2:Incrementing, выполняющий согласование sa, рассчитывает одним** | Router2 отсылает сообщение респондента в маршрутизатор 1. |
| Маршрутизатор 1 получает ответный пакет IKE_SA_INIT от маршрутизатора 2. | *11 ноября 19:30:34.823: IKEv2:Got пакет от диспетчера<br>*11 ноября 19:30:34.823: IKEv2:Got пакет от диспетчера<br>*11 ноября 19:30:34.823: IKEv2:Processing элемент от очереди pak | I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE **Event:EV_START_TMR** | Респондент запускает таймер для Подлинного процесса. |
| Router1 проверяет и обрабатывает ответ: (1) секретный ключ | *11 ноября 19:30:34.823: IKEv2: (ID SA = 1): Следующее информационное наполнение: SA, версия: 2.0 Exchange type: IKE_SA_INIT, флаги : **RESPONDER MSG-RESPONSE Message id** : 0, длина: 449 | | |

Содержание информационного наполнения:
SA Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 48
последнее предложение: 0x0, зарезервированный: 0x0, длина: 44
Предложение: 1, Идентификатор протокола: IKE, размер SPI: 0, #trans: 4 последних преобразования: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA1
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1024_MODP/Group 2
KE Следующее информационное наполнение: N, зарезервированный: 0x0, длина: 136
Группа DH: 2, Зарезервированный: 0x0
N Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 24

DH инициатора вычислен, и (2), инициатор skeyid также генерируется.

*11 ноября 19:30:34.823: IKEv2:Parse Определяемое поставщиком Информационное наполнение: VID СИСКО-ДЕЛЕТ-РИСОНА Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 23

*11 ноября 19:30:34.823: IKEv2:Parse Определяемое поставщиком Информационное наполнение: (ПОЛЬЗОВАТЕЛЬСКИЙ) VID Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 21

*11 ноября 19:30:34.823: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP УВЕДОМЛЯЮТ (NAT_DETECTION_SOURCE_IP) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 28
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NAT_DETECTION_SOURCE_IP

*11 ноября 19:30:34.824: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP УВЕДОМЛЯЮТ (NAT_DETECTION_DESTINATION_IP) Следующее информационное наполнение: CERTREQ, зарезервированный: 0x0, длина: 28
Идентификатор протокола безопасности: IKE, spi

размер: 0, введите: NAT_DETECTION_DESTINATION_IP
 CERTREQ Следующее информационное наполнение:
NOTIFY, зарезервированный: 0x0, длина: 105
  Свидетельство, кодирующее Хэш и URL PKIX

*11 ноября 19:30:34.824: IKEv2:Parse Notify Payload:
HTTP_CERT_LOOKUP_SUPPORTED УВЕДОМЛЯЮТ
(HTTP_CERT_LOOKUP_SUPPORTED) Следующее
информационное наполнение: NONE,
зарезервированный: 0x0, длина: 8
  Идентификатор протокола безопасности: IKE, spi
размер: 0, введите:
HTTP_CERT_LOOKUP_SUPPORTED
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000
CurState: Событие I_WAIT_INIT: EV_RECV_INIT
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1): Обработка
сообщение IKE_SA_INIT
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000
CurState: Событие I_PROC_INIT: EV_CHK4_NOTIFY
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000
CurState: Событие I_PROC_INIT: EV_VERIFY_MSG
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000
CurState: Событие I_PROC_INIT: EV_PROC_MSG
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000
CurState: Событие I_PROC_INIT: EV_DETECT_NAT
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):
обнаружение NAT Процесса уведомляет
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1): Обработка
nat обнаруживает src, уведомляют
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1): Удаленный
адрес совпал
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1): Обработка
nat обнаруживает dst, уведомляют
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1): Локальный
адрес совпал
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1): Никакой
NAT не найден
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000
CurState: Событие I_PROC_INIT: EV_CHK_NAT_T
*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B

| | |
|---|---|
| | R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: Событие I_PROC_INIT:<br>EV_CHK_CONFIG_MODE<br>*11 ноября 19:30:34.824: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: INIT_DONE **Event:EV_GEN_DH_SECRET**<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: Событие INIT_DONE: EV_NO_EVENT<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: Событие INIT_DONE:<br>EV_OK_RECD_DH_SECRET_RESP<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1): Действие:<br>Action_Null<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: INIT_DONE **Event:EV_GEN_SKEYID**<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>**Генерируйте skeyid**<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: Событие INIT_DONE: EV_DONE<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1): Cisco<br>DeleteReason Уведомляет, включен<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: Событие INIT_DONE: EV_CHK4_ROLE<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: Событие I_BLD_AUTH:<br>EV_GET_CONFIG_MODE<br>*11 ноября 19:30:34.831: IKEv2:Sending конфигурируют<br>данные к инструментарию<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: Событие I_BLD_AUTH: EV_CHK_EAP |
| Инициатор запускает обмен IKE_AUTH и генерирует опознавательное информационное наполнение. Пакет IKE_AUTH | *11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: **I_BLD_AUTH Event:EV_GEN_AUTH**<br>*11 ноября 19:30:34.831: IKEv2: (ID SA = 1):<br>Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B<br>R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000<br>CurState: Событие I_BLD_AUTH: EV_CHK_AUTH_TYPE |

содержит: Заголовок ISAKMP (SPI / версия/флаги), IDI (идентичность инициатора), информационное наполнение AUTH, SAi2 (инициирует подобное SA обмену набора преобразований фазы 2 в IKEv1), и TSI и TSr (Инициатор и Селекторы трафика Респондента): Они содержат адрес источника и назначения инициатора и респондента соответственно для передачи/получения зашифрованного потока данных. Диапазон адресов указывает, что туннелирован весь трафик к и из того диапазона. Если предложение приемлемо для респондента, оно передает идентичные информационные наполнения TS обратно. Первый CHILD_SA создан для proxy_ID пары, которая совпадает с триггерным пакетом.

**Соответствующая конфигурация:** `crypto ipsec`

*11 ноября 19:30:34.831: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: Событие I_BLD_AUTH: EV_OK_AUTH_GEN
*11 ноября 19:30:34.831: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: Событие I_BLD_AUTH: EV_SEND_AUTH
*11 ноября 19:30:34.831: IKEv2:Construct определяемое поставщиком информационное наполнение: GRANITE CISCO
*11 ноября 19:30:34.831: IKEv2:Construct Notify Payload: INITIAL_CONTACT
*11 ноября 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE
*11 ноября 19:30:34.831: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT
*11 ноября 19:30:34.831: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS
**Содержание информационного наполнения:**
VID Следующее информационное наполнение: IDI, зарезервированный: 0x0, длина: 20
**IDI** Следующее информационное наполнение: AUTH, зарезервированный: 0x0, длина: 12
ID Type: Адрес IPv4, Зарезервированный: 0x0 0x0
**AUTH** Следующее информационное наполнение: CFG, зарезервированный: 0x0, длина: 28
Подлинный PSK метода, зарезервированный: 0x0, зарезервированный 0x0
**CFG** Следующее информационное наполнение: SA, зарезервированный: 0x0, длина: 309
тип cfg: CFG_REQUEST, зарезервированный: 0x0, зарезервированный: 0x0
*11 ноября 19:30:34.831: SA Следующее информационное наполнение: **TSI**, зарезервированный: 0x0, длина: 40
последнее предложение: 0x0, зарезервированный: 0x0, длина: 36
Предложение: 1, Идентификатор протокола: ESP, размер SPI: 4, #trans: 3 последних преобразования: 0x3, зарезервированный: 0x0: длина: 8
введите : 1, зарезервированный: 0x0, идентификатор: 3DES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 5, зарезервированный: 0x0, идентификатор: не используйте ESN
**TSI** Следующее информационное наполнение: TSr, зарезервированный: 0x0, длина: 24

| | | |
|---|---|---|
| | Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0<br>Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор: 0, длина: 16<br>начальный порт: 0, оконечный порт: 65535<br>запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255<br>**TSr** Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 24<br>Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0<br>Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор: 0, длина: 16<br>начальный порт: 0, оконечный порт: 65535<br>запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255<br>УВЕДОМЬТЕ (INITIAL_CONTACT) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 8<br>Идентификатор протокола безопасности: IKE, spi размер: 0, введите: INITIAL_CONTACT<br>УВЕДОМЬТЕ (SET_WINDOW_SIZE) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 12<br>Идентификатор протокола безопасности: IKE, spi размер: 0, введите: SET_WINDOW_SIZE<br>УВЕДОМЬТЕ (ESP_TFC_NO_SUPPORT) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 8<br>Идентификатор протокола безопасности: IKE, spi размер: 0, введите: ESP_TFC_NO_SUPPORT<br>УВЕДОМЬТЕ (NON_FIRST_FRAGS) Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 8<br>Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NON_FIRST_FRAGS | |
| `transform-set TS esp-3des esp-sha-hmac crypto ipsec profile phse2-prof set transform-set TS set ikev2-profile IKEV2-SETUP` | | |
| | *11 ноября 19:30:34.832: IKEv2: (ID SA = 1): Следующее информационное наполнение: ENCR, версия: 2.0<br>Exchange type : **IKE_AUTH**, флаги: Идентификатор сообщения **INITIATOR**: 1, длина: 556<br>Содержание информационного наполнения: ENCR Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 528<br><br>*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 **CurState:** Событие **I_WAIT_AUTH**: EV_NO_EVENT<br>*11 ноября 19:30:34.832: IKEv2:Got пакет от диспетчера<br>*11 ноября 19:30:34.832: IKEv2:Processing элемент от очереди pak | Маршрутизатор 2 получает и проверяет данные |

*11 ноября 19:30:34.832: IKEv2: (ID SA = 1): Запрос имеет mess_id 1; ожидаемый 1 до 1
*11 ноября 19:30:34.832: **IKEv2: (ID SA = 1)**: Следующее информационное наполнение: ENCR, версия: 2.0
Exchange type : **IKE_AUTH**, флаги: Идентификатор сообщения **INITIATOR**: 1, длина: 556
Содержание информационного наполнения:
*11 ноября 19:30:34.832: IKEv2:Parse Определяемое поставщиком Информационное наполнение: (ПОЛЬЗОВАТЕЛЬСКИЙ) VID Следующее информационное наполнение: IDI, зарезервированный: 0x0, длина: 20
**IDI** Следующее информационное наполнение: AUTH, зарезервированный: 0x0, длина: 12
ID Type: Адрес IPv4, Зарезервированный: 0x0 0x0
**AUTH** Следующее информационное наполнение: CFG, зарезервированный: 0x0, длина: 28
Подлинный PSK метода, зарезервированный: 0x0, зарезервированный 0x0
**CFG** Следующее информационное наполнение: SA, зарезервированный: 0x0, длина: 309
тип cfg: CFG_REQUEST, зарезервированный: 0x0, зарезервированный: 0x0
*11 ноября 19:30:34.832: тип attrib: внутренний IP4 DNS, длина: 0
*11 ноября 19:30:34.832: тип attrib: внутренний IP4 DNS, длина: 0
*11 ноября 19:30:34.832: тип attrib: внутренний IP4 NBNS, длина: 0
*11 ноября 19:30:34.832: тип attrib: внутренний IP4 NBNS, длина: 0
*11 ноября 19:30:34.832: тип attrib: внутренняя подсеть IP4, длина: 0
*11 ноября 19:30:34.832: тип attrib: версия приложения, длина: 257
тип attrib: Неизвестный - 28675, длина: 0
*11 ноября 19:30:34.832: тип attrib: Неизвестный - 28672, длина: 0
*11 ноября 19:30:34.832: тип attrib: Неизвестный - 28692, длина: 0
*11 ноября 19:30:34.832: тип attrib: Неизвестный - 28681, длина: 0
*11 ноября 19:30:34.832: тип attrib: Неизвестный - 28674, длина: 0
*11 ноября 19:30:34.832: **SA** Следующее информационное наполнение: TSI, зарезервированный: 0x0, длина: 40
последнее предложение: 0x0, зарезервированный: 0x0, длина: 36
Предложение: 1, Идентификатор протокола: ESP, размер SPI: 4, #trans: 3 последних преобразования: 0x3, зарезервированный: 0x0: длина: 8
введите : 1, зарезервированный: 0x0, идентификатор:

проверки подлинности, полученные от маршрутизатора 1.

**Соответствующая конфигурация**:

```
cry
pto ipsec ikev2
ipsec-proposal
AES256 protocol esp
encryption aes-256
protocol esp
integrity sha-1 md5
```

3DES
  последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
  введите : 3, зарезервированный: 0x0, идентификатор: SHA96
  последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
  введите : 5, зарезервированный: 0x0, идентификатор: не используйте ESN
**TSI** Следующее информационное наполнение: TSr, зарезервированный: 0x0, длина: 24
  Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0
  Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор: 0, длина: 16
  начальный порт: 0, оконечный порт: 65535
  запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255
**TSr** Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 24
  Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0
  Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор: 0, длина: 16
  начальный порт: 0, оконечный порт: 65535
  запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255

| | |
|---|---|
| *11 ноября 19:30:34.832: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_WAIT_AUTH: EV_RECV_AUTH<br>*11 ноября 19:30:34.832: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_WAIT_AUTH: EV_CHK_NAT_T<br>*11 ноября 19:30:34.832: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_WAIT_AUTH: EV_PROC_ID<br>*11 ноября 19:30:34.832: IKEv2: (ID SA = 1): Полученные допустимые параметры в идентификаторе процесса<br>*11 ноября 19:30:34.832: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_WAIT_AUTH: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL<br>*11 ноября 19:30:34.832: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_WAIT_AUTH: EV_GET_POLICY_BY_PEERID<br>*11 ноября 19:30:34.833: IKEv2: (1): Выбор IKE | Маршрутизатор 2 создает ответ на пакет IKE_AUTH, который это получило от маршрутизатора 1. Этот ответный пакет содержит: Заголовок ISAKMP (SPI / версия/флаги), IDr (идентичность респондента), информационное наполнение AUTH, SAr2 (инициирует подобное SA обмену набора преобразований фазы 2 в IKEv1), и TSI и TSr (Инициатор и Селекторы трафика Респондента). |

```
представляет IKEV2-НАСТРОЙКУ
*11 ноября 19:30:34.833: IKEv2: общий ключ Получения
% адресом 10.0.0.1
*11 ноября 19:30:34.833: IKEv2: общий ключ Получения
% адресом 10.0.0.1
*11 ноября 19:30:34.833: по умолчанию Предложения
IKEv2:Adding к политике инструментария
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Использование IKEv2 представляет 'IKEV2-
НАСТРОЙКУ'
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_WAIT_AUTH: EV_SET_POLICY
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Установка
настроенной политики
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_WAIT_AUTH:
EV_VERIFY_POLICY_BY_PEERID
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_WAIT_AUTH: EV_CHK_AUTH4EAP
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_WAIT_AUTH:
EV_CHK_POLREQEAP
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_VERIFY_AUTH:
EV_CHK_AUTH_TYPE
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_VERIFY_AUTH:
EV_GET_PRESHR_KEY
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_VERIFY_AUTH: EV_VERIFY_AUTH
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_VERIFY_AUTH: EV_CHK4_IC
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_VERIFY_AUTH:
EV_CHK_REDIRECT
```

Они содержат адрес источника и назначения инициатора и респондента соответственно для передачи/получения зашифрованного потока данных. Диапазон адресов указывает, что туннелирован весь трафик к и из того диапазона. Эти параметры идентичны тому, который был получен от ASA1.

*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): проверка Перенаправления не необходима, пропуская его
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_VERIFY_AUTH: EV_NOTIFY_AUTH_DONE
*11 ноября 19:30:34.833: авторизация группы IKEv2:AAA не настроена
*11 ноября 19:30:34.833: авторизация пользователя IKEv2:AAA не настроена
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_VERIFY_AUTH: EV_CHK_CONFIG_MODE
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_VERIFY_AUTH: EV_SET_RECD_CONFIG_MODE
*11 ноября 19:30:34.833: IKEv2:Received конфигурируют данные от инструментария:
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_VERIFY_AUTH: EV_PROC_SA_TS
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_VERIFY_AUTH: EV_GET_CONFIG_MODE
*11 ноября 19:30:34.833: IKEv2:Error, создающий ответ config
*11 ноября 19:30:34.833: IKEv2:No конфигурируют данные для передачи к инструментарию:
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_BLD_AUTH: EV_MY_AUTH_METHOD
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_BLD_AUTH: EV_GET_PRESHR_KEY
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие R_BLD_AUTH: EV_GEN_AUTH
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001

CurState: Событие R_BLD_AUTH: EV_CHK4_SIGN
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_BLD_AUTH: EV_OK_AUTH_GEN
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие R_BLD_AUTH: EV_SEND_AUTH
*11 ноября 19:30:34.833: IKEv2:Construct определяемое поставщиком информационное наполнение: GRANITE CISCO
*11 ноября 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE
*11 ноября 19:30:34.833: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT
*11 ноября 19:30:34.833: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Следующее информационное наполнение: ENCR, версия: 2.0
Exchange type **: IKE_AUTH**, флаги : **RESPONDER MSG-RESPONSE Message id** : 1, длина: 252
Содержание информационного наполнения:
**ENCR** Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 224
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие AUTH_DONE: EV_OK
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Действие: Action_Null
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие AUTH_DONE: EV_PKI_SESH_CLOSE
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1): Закрытие сеанса PKI

Респондент передает ответ за IKE_AUTH.

*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие AUTH_DONE:
EV_UPDATE_CAC_STATS
*11 ноября 19:30:34.833: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: AUTH_DONE **Event:EV_INSERT_IKE**
*11 ноября 19:30:34.834: индекс ikev2 1 МиБ IKEv2:Store, платформа 60
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001
CurState: Событие AUTH_DONE: EV_GEN_LOAD_IPSEC
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1):

| | | | |
|---|---|---|---|
| | Асинхронный запрос помещен в очередь<br>*11 ноября 19:30:34.834: IKEv2: (ID SA = 1):<br>*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие **AUTH_DONE**: EV_NO_EVENT | *11 ноября 19:30:34.840: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_OK_RECD_LOAD_IPSEC<br>*11 ноября 19:30:34.840: IKEv2: (ID SA = 1): Действие: Action_Null<br>*11 ноября 19:30:34.840: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_START_ACCT<br>*11 ноября 19:30:34.840: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_CHECK_DUPE<br>*11 ноября 19:30:34.840: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_CHK4_ROLE | |
| Инициатор получает ответ от Респондента. | *11 ноября 19:30:34.834: IKEv2:Got пакет от диспетчера<br><br>*11 ноября 19:30:34.834: IKEv2:Processing элемент от очереди pak | | Респондент вставляет запись в SAD. |
| Маршрутизатор 1 проверяет и обрабатывает данные проверки подлинности в этом пакете. | *11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Следующее информационное наполнение: ENCR, версия: 2.0 Exchange type : **IKE_AUTH**, флаги : **RESPONDER MSG-RESPONSE Message id** : 1, длина: 252 **Содержание информационного наполнения:** | | |
| Маршрутизатор 1 | *11 ноября 19:30:34.834: IKEv2:Parse Определяемое | | |

поставщиком Информационное наполнение: (ПОЛЬЗОВАТЕЛЬСКИЙ) VID Следующее информационное наполнение: IDr, зарезервированный: 0x0, длина: 20
IDr Следующее информационное наполнение: AUTH, зарезервированный: 0x0, длина: 12
ID Type: Адрес IPv4, Зарезервированный: 0x0 0x0
AUTH Следующее информационное наполнение: SA, зарезервированный: 0x0, длина: 28
Подлинный PSK метода, зарезервированный: 0x0, зарезервированный 0x0
SA Следующее информационное наполнение: TSI, зарезервированный: 0x0, длина: 40
последнее предложение: 0x0, зарезервированный: 0x0, длина: 36
Предложение: 1, Идентификатор протокола: ESP, размер SPI: 4, #trans: 3 последних преобразования: 0x3, зарезервированный: 0x0: длина: 8
введите : 1, зарезервированный: 0x0, идентификатор: 3DES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 5, зарезервированный: 0x0, идентификатор: не используйте ESN
TSI Следующее информационное наполнение: TSr, зарезервированный: 0x0, длина: 24
Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0
Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор: 0, длина: 16
начальный порт: 0, оконечный порт: 65535
запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255
TSr Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 24
Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0
Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор: 0, длина: 16
начальный порт: 0, оконечный порт: 65535
запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255

тогда вставляет этот SA в свой SAD.

*11 ноября 19:30:34.834: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE УВЕДОМЛЯЮТ (SET_WINDOW_SIZE) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 12
Идентификатор протокола безопасности: IKE, spi

размер: 0, введите: SET_WINDOW_SIZE

*11 ноября 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT УВЕДОМЛЯЮТ (ESP_TFC_NO_SUPPORT) Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 8
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: ESP_TFC_NO_SUPPORT

*11 ноября 19:30:34.834: IKEv2:Parse Notify Payload: NON_FIRST_FRAGS УВЕДОМЛЯЮТ (NON_FIRST_FRAGS) Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 8
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: NON_FIRST_FRAGS

*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_WAIT_AUTH Event:EV_RECV_AUTH
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Действие: Action_Null
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие I_PROC_AUTH: EV_CHK4_NOTIFY
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:EV_PROC_MSG
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие I_PROC_AUTH: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие I_PROC_AUTH: EV_GET_POLICY_BY_PEERID
*11 ноября 19:30:34.834: PHASE1-опора Предложения IKEv2:Adding к политике инструментария
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Использование IKEv2 представляет 'IKEV2-НАСТРОЙКУ'
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие I_PROC_AUTH: EV_VERIFY_POLICY_BY_PEERID
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1):

Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие I_PROC_AUTH:
EV_CHK_AUTH_TYPE
*11 ноября 19:30:34.834: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие I_PROC_AUTH:
EV_GET_PRESHR_KEY
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: **I_PROC_AUTH Event:EV_VERIFY_AUTH**
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие I_PROC_AUTH: EV_CHK_EAP
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: **I_PROC_AUTH**
**Event:EV_NOTIFY_AUTH_DONE**
*11 ноября 19:30:34.835: авторизация группы
IKEv2:AAA не настроена
*11 ноября 19:30:34.835: авторизация пользователя
IKEv2:AAA не настроена
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие I_PROC_AUTH:
EV_CHK_CONFIG_MODE
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие I_PROC_AUTH: EV_CHK4_IC
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие I_PROC_AUTH: EV_CHK_IKE_ONLY
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие I_PROC_AUTH: EV_PROC_SA_TS
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие AUTH_DONE: EV_OK
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1): Действие:
Action_Null
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001
CurState: Событие AUTH_DONE: EV_PKI_SESH_CLOSE

*11 ноября 19:30:34.835: IKEv2: (ID SA = 1): Закрытие сеанса PKI
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_UPDATE_CAC_STATS
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_INSERT_IKE
*11 ноября 19:30:34.835: индекс ikev2 1 МиБ IKEv2:Store, платформа 60
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_GEN_LOAD_IPSEC
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1): Асинхронный запрос помещен в очередь

*11 ноября 19:30:34.835: IKEv2: (ID SA = 1):
*11 ноября 19:30:34.835: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_NO_EVENT
*11 ноября 19:30:34.835: сообщение 8 IKEv2:KMI использовано. Никакие принятые меры.
*11 ноября 19:30:34.835: сообщение 12 IKEv2:KMI использовано. Никакие принятые меры.
*11 ноября 19:30:34.835: данные IKEv2:No для передачи в наборе настройки режима.
*11 ноября 19:30:34.841: идентификатор IKEv2:Adding обрабатывает 0x80000002, привязанный к SPI 0x9506D414 для сеанса 8

*11 ноября 19:30:34.841: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_OK_RECD_LOAD_IPSEC
*11 ноября 19:30:34.841: IKEv2: (ID SA = 1): Действие: Action_Null
*11 ноября 19:30:34.841: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_START_ACCT
*11 ноября 19:30:34.841: IKEv2: (ID SA = 1): Учет, не требуемый
*11 ноября 19:30:34.841: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие AUTH_DONE: EV_CHECK_DUPE
*11 ноября 19:30:34.841: IKEv2: (ID SA = 1):

| | | | |
|---|---|---|---|
| Туннель подключен на Инициаторе и статусе *showsREADY*. | Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Событие **AUTH_DONE**: EV_CHK4_ROLE<br>*11 ноября 19:30:34.841: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: **READYEvent**: EV_CHK_IKE_ONLY<br>*11 ноября 19:30:34.841: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: ГОТОВОЕ Событие: EV_I_OK | *11 ноября 19:30:34.840: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **ГОТОВОЕ** Событие: EV_R_OK<br>*11 ноября 19:30:34.840: IKEv2: (ID SA = 1): Трассировка SM-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: ГОТОВОЕ Событие: EV_NO_EVENT | Туннель подключен на Респонденте. Туннель Респондента обычно подходит перед Инициатором. |

## Отладки CHILD_SA

Этот обмен состоит из одиночной пары запроса/ответа и упоминался как обмен фазы 2 в IKEv1. Это могло бы инициироваться к любому концу IKE_SA после того, как завершены начальные обмены.

| **Маршрутизатор 1 описание сообщения CHILD_SA** | **Отладка** | **Маршрутизатор 2 описание сообщения CHILD_SA** |
|---|---|---|
| Маршрутизатор 1 инициирует обмен CHILD_SA. Это - запрос CREATE_CHILD_SA. Пакет CHILD_SA, как правило, содержит:<br>• HDR SA (version.flags/exchange тип)<br>• Параметр (дополнительный) Ni: Если CHILD_SA создан как часть начального обмена, второе | *11 ноября 19:31:35.873: IKEv2:Got пакет от диспетчера<br>*11 ноября 19:31:35.873: IKEv2:Processing элемент от очереди pak<br>*11 ноября 19:31:35.873: IKEv2: (ID SA = 2): Запрос имеет mess_id 3; ожидаемый 3 - 7<br>*11 ноября 19:31:35.873: IKEv2: (ID SA = 2): Следующее информационное наполнение: ENCR, версия: **2.0** **Exchange type: CREATE_CHILD_SA**, флаги: Идентификатор сообщения **INITIATOR**: 3, длина: 396<br>Содержание информационного наполнения:<br>**SA** Следующее информационное наполнение: N, зарезервированный: 0x0, длина: 152<br>последнее предложение: 0x0, зарезервированный: 0x0, длина: 148<br>Предложение: 1, Идентификатор протокола: IKE, размер SPI: 8, #trans: 15 последних преобразований: 0x3, зарезервированный: 0x0: длина: 12<br>введите : 1, зарезервированный: 0x0, идентификатор: | |

информационное наполнение KE и параметр не должны быть переданы),

- Информационное наполнение SA
- (Ключевой дополнительный) KEi: запрос CREATE_CHILD_SA мог бы дополнительно содержать информационное наполнение KE для дополнительного обмена DH для включения более сильных гарантий прямой секретности для CHILD_SA. Если предложения SA включают другие группы DH, KEi должен быть элементом группы, которую инициатор ожидает, что респондент примет. Если

CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA512
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA384
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA256
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA1
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: MD5
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA512
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA384
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA256
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: MD596
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1536_MODP/Group 5

это не угадывает, сбои обмена CREATE_CHILD_SA, и это должно будет повторить с другим KEi

- N (Уведомляют дополнительный информационным наполнением). Уведомлять Информационное наполнение, используется для передачи информационных данных, таких как состояния ошибки и изменения состояния, к узлу IKE. Уведомлять Информационное наполнение может появиться в ответном сообщении (обычно определение, почему запрос был отклонен), в ИНФОРМАЦИОННОМ Exchange (для создания отчетов об

последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1024_MODP/Group 2
**N** Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 24
**KE** Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 136
Группа DH: 2, Зарезервированный: 0x0

*11 ноября 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE **УВЕДОМЛЯЮТ** (SET_WINDOW_SIZE) Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 12
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: SET_WINDOW_SIZE

*11 ноября 19:31:35.874: IKEv2: (**ID SA = 2**): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: ГОТОВОЕ
Событие: **EV_RECV_CREATE_CHILD**
*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Действие: Action_Null
*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_INIT: EV_RECV_CREATE_CHILD
*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Действие: Action_Null
*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_INIT: EV_VERIFY_MSG
*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_INIT: EV_CHK_CC_TYPE
*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_IKE: **EV_REKEY_IKESA**
*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_IKE: EV_GET_IKE_POLICY
*11 ноября 19:31:35.874: IKEv2: **общий ключ Получения % адресом 10.0.0.2**
*11 ноября 19:31:35.874: IKEv2: общий ключ Получения % адресом 10.0.0.2
*11 ноября 19:31:35.874: PHASE1-опора Предложения IKEv2:Adding к политике инструментария

| | |
|---|---|
| ошибке не в запросе IKE), или в любом другом сообщении, чтобы указать на возможности отправителя или модифицировать значение запроса. Если этот обмен CREATE_CHILD_SA повторно вводит существующий SA кроме IKE_SA, продвижение N информационное наполнение типа REKEY_SA, MUST определяет повторно вводимый SA. Если этот обмен CREATE_CHILD_SA не повторно вводит существующий SA, информационное наполнение N, MUST опущен. | *11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Использование IKEv2 представляет 'IKEV2-НАСТРОЙКУ'<br>*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_IKE: EV_PROC_MSG<br>*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_IKE: EV_SET_POLICY<br>*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): **Установка настроенной политики**<br>*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_BLD_MSG: EV_GEN_DH_KEY<br>*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_BLD_MSG: EV_NO_EVENT<br>*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_BLD_MSG: EV_OK_RECD_DH_PUBKEY_RESP<br>*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Действие: Action_Null<br>*11 ноября 19:31:35.874: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG **Event:EV_GEN_DH_SECRET**<br>*11 ноября 19:31:35.881: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_BLD_MSG: EV_NO_EVENT<br>*11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_BLD_MSG: EV_OK_RECD_DH_SECRET_RESP<br>*11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Действие: Action_Null<br>*11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_BLD_MSG: EV_BLD_MSG<br>*11 ноября 19:31:35.882 : **IKEv2:Construct Notify Payload** : SET_WINDOW_SIZE<br>Содержание информационного наполнения:<br>**SA** Следующее информационное наполнение: N, |

зарезервированный: 0x0, длина: 56
последнее предложение: 0x0, зарезервированный:
0x0, длина: 52
Предложение: 1, Идентификатор протокола: IKE,
размер SPI: 8, #trans: 4 последних преобразования:
0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор:
CBC AES
последнее преобразование: 0x3, зарезервированный:
0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор:
SHA1
последнее преобразование: 0x3, зарезервированный:
0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор:
SHA96
последнее преобразование: 0x0, зарезервированный:
0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор:
DH_GROUP_1024_MODP/Group 2
N Следующее информационное наполнение: KE,
зарезервированный: 0x0, длина: 24
KE Следующее информационное наполнение:
NOTIFY, зарезервированный: 0x0, длина: 136
Группа DH: 2, Зарезервированный: 0x0
УВЕДОМЬТЕ (SET_WINDOW_SIZE) Следующее
информационное наполнение: NONE,
зарезервированный: 0x0, длина: 12
Идентификатор протокола безопасности: IKE, spi
размер: 0, введите: SET_WINDOW_SIZE
*11 ноября 19:31:35.869: IKEv2: (ID SA = 2): Следующее
информационное наполнение: ENCR, версия: 2.0
Exchange type : CREATE_CHILD_SA,
флаги: Идентификатор сообщения INITIATOR: 2,
длина: 460
Содержание информационного наполнения:
ENCR Следующее информационное наполнение: SA,
зарезервированный: 0x0, длина: 432
*11 ноября 19:31:35.873: IKEv2:Construct Notify Payload:
SET_WINDOW_SIZE
Содержание информационного наполнения:
SA Следующее информационное наполнение: N,
зарезервированный: 0x0, длина: 152
последнее предложение: 0x0, зарезервированный: 0x0,
длина: 148
Предложение: 1, Идентификатор протокола: IKE,
размер SPI: 8, #trans: 15 последних преобразований:
0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор:
CBC AES
последнее преобразование: 0x3, зарезервированный:
0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор:

Этот пакет получен маршрутизатором 2.

CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA512
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA384
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA256
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA1
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: MD5
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA512
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA384
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA256
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: MD596
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1536_MODP/Group 5
последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1024_MODP/Group 2

**N** Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 24
**KE** Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 136
Группа DH: 2, Зарезервированный: 0x0
**УВЕДОМЬТЕ** (SET_WINDOW_SIZE) Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 12
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: SET_WINDOW_SIZE

*11 ноября 19:31:35.882: IKEv2: (**ID SA = 2**): Следующее информационное наполнение: ENCR, версия: 2.0
Exchange type : **CREATE_CHILD_SA,** флаги : **RESPONDER MSG-RESPONSE Message id** : 3, длина: 300
Содержание информационного наполнения:
**SA** Следующее информационное наполнение: N, зарезервированный: 0x0, длина: 56
последнее предложение: 0x0, зарезервированный: 0x0, длина: 52
Предложение: 1, Идентификатор протокола: IKE, размер SPI: 8, #trans: 4 последних преобразования: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA1
последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1024_MODP/Group 2
**N** Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 24
**KE** Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 136
Группа DH: 2, Зарезервированный: 0x0

*11 ноября 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE **УВЕДОМЛЯЮТ** (SET_WINDOW_SIZE) Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 12
Идентификатор протокола безопасности: IKE, spi размер: 0, введите: SET_WINDOW_SIZE

*11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003

Маршрутизатор 2 теперь создает ответ для обмена CHILD_SA. Это - ответ CREATE_CHILD_SA. Пакет CHILD_SA, как правило, содержит:

- HDR SA (version.flags/exchange тип)
- Параметр (дополнительный) Ni: Если CHILD_SA создан как часть начального обмена, второе информационное наполнение KE и параметр не должны быть переданы.
- Информационное наполнение SA
- (Ключевой дополнительный) KEi: запрос CREATE_CHILD_SA мог бы дополнительн

CurState:  Событие
**CHILD_I_WAIT**: **EV_RECV_CREATE_CHILD**
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Действие:
Action_Null
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState:  Событие **CHILD_I_PROC**: EV_CHK4_NOTIFY
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: Событие CHILD_I_PROC: **EV_VERIFY_MSG**
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: Событие CHILD_I_PROC: EV_PROC_MSG
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: Событие CHILD_I_PROC: EV_CHK4_PFS
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: Событие CHILD_I_PROC:
EV_GEN_DH_SECRET
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: Событие CHILD_I_PROC: EV_NO_EVENT
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: Событие CHILD_I_PROC:
EV_OK_RECD_DH_SECRET_RESP
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2): Действие:
Action_Null
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: Событие CHILD_I_PROC:
EV_CHK_IKE_REKEY
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState: Событие CHILD_I_PROC: EV_GEN_SKEYID
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2):
Генерируйте skeyid
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003
CurState:  Событие
**CHILD_I_DONE**: **EV_ACTIVATE_NEW_SA**
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2):

о содержать информационное наполнение KE для дополнительного обмена DH для включения более сильных гарантий прямой секретности для CHILD_SA. Если предложения SA включают другие группы DH, KEi должен быть элементом группы, которую инициатор ожидает, что респондент примет. Если это не угадывает, сбои обмена CREATE_CHILD_SA, и это должно повторить с другим KEi.

- N (Уведомляют дополнительный информационным наполнением): Уведомлять Информационное

Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: Событие CHILD_I_DONE: EV_UPDATE_CAC_STATS
*11 ноября 19:31:35.890: запрос IKEv2:New ikev2 sa активирован
*11 ноября 19:31:35.890: IKEv2:Failed для постепенного уменьшения счета для исходящего согласования
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: Событие CHILD_I_DONE: EV_CHECK_DUPE
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: Событие CHILD_I_DONE: EV_OK
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: Событие EXIT: EV_CHK_PENDING
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2): Обработанный ответ с идентификатором сообщения 3, Запросы могут быть отправлены из диапазона 4 - 8
*11 ноября 19:31:35.890: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 **CurState: Событие EXIT** : EV_NO_EVENT

наполнение используется для передачи информационных данных, таких как состояния ошибки и изменения состояния, к узлу IKE. Уведомлять Информационное наполнение могло бы появиться в ответном сообщении (обычно определение, почему запрос был отклонен), в информационном обмене (для создания отчетов об ошибке не в запросе IKE), или в любом другом сообщении, чтобы указать на возможности отправителя или модифицировать значение запроса. Если этот обмен CREATE_CHILD_SA повторно вводит существующи

| | | |
|---|---|---|
| | | й SA кроме IKE_SA, продвижение N информационное наполнение типа, REKEY_SA должен определить повторно вводимый SA. Если этот обмен CREATE_CHILD_SA не повторно вводит существующий SA, информационное наполнение N должно быть опущено. |
| | | Маршрутизатор 2 отсылает ответ и завершает активацию новой CHILD SA. |
| Маршрутизатор 1 получает ответный пакет от маршрутизатора 2 и завершает активацию CHILD_SA. | *11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Следующее информационное наполнение: ENCR, версия: 2.0 Exchange type : **CREATE_CHILD_SA**, флаги : **RESPONDER MSG-RESPONSE Message id** : 3, длина: 300<br>Содержание информационного наполнения:<br>ENCR Следующее информационное наполнение: SA, зарезервированный: 0x0, длина: 272<br><br>*11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG **Event:EV_CHK_IKE_REKEY**<br>*11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: Событие CHILD_R_BLD_MSG: EV_GEN_SKEYID | |

*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
**Генерируйте skeyid**
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: CHILD_R_DONE
**Event:EV_ACTIVATE_NEW_SA**
*11 ноября 19:31:35.882: индекс ikev2 3 МиБ
IKEv2:Store, платформа 62
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: Событие CHILD_R_DONE:
EV_UPDATE_CAC_STATS
*11 ноября 19:31:35.882: запрос IKEv2:New ikev2 sa
активирован
*11 ноября 19:31:35.882: IKEv2:Failed для постепенного
уменьшения счета для входящего согласования
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState:  Событие **CHILD_R_DONE**: EV_CHECK_DUPE
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: Событие CHILD_R_DONE: EV_OK
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: Событие CHILD_R_DONE:
EV_START_DEL_NEG_TMR
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2): Действие:
Action_Null
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003
CurState: Событие EXIT: EV_CHK_PENDING
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Передаваемый ответ с идентификатором сообщения 3,
Запросы могут быть приняты из диапазона 4 - 8
*11 ноября 19:31:35.882: IKEv2: (ID SA = 2):
Трассировка SM-> SA: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R) MsgID =
00000003 **CurState: Событие EXIT** : EV_NO_EVENT

# Туннельная проверка

## ISAKMP

**Команда**

**show crypto ikev2 sa detailed**

### Выходные данные маршрутизатора 1

```
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
```

### Выходные данные маршрутизатора 2

```
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

### Команда

**show crypto ipsec sa**

> **Примечание:** В этих выходных данных, в отличие от этого в IKEv1, групповое значение DH безопасной пересылки (PFS) появляется как "безопасная пересылка (PFS) (Y/N): N, группа DH: ни один" во время первого согласования туннеля, но, после повторно введения не происходит, правильные значения появляются. Это не дефект, даже при том, что поведение описано в идентификаторе ошибки Cisco CSCug67056.

Различие между IKEv1 и IKEv2 - то, что в последнем Дочерние SA созданы как часть самого обмена AUTH. DH Group, настроенная под криптокартой, использовалась бы только во время, повторно вводят. Следовательно, вы видели бы 'безопасную пересылку (PFS) (Y/N): N, группа DH: ни один' до первого не повторно вводит.

С IKEv1 вы видите другое поведение, потому что создание Child SA происходит во время Быстрого режима, и сообщение CREATE_CHILD_SA имеет условие для переноса информационного наполнения Обмена ключами, которое задает параметры DH для получения нового общего секретного ключа.

### Выходные данные маршрутизатора 1

```
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:
```

## Выходные данные маршрутизатора 2

```
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:
```

Можно также проверить выходные данные **команды show crypto session** на обоих маршрутизаторах; эти выходные данные показывают статус туннельного сеанса как АКТИВНЫЙ ПРОТИВ UP.

```
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
```

# Дополнительные сведения

- Обмен пакетами IKEv2 и отладка уровня протокола
- Cisco Systems – техническая поддержка и документация