

Отладки ASA IKEv2 для сквозного VPN-соединение с PSK

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Базовая проблема](#)

[Используемые отладки](#)

[Конфигурации ASA](#)

[ASA1](#)

[ASA2](#)

[Отладка](#)

[Дочерние отладки сопоставления безопасности](#)

[Туннельная проверка](#)

[ISAKMP](#)

[IPSec](#)

[Дополнительные сведения](#)

[Введение](#)

Когда общий ключ (PSK) используется, этот документ предоставляет сведения для понимания отладок IKEv2 на Устройстве адаптивной защиты (ASA).

[Предварительные условия](#)

[Требования](#)

Для этого документа отсутствуют особые требования.

[Используемые компоненты](#)

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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 того, что это было в IKEv1. Принимая во внимание, что в IKEv1 был ясно разграниченный обмен phase1, который состоял из 6 пакетов, придерживавшихся обменом фазы 2, который состоял из 3 пакетов, обмен IKEv2 является переменным. Для более подробной информации о различиях и пояснении обмена пакетами, обратитесь к [Отладке Обмена пакетами и Уровня протокола IKEv2.](#)

Используемые отладки

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
```

Конфигурации ASA

ASA1

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.0

interface GigabitEthernet0/2
 nameif inside
 security-level 100
 ip address 192.168.1.2 255.255.255.0

crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5

access-list 121_list extended permit ip host 192.168.1.1
 host 192.168.2.99
access-list 121_list extended permit ip host 192.168.1.12
 host 192.168.2.99

crypto map outside_map 1 match address 121_list
crypto map outside_map 1 set peer 10.0.0.2
crypto map outside_map 1 set ikev2 ipsec-proposal AES256
crypto map outside_map interface outside

crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 2
 prf sha
 lifetime seconds 86400

crypto ikev2 enable outside

tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

ASA2

```
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.0.0.2 255.255.255.0

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 192.168.2.1 255.255.255.0

crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5

access-list l2l_list extended permit ip host 192.168.2.99
host 191.168.1.1
access-list l2l_list extended permit ip host 192.168.2.99
host 191.168.1.12

crypto map outside_map 1 match address l2l_list
crypto map outside_map 1 set peer 10.0.0.1
crypto map outside_map 1 set ikev2 ipsec-proposal AES256
crypto map outside_map interface outside

crypto ikev2 policy 1
encryption aes-256
integrity sha
group 2
prf sha
lifetime seconds 86400

crypto ikev2 enable outside
tunnel-group 10.0.0.1 type ipsec-l2l
tunnel-group 10.0.0.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

Отладка

ASA1 (инициатор) описание сообщения	Отладка	ASA2 (респондент) описание сообщения
ASA1 получает пакет, который совпадает с крипто-	IKEv2-PLAT-3: attempting to find tunnel group for IP: 10.0.0.2 IKEv2-PLAT-3: mapped to tunnel group 10.0.0.2 using peer IP IKEv2-PLAT-3: my_auth_method = 2 IKEv2-PLAT-3: supported_peers_auth_method = 2 IKEv2-PLAT-3: P1 ID = 0 IKEv2-PLAT-3: Translating IKE_ID_AUTO to = 255	

<p>асл для однора нгового ASA 10.0.0.2 . Создан ие Initiates SA.</p>	<pre>IKEv2-PLAT-3: (16) tp_name set to: IKEv2-PLAT-3: (16) tg_name set to: 10.0.0.2 IKEv2-PLAT-3: (16) tunn grp type set to: L2L IKEv2-PLAT-5: New ikev2 sa request admitted IKEv2-PLAT-5: Incrementing outgoing negotiating sa count by one</pre>	
<p>Первая пара сообще ний являетс я обмено м IKE_SA _INIT. Эти сообще ния выполн яют согласо вание о криптог рафиче ских алгорит мах, обмени ваются параме трами и делают Обмен Диффи - Хеллма на. Соотве тствующ ая конфиг урация: crypto ikev2 policy 1 encrypti on aes-256</p>	<pre>IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: IDLE Event: EV_INIT_SA IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_IKE_POLICY IKEv2-PROTO-3: (16): Getting configured policies IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_SET_POLICY IKEv2-PROTO-3: (16): Setting configured policies IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_CHK_AUTH4PKI IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GEN_DH_KEY IKEv2-PROTO-3: (16): Computing DH public key IKEv2-PROTO-3: (16): IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_NO_EVENT IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_OK_RECD_DH_PUBKEY_RESP IKEv2-PROTO-5: (16): Action: Action_Null IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_CONFIG_MODE IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958</pre>	

<pre> integrit y sha group 2 prf sha lifetime seconds 86400 crypto ikev2 enable outside Tunnel Group matching the identity name is present: tunnel- group 10.0.0.2 type ipsec- 121 tunnel- group 10.0.0.2 ipsec- attribut es ikev2 remote- authenti cation pre- shared- key ***** ikev2 local- authenti cation pre- shared- key ***** </pre>		
<p>Инициатор создает пакет</p>	<pre> R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_BLD_MSG IKEv2-PROTO-2: (16): Sending initial message IKEv2-PROTO-3: Tx [L </pre>	

IKE_INI
T_SA.
Это
содерж
ит:

1. За

го
ло
во
к
IS
AK
M
P-
SP
I/v
er
sio
n/fl
ag
s
2. SA
i1
-
кр
ип
то
гр
а
ф
ич
ес
ки
й
ал
го
ри
тм
то
т
ин
иц
иа
то
р
ИК
Е
по

```
10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0]
m_id: 0x0 IKEv2-PROTO-3:
HDR[i:DFA3B583A4369958 - r:
0000000000000000] IKEv2-PROTO-4: IKEV2
HDR ispi: DFA3B583A4369958 - rspi:
0000000000000000 IKEv2-PROTO-4: Next
payload: SA, version: 2.0 IKEv2-PROTO-4:
Exchange type: IKE_SA_INIT, flags:
INITIATOR IKEv2-PROTO-4: Message id: 0x0,
length: 338 SA Next payload: KE,
reserved: 0x0, length: 48 IKEv2-PROTO-4:
last proposal: 0x0, reserved: 0x0,
length: 44 Proposal: 1, Protocol id: IKE,
SPI size: 0, #trans: 4 IKEv2-PROTO-4:
last transform: 0x3, reserved: 0x0:
length: 12 type: 1, reserved: 0x0, id:
AES-CBC IKEv2-PROTO-4: last transform:
0x3, reserved: 0x0: length: 8 type: 2,
reserved: 0x0, id: SHA1 IKEv2-PROTO-4:
last transform: 0x3, reserved: 0x0:
length: 8 type: 3, reserved: 0x0, id:
SHA96 IKEv2-PROTO-4: last transform: 0x0,
reserved: 0x0: length: 8 type: 4,
reserved: 0x0, id:
DH_GROUP_1024_MODP/Group 2 KE Next
payload: N, reserved: 0x0, length: 136 DH
group: 2, Reserved: 0x0 19 65 43 45 d2 72
a7 11 b8 a4 93 3f 44 95 6c b8 6d 5a f0 f8
1f f3 d4 b9 ff 41 7b 0d 13 90 82 cf 34 2e
74 e3 03 6e 9e 00 88 80 5d 86 2c 4c 79 35
ee e6 98 91 89 f3 48 83 75 09 02 f1 3c b1
7f f5 be 05 f1 fa 7e 8a 4c 43 eb a9 2c 3a
47 c0 68 40 f5 dd 02 9d a5 b5 a2 a6 90 64
95 fc 57 b5 69 e8 b2 4f 8e f2 a5 05 e3 c7
17 f9 c0 e0 c8 3e 91 ed c1 09 23 3e e5 09
4f be 1a 6a d4 d9 fb 65 44 ld N Next
payload: VID, reserved: 0x0, length: 24
84 8b 80 c2 52 6c 4f c7 f8 08 b8 ed! 52
af a2 f4 d5 dd d4 f4 VID Next payload:
VID, reserved: 0x0, length: 23 43 49 53
43 4f 2d 44 45 4c 45 54 45 2d 52 45 41 53
4f 4e VID Next payload: VID, reserved:
0x0, length: 59 43 49 53 43 4f 28 43 4f
50 59 52 49 47 48 54 29 26 43 6f 70 79 72
69 67 68 74 20 28 63 29 20 32 30 30 39 20
43 69 73 63 6f 20 53 79 73 74 65 6d 73 2c
20 49 6e 63 2e VID Next payload: NONE,
reserved: 0x0, length: 20 40 48 b7 d5 6e
bc e8 85 25 e7 de 7f 00 d6 c2 d3
```

ДД ер жк и 3. Ке і - зн ач ен ие от кр ыт ог о кл юч а Д Н ин иц иа то ра 4. Па ра ме тр Н- ин иц иа то ра		
Инициатор передается.	IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [10.0.0.1]:500->[10.0.0.2]:500	
-----Инициатор передал IKE_INIT_SA----->		
	IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [10.0.0.1]:500->[10.0.0.2]:500 InitSPI=0xdfa3b583a4369958 RespSPI=0x0000000000000000 MID=00000000	Респондент получает IKEV_I NIT_SA .

	<pre> IKEv2-PROTO-3: Rx [L 10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0] m_id: 0x0 IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 0000000000000000] IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 - rspi: 0000000000000000 IKEv2-PROTO-4: Next payload: SA, version: 2.0 IKEv2-PROTO-4: Exchange type: IKE_SA_INIT, flags: INITIATOR IKEv2-PROTO-4: Message id: 0x0, length: 338 IKEv2-PLAT-5: New ikev2 sa request admitted IKEv2-PLAT-5: Incrementing incoming negotiating sa count by one SA Next payload: KE, reserved: 0x0, length: 48 IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0, length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 IKEv2-PROTO-4: last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 KE Next payload: N, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000000 CurState: IDLE Event: EV_RECV_INIT IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) </pre>	<p>Респон дент иниции рует создан ие SA для того узла.</p>
	<pre> MsgID = 00000000 CurState: R_INIT Event: EV_VERIFY_MSG IKEv2-PROTO-3: (16): Verify SA init message IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000000 CurState: R_INIT Event: EV_INSERT_SA IKEv2-PROTO-3: (16): Insert SA IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000000 CurState: R_INIT Event: EV_GET_IKE_POLICY IKEv2-PROTO-3: (16): Getting configured policies IKEv2-PROTO- 5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000000 CurState: R_INIT Event:EV_PROC_MSG IKEv2-PROTO-2: (16): Processing initial message IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 </pre>	<p>Респон дент провер яет и обраба тывает сообще ние IKE_INI T:</p> <p>1. В ыб ир ае т кр ип</p>


```

R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_INIT Event:
EV_DETECT_NAT IKEv2-PROTO-3: (16):
Process NAT discovery notify IKEv2-PROTO-
5: (16): No NAT found IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_INIT Event:
EV_CHK_CONFIG_MODE IKEv2-PROTO-5: (16):
SM Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_SET_POLICY IKEv2-PROTO-3: (16):
Setting configured policies IKEv2-PROTO-
5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_CHK_AUTH4PKI IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_PKI_SESH_OPEN IKEv2-PROTO-3: (16):
Opening a PKI session IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_GEN_DH_KEY IKEv2-PROTO-3: (16):
Computing DH public key IKEv2-PROTO-3:
(16): IKEv2-PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_NO_EVENT IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_OK_REC'D_DH_PUBKEY_RESP IKEv2-PROTO-5:
(16): Action: Action_Null IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_GEN_DH_SECRET IKEv2-PROTO-3: (16):
Computing DH secret key IKEv2-PROTO-3:
(16): IKEv2-PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_NO_EVENT IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_OK_REC'D_DH_SECRET_RESP IKEv2-PROTO-5:
(16): Action: Action_Null IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958_I_SPI=27C943C13FD946
65 (R) MsgID = 00000000 CurState:
R_BLD_INIT Event: EV_GEN_SKEYID IKEv2-
PROTO-3: (16): Generate skeyid IKEv2-
PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958

```

ТО
-
КО
МП
ЛЕ
КТ
ИЗ
ПР
ЕД
ЛА
ГА
ЕМ
ЫХ
ИН
ИЦ
ИА
ТО
РО
М.
2. В
ЫЧ
ИС
ЛЯ
ЕТ
ЕГ
О
СО
БС
ТВ
ЕН
НЫ
Й
СЕ
КРЕ
ТНЫ
Й
КЛ
ЮЧ
Д
Н.
3. ЭТ
О
ТА
КЖ
Е
ВЫ

чи
сл
яе
т
зн
ач
ен
ие
sk
eyi
d,
из
ко
то
ро
го
вс
е
кл
юч
и
мо
гу
т
бы
ть
по
лу
че
ны
дл
я
эт
ог
о
IK
E_
S
A.
Вс
е
кр
ом
е
за
го
ло

R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_GET_CONFIG_MODE IKEv2-PROTO-5: (16):
SM Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000000 CurState: R_BLD_INIT Event:
EV_BLD_MSG

		ВК ОВ ВС ЕХ СО ОБ Щ ЕН ИЙ , КО ТО РЫ Е ПР ИД ЕР ЖИ ВА ЮТ СЯ, Ш И Ф РУ ЮТ СЯ И АУ ТЕ НТ И Ф ИЦ ИР ЮЮ ТС Я. Кл юч и, ис по ль зу ем ые
--	--	--

		Д Л я ш и ф р о в а н и я и з а щ и т ы ц е л о с т н о с т и, п о л у ч е н ы и з S K E Y I D и и з в е с т н ы к а к: о. S K_ е (ш и ф р о в а н и
--	--	---

е).
b.
S
K_
a
(а
ут
ен
ти
ф
ик
ац
ия
).
с.
S
K_
d
по
лу
ча
ет
ся
и
ис
по
ль
зу
ет
ся
дл
я
де
ри
ва
ци
и
да
ль
ней
ше
го
ма
те
ри

		ал а дл я ко ди ро ва ни я дл я С Н I L D _S As . От де ль ны й S K_ е и S K_ а вы чи сл ен ы дл я ка жд ог о на пр ав ле ни я.
--	--	--

Соответствующая конфигурация:

```
crypto
ikev2

policy 1
encryption
    aes-
    256
integrity sha
group 2
prf sha
lifetime
seconds
    86400
crypto
ikev2

enable

outside

Tunnel
Group
matching
the
identity
name
is
present:

tunnel-
group

10.0.0.1
type
ipsec-
121
tunnel-
group

10.0.0.1

ipsec-

attribut
es
ikev2
remote-

authenti
cation
pre-
shared-
key
****
ikev2
```

		local- authenti- cation pre- shared- key *****
	<p>IKEv2-PROTO-2: (16): Sending initial message IKEv2-PROTO-3: IKE Proposal: 1, SPI size: 0 (initial negotiation), Num. transforms: 4 AES-CBC SHA1 SHA96 DH_GROUP_1024_MODP/Group 2 IKEv2-PROTO-5: Construct Vendor Specific Payload: FRAGMENTATIONIKEv2-PROTO-3: Tx [L 10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0] m_id: 0x0 IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665] IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 - rspi: 27C943C13FD94665 IKEv2-PROTO-4: Next payload: SA, version: 2.0 IKEv2-PROTO-4: Exchange type: IKE_SA_INIT, flags: RESPONDER MSG-RESPONSE IKEv2-PROTO-4: Message id: 0x0, length: 338 SA Next payload: KE, reserved: 0x0, length: 48 IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0, length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 IKEv2-PROTO-4: last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 KE Next payload: N, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0</p>	<p>ASA2 создает сообще- ние респон- дента для обмена IKE_SA _INIT, которы й получе- н ASA1. Этот пакет содерж- ит:</p> <p>1. За- го- ло- во- к- IS- A- K- M- P- (S- PI- /- ве- рс- ия- /ф- ла- ги)</p> <p>2. S- Ar- 1- (к- ри- пт</p>

		о р а ф и ч е с к и й а л г о р и т м , к о т о р ы й р е с п о н д е н т и к е в ы б и р а е т) 3. К Е г (з н а ч е н и е о т к р ы т о г о к л ю ч а D H р е с п
--	--	--

он
де
нт
а)
4. Па
ра
ме
тр
ре
сп
он
де
нт
а

IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT]
[10.0.0.2]:500->[10.0.0.1]:500
InitSPI=0xdfa3b583a4369958
RespSPI=0x27c943c13fd94665
MID=00000000

ASA2
отсыла
ет
сообщ
ение
респон
дента в
ASA1.

←-----Респондент передал
IKE_INIT_SA-----

ASA1
получа
ет
ответн
ый
пакет
IKE_SA
_INIT от
ASA2.

IKEv2-PLAT-4: RECV
PKT
[IKE_SA_INIT]
[10.0.0.2]:500->
[10.0.0.1]:500
InitSPI=0xdfa3b583a
4369958
RespSPI=0x27c943c13
fd94665
MID=00000000

IKEv2-PROTO-5:
(16):
SM Trace->
SA:
I_SPI=DFA3B583A4369
958
R_SPI=27C943C13FD94
665 (R)
MsgID = 00000000
CurState:
INIT_DONE
Event: EV_DONE
IKEv2-PROTO-3:
(16):
Fragmentation is
enabled
IKEv2-PROTO-3:
(16): Cisco
DeleteReason
Notify
is enabled
IKEv2-PROTO-3:
(16): Complete
SA init exchange
IKEv2-PROTO-5:
(16):
SM Trace->
SA:
I_SPI=DFA3B583A4369
958

Респон
дент
запуска
ет
таймер
для
Подлин
ного
процес
са.

		<pre> R_SPI=27C943C13FD94 665 (R) MsgID = 00000000 CurState: INIT_DONE Event: EV_CHK4_ROLE IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (R) MsgID = 00000000 CurState: INIT_DONE Event: EV_START_TMR IKEv2-PROTO-3: (16): Starting timer to wait for auth message (30 sec) IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (R) MsgID = 00000000 CurState: R_WAIT_AUTH Event: EV_NO_EVENT </pre>	
--	--	---	--

<p>ASA1 провер яет и обраба тывает ответ:</p> <p>1. Се кр ет ны й кл юч D H ин иц иа то ра вы чи</p>	<pre> IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0] m_id: 0x0 IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665] IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 - rspi: 27C943C13FD94665 IKEv2-PROTO-4: Next payload: SA, version: 2.0 IKEv2-PROTO-4: Exchange type: IKE_SA_INIT, flags: RESPONDER MSG-RESPONSE IKEv2-PROTO-4: Message id: 0x0, length: 338 SA Next payload: KE, reserved: 0x0, length: 48 IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0, length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: </pre>	
--	---	--

Сл
ен
2. Ин
иц
иа
то
р
sk
ey
d
та
ж
е
ге
не
ри
ру
ет
ся

```
length: 8 type: 2, reserved: 0x0, id:
SHA1
IKEv2-PROTO-4:      last transform: 0x3,
reserved: 0x0:
length: 8 type: 3, reserved: 0x0, id:
SHA96
IKEv2-PROTO-4:      last transform: 0x0,
reserved: 0x0:
length: 8 type: 4, reserved: 0x0,
id: DH_GROUP_1024_MODP/Group 2
KE Next payload: N, reserved: 0x0,
length: 136
DH group: 2, Reserved: 0x0

IKEv2-PROTO-5: (16): SM Trace->
SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I)
MsgID = 00000000 CurState: I_WAIT_INIT
Event: EV_RECV_INIT
IKEv2-PROTO-5: (16): Processing initial
message IKEv2-PROTO-5: (16): SM Trace->
SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000000 CurState: I_PROC_INIT Event:
EV_CHK4_NOTIFY IKEv2-PROTO-2: (16):
Processing initial message IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000000 CurState: I_PROC_INIT Event:
EV_VERIFY_MSG IKEv2-PROTO-3: (16): Verify
SA init message IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000000 CurState: I_PROC_INIT Event:
EV_PROC_MSG IKEv2-PROTO-2: (16):
Processing initial message IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000000 CurState: I_PROC_INIT Event:
EV_DETECT_NAT IKEv2-PROTO-3: (16):
Process NAT discovery notify IKEv2-PROTO-
3: (16): NAT-T is disabled IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000000 CurState: I_PROC_INIT Event:
EV_CHK_NAT_T IKEv2-PROTO-3: (16): Check
NAT discovery IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000000 CurState: I_PROC_INIT Event:
EV_CHK_CONFIG_MODE IKEv2-PROTO-5: (16):
SM Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000000 CurState: INIT_DONE Event:
EV_GEN_DH_SECRET IKEv2-PROTO-3: (16):
Computing DH secret key IKEv2-PROTO-3:
(16): IKEv2-PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000000 CurState: INIT_DONE Event:
EV_NO_EVENT IKEv2-PROTO-5: (16): SM
```

	<pre>Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_OK_REC'D_DH_SECRET_RESP IKEv2-PROTO-5: (16): Action: Action_Null IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_GEN_SKEYID IKEv2-PROTO-3: (16): Generate skeyid IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_DONE IKEv2-PROTO-3: (16): Fragmentation is enabled IKEv2-PROTO-3: (16): Cisco DeleteReason Notify is enabled</pre>	
<p>Обмен IKE_INIT_SA между ASA теперь заверш ен.</p>	<pre>IKEv2-PROTO-3: (16): Complete SA init exchange</pre>	
<p>Инициа тор запуска ет обмен "IKE_A UTH" и запуска ет генера цию опозна ватель ного инфор мацион ного наполн ения. Пакет IKE_AUTH содерж ит: 1. За го ло во к</p>	<pre>IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_GEN_AUTH IKEv2-PROTO-3: (16): Generate my authentication data IKEv2-PROTO-3: (16): Use preshared key for id 10.0.0.1, key len 5 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_CHK_AUTH_TYPE IKEv2-PROTO-3: (16): Get my authentication method IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_OK_AUTH_GEN IKEv2-PROTO-3: (16): Check for EAP exchange IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_SEND_AUTH IKEv2-PROTO-2: (16): Sending auth message IKEv2-PROTO-5: Construct Vendor Specific Payload: CISCO-GRANITE IKEv2-PROTO-3: ESP Proposal: 1, SPI size: 4 (IPSec negotiation), Num. transforms: 4 AES-CBC SHA96 MD596 IKEv2-PROTO-5: Construct Notify Payload: INITIAL_CONTACT IKEv2-PROTO-5: Construct Notify Payload: ESP_TFC_NO_SUPPORT IKEv2-PROTO-5:</pre>	

IS
AK
M
P
(S
PI
/
ве
р
с
ия
/ф
ла
ги)
.
2. IDI
(и
де
нт
ич
но
ст
ь
ин
иц
иа
то
ра
).
3. Ин
ф
ор
ма
ци
он
но
е
на
по
лн
ен
ие
А
УТ
Н.
4. SA
i2
(и

Construct Notify Payload: NON_FIRST_FRAGS
IKEv2-PROTO-3: (16): Building packet for encryption; contents are: VID Next payload: IDi, reserved: 0x0, length: 20 dd a3 b4 83 b7 01 6a 1f 3d b7 84 1a 75 e6 83 a6 IDi Next payload: AUTH, reserved: 0x0, length: 12 Id type: IPv4 address, Reserved: 0x0 0x0 47 01 01 01 AUTH Next payload: SA, reserved: 0x0, length: 28 Auth method PSK, reserved: 0x0, reserved 0x0 Auth data: 20 bytes SA Next payload: TSi, reserved: 0x0, length: 52 IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0, length: 48 Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 4 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: MD596 IKEv2-PROTO-4: last transform: 0x0, reserved: 0x0: length: 8 type: 5, reserved: 0x0, id: TSi Next payload: TSr, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 192.168.1.1, end addr: 192.168.1.1 TSr Next payload: NOTIFY, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 192.168.2.99, end addr: 192.168.2.99 IKEv2-PROTO-3: Tx [L 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0] m_id: 0x1 IKEv2-PROTO-3:
HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665] IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 - rspi: 27C943C13FD94665 IKEv2-PROTO-4: Next payload: ENCR, version: 2.0 IKEv2-PROTO-4: Exchange type: IKE_AUTH, flags: INITIATOR IKEv2-PROTO-4: Message id: 0x1, length: 284 ENCR Next payload: VID, reserved: 0x0, length: 256 Encrypted data: 252 bytes

ни
ци
ир
уе
т
по
до
бн
ое
SA
об
ме
ну
на
бо
ра
пр
ео
бр
аз
ов
ан
ий
ф
аз
ы
2
в
IK
Ev
1).

5. TS
I и
TS
г
(И
ни
ци
ат
ор
и
Се
ле
кт
ор
ы
тр

а
ф
ик
а
Ре
сп
он
де
нт
а):
Он
и
со
де
рж
ат
ад
ре
с
ис
то
чн
ик
а
и
на
зн
ач
ен
ия
ин
иц
иа
то
ра
и
ре
сп
он
де
нт
а
со
от
ве
ст
ств

ен
но
дл
я
пе
ре
да
чи
за
ш
и
ф
ро
ва
нн
ог
о
по
то
ка
да
нн
ых
. Ди
ап
аз
он
ад
ре
со
в
ук
аз
ыв
ает,
что
будет
т
ту
нн
ел
ир
ов

ан
ве
сь
тр
а
ф
ик
к и
из
то
го
ди
ап
аз
он
а.
Ес
ли
пр
ед
ло
же
ни
е
пр
ие
мл
ем
о
дл
я
ре
сп
он
де
нт
а,
он
о
пе
ре
да
ет
ид
ен
ти
чн

ые
ин
ф
ор
ма
ци
он
ны
е
на
по
лн
ен
ия
TS
об
ра
тно.

1-й
CHILD_
SA
создан
для
проху_I
D пары,
которая
совпад
ает с
триггер
ным
пакето
м.
**Соотве
тствующ
ая
конфиг
урация:**
crypto
ipsec
ikev2

ipsec-
proposal

AES256

protocol
esp

encrypti
on
aes-

<pre> 256 protocol esp integrity sha-1 md5 access- list l2l_list extended permit ip host 10.0.0.2 host 10.0.0.1 </pre>		
ASA1 отсылает пакет IKE_AUTH в ASA2.	<pre> IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:500->[10.0.0.2]:500 InitSPI=0xdfa3b583a4369958 RespSPI=0x27c943c13fd94665 MID=00000001 </pre>	
<p>-----Инициатор передал IKE_AUTH-----></p>		
	<pre> IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [10.0.0.1]:500->[10.0.0.2]:500 InitSPI=0xdfa3b583a4369958 RespSPI=0x27c943c13fd94665 MID=00000001 </pre>	ASA2 получает этот пакет от ASA1.
	<pre> IKEv2-PROTO-3: Rx [L 10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0] m_id: 0x1 IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665] IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 - rspi: 27C943C13FD94665 IKEv2-PROTO-4: Next payload: ENCR, version: 2.0 IKEv2-PROTO-4: Exchange type: IKE_AUTH, flags: INITIATOR IKEv2-PROTO-4: Message id: 0x1, length: 284 IKEv2-PROTO-5: (16): Request has mess_id 1; expected 1 through 1 REAL Decrypted packet: Data: 216 bytes IKEv2-PROTO-5: Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDi, reserved: 0x0, </pre>	ASA2 останавливает подлинный таймер и проверяет данные проверки подлинности, полученные от ASA1.

<pre> length: 20 dd a3 b4 83 b7 01 6a 1f 3d b7 84 1a 75 e6 83 a6 IDi Next payload: AUTH, reserved: 0x0, length: 12 Id type: IPv4 address, Reserved: 0x0 0x0 47 01 01 01 AUTH Next payload: SA, reserved: 0x0, length: 28 Auth method PSK, reserved: 0x0, reserved 0x0 Auth data: 20 bytes SA Next payload: TSi, reserved: 0x0, length: 52 IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0, length: 48 Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 4 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: MD596 IKEv2-PROTO-4: last transform: 0x0, reserved: 0x0: length: 8 type: 5, reserved: 0x0, id: TSi Next payload: TSr, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 192.168.1.1, end addr: 192.168.1.1 TSr Next payload: NOTIFY, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 192.168.2.99, end addr: 192.168.2.99 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_RECV_AUTH IKEv2-PROTO-3: (16): Stopping timer to wait for auth message IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_CHK_NAT_T IKEv2-PROTO-3: (16): Check NAT discovery IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_PROC_ID IKEv2-PROTO-2: (16): Recieved valid parameteres in process id IKEv2- PLAT-3: (16) peer auth method set to: 2 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_F OR_PROF_SEL IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = </pre>	<p>Затем это генерирует свои собственные данные проверки подлинности, точно как ASA1 сделал. Соответствующая конфигурация:</p> <pre> crypto ipsec ikev2 ipsec- proposal AES256 protocol esp encryption aes- 256 protocol esp integrity sha-1 md5 </pre>
--	--

```
00000001 CurState: R_WAIT_AUTH Event:
EV_GET_POLICY_BY_PEERID IKEv2-PROTO-3:
(16): Getting configured policies IKEv2-
PLAT-3: attempting to find tunnel group
for ID: 10.0.0.1 IKEv2-PLAT-3: mapped to
tunnel group 10.0.0.1 using phase 1 ID
IKEv2-PLAT-3: (16) tg_name set to:
10.0.0.1 IKEv2-PLAT-3: (16) tunn grp type
set to: L2L IKEv2-PLAT-3: my_auth_method
= 2 IKEv2-PLAT-3:
supported_peers_auth_method = 2 IKEv2-
PLAT-3: P1 ID = 0 IKEv2-PLAT-3:
Translating IKE_ID_AUTO to = 255 IKEv2-
PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_WAIT_AUTH Event:
EV_SET_POLICY IKEv2-PROTO-3: (16):
Setting configured policies IKEv2-PROTO-
5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_WAIT_AUTH Event:
EV_VERIFY_POLICY_BY_PEERID IKEv2-PROTO-3:
(16): Verify peer's policy IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_WAIT_AUTH Event:
EV_CHK_CONFIG_MODE IKEv2-PROTO-5: (16):
SM Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_WAIT_AUTH Event:
EV_CHK_AUTH4EAP IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_WAIT_AUTH Event:
EV_CHK_POLREQEAP IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_VERIFY_AUTH Event:
EV_CHK_AUTH_TYPE IKEv2-PROTO-3: (16): Get
peer authentication method IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_VERIFY_AUTH Event:
EV_GET_PRESHR_KEY IKEv2-PROTO-3: (16):
Get peer's preshared key for 10.0.0.1
IKEv2-PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_VERIFY_AUTH Event:
EV_VERIFY_AUTH IKEv2-PROTO-3: (16):
Verify authentication data IKEv2-PROTO-3:
(16): Use preshared key for id 10.0.0.1,
key len 5 IKEv2-PROTO-5: (16): SM Trace->
SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R) MsgID =
00000001 CurState: R_VERIFY_AUTH Event:
EV_GET_CONFIG_MODE IKEv2-PLAT-2: Build
config mode reply: no request stored
IKEv2-PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
```

	<pre> R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK4_IC IKEv2-PROTO-3: (16): Processing initial contact IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK_REDIRECT IKEv2-PROTO-5: (16): Redirect check is not needed, skipping it IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_PROC_SA_TS IKEv2-PROTO-2: (16): Processing auth message IKEv2-PLAT-3: Selector received from peer is accepted IKEv2-PLAT-3: PROXY MATCH on crypto map outside_map seq 1 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_NO_EVENT IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_OK_REC'D_IPSEC_RESP IKEv2-PROTO-2: (16): Processing auth message </pre>	
	<pre> IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_MY_AUTH_METHOD IKEv2-PROTO-3: (16): Get my authentication method IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_GET_PRESHR_KEY IKEv2-PROTO-3: (16): Get peer's preshared key for 10.0.0.1 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_GEN_AUTH IKEv2-PROTO-3: (16): Generate my authentication data IKEv2-PROTO-3: (16): Use preshared key for id 10.0.0.2, key len 5 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_CHK4_SIGN IKEv2-PROTO-3: (16): Get my authentication method IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_OK_AUTH_GEN </pre>	<p>Пакет IKE_AU TH, переда нный от ASA2, содерж ит:</p> <p>1. За го ло во к IS A К М P (S PI / ве рс ия /ф ла ги)</p>

```

IKEv2-PROTO-5: (16): SM Trace->
  SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (R)
  MsgID = 00000001 CurState: R_BLD_AUTH
  Event: EV_SEND_AUTH
IKEv2-PROTO-2: (16): Sending auth message
IKEv2-PROTO-5: Construct Vendor Specific
Payload:
  CISCO-GRANITE
IKEv2-PROTO-3:   ESP Proposal: 1, SPI
size: 4 (IPSec
  negotiation),
Num. transforms: 3
  AES-CBC   SHA96
IKEv2-PROTO-5: Construct Notify Payload:
  ESP_TFC_NO_SUPPORTIKEv2-PROTO-5:
  Construct Notify Payload:
NON_FIRST_FRAGSIKEv2-PROTO-3:
  (16):
Building packet for encryption; contents
are:
  VID Next payload: IDr, reserved: 0x0,
length: 20
    25 c9 42 c1 2c ee b5 22 3d b7 84 1a
75 e6 83 a6
  IDr Next payload: AUTH, reserved: 0x0,
length: 12 Id type: IPv4 address,
Reserved: 0x0 0x0 51 01 01 01 AUTH Next
payload: SA, reserved: 0x0, length: 28
Auth method PSK, reserved: 0x0, reserved
0x0 Auth data: 20 bytes SA Next payload:
TSi, reserved: 0x0, length: 44 IKEv2-
PROTO-4: last proposal: 0x0, reserved:
0x0, length: 40 Proposal: 1, Protocol id:
ESP, SPI size: 4, #trans: 3 IKEv2-PROTO-
4: last transform: 0x3, reserved: 0x0:
length: 12 type: 1, reserved: 0x0, id:
AES-CBC IKEv2-PROTO-4: last transform:
0x3, reserved: 0x0: length: 8 type: 3,
reserved: 0x0, id: SHA96 IKEv2-PROTO-4:
last transform: 0x0, reserved: 0x0:
length: 8 type: 5, reserved: 0x0, id: TSi
Next payload: TSr, reserved: 0x0, length:
24 Num of TSs: 1, reserved 0x0, reserved
0x0 TS type: TS_IPV4_ADDR_RANGE, proto
id: 0, length: 16 start port: 0, end
port: 65535 start addr: 192.168.1.1, end
addr: 192.168.1.1 TSr Next payload:
NOTIFY, reserved: 0x0, length: 24 Num of
TSs: 1, reserved 0x0, reserved 0x0 TS
type: TS_IPV4_ADDR_RANGE, proto id: 0,
length: 16 start port: 0, end port: 65535
start addr: 192.168.2.99, end addr:
192.168.2.99 NOTIFY(ESP_TFC_NO_SUPPORT)
Next payload: NOTIFY, reserved: 0x0,
length: 8 Security protocol id: IKE, spi
size: 0, type: ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) Next payload:
NONE, reserved: 0x0, length: 8 Security
protocol id: IKE, spi size: 0, type:
NON_FIRST_FRAGS IKEv2-PROTO-3: Tx [L
10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0]
m_id: 0x1 IKEv2-PROTO-3:
HDR[i:DFA3B583A4369958 - r:

```

.

2. ID

r

(и

де

нт

ич

но

ст

ь

ре

сп

он

де

нт

а).

3. Ин

ф

ор

ма

ци

он

но

е

на

по

лн

ен

ие

А

У

Т

Н.

4. S

Ar

2

(и

ни

ци

ир

уе

т

по

до

бн

ое

S

А
об
ме
ну
на
бо
ра
пр
ео
бр
аз
ов
ан
ий
ф
аз
ы
2
в
IK
Ev
1).
5. TS
I
и
TS
г
(И
ни
ци
ат
ор
и
Се
ле
кт
ор
ы
тр
а
ф
ик
а
Ре
сп
он
де
нт

```
27C943C13FD94665] IKEv2-PROTO-4: IKEV2
HDR ispi: DFA3B583A4369958 - rspi:
27C943C13FD94665 IKEv2-PROTO-4: Next
payload: ENCR, version: 2.0 IKEv2-PROTO-
4: Exchange type: IKE_AUTH, flags:
RESPONDER MSG-RESPONSE IKEv2-PROTO-4:
Message id: 0x1, length: 236 ENCR Next
payload: VID, reserved: 0x0, length: 208
Encrypted data: 204 bytes
```

		а): О ни со де рж ат ад ре с ис то чн ик а и на зн ач ен ия Ин иц иа то ра и Ре сп он де нт а со от ве тс тв ен но дл я пе ре да чи за
--	--	--

		Ш и ф ро ва нн ог о по то ка да нн ых . Ди ап аз он ад ре со в ук аз ыв ае т, чт о бу де т ту нн ел ир ов ан ве сь тр а ф ик ки из
--	--	---

то
го
ди
ап
аз
он
а.
Эт
и
па
ра
ме
тр
ы
ид
ен
ти
чн
ы
то
му
,
ко
то
ры
й
бы
л
по
лу
че
н
от
A
S
A1
.

IKEv2-PLAT-4: SENT PKT [IKE_AUTH]
[10.0.0.2]:500->[10.0.0.1]:500
InitSPI=0xdfa3b583a4369958
RespSPI=0x27c943c13fd94665
MID=00000001

Респон
дент
переда
ет
ответ
за
IKE_AU
TH.

<-----Респондент передал-----

Инициа

IKEv2-PLAT-4:

IKEv2-PROTO-5:

Респон

<p>тор получа ет ответ от Респон дента.</p>	<p>RECV PKT [IKE_AUTH] [10.0.0.2]:500-> [10.0.0.1]:500 InitSPI=0xdfa3b583a 4369958 RespSPI=0x27c943c13 fd94665 MID=00000001</p>	<pre>(16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK IKEv2-PROTO-5: (16): Action: Action_Null IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_PKI_SESH_CLOSE IKEv2-PROTO-3: (16): Closing the PKI session IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_INSERT_IKE IKEv2-PROTO-2: (16): SA created; inserting SA into database</pre>	<p>ДЕНТ ВСТАВЛ ЯЕТ ЗАПИСЬ В SAD.</p>
<p>ASA1 провер яет и обраба тывает данные провер ки ПОДЛИН НОСТИ В</p>	<pre>IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0] m_id: 0x1 IKEv2-PROTO-3: HDR[i:DFA3B583A4369958 - r: 27C943C13FD94665] IKEv2-PROTO-4: IKEV2 HDR ispi: DFA3B583A4369958 - rspi: 27C943C13FD94665 IKEv2-PROTO-4: Next payload: ENCR, version: 2.0 IKEv2-PROTO-4: Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE IKEv2-PROTO-4: Message id: 0x1, length:</pre>		

ЭТОМ пакете. ASA1 тогда вставля ет ЭТОТ SA в свой SAD.

```
236
REAL Decrypted packet:Data: 168 bytes
IKEv2-PROTO-5: Parse Vendor Specific
Payload: (CUSTOM) VID
  Next payload: IDr, reserved: 0x0,
length: 20

    25 c9 42 c1 2c ee b5 22 3d b7 84 1a
75 e6 83 a6
  IDr Next payload: AUTH, reserved: 0x0,
length: 12
  Id type: IPv4 address, Reserved: 0x0
0x0

    51 01 01 01
  AUTH Next payload: SA, reserved: 0x0,
length: 28
  Auth method PSK, reserved: 0x0,
reserved 0x0
  Auth data: 20 bytes
  SA Next payload: TSi, reserved: 0x0,
length: 44
IKEv2-PROTO-4: last proposal: 0x0,
reserved: 0x0,
  length: 40 Proposal: 1, Protocol id:
ESP, SPI size: 4,
  #trans: 3
IKEv2-PROTO-4: last transform: 0x3,
reserved: 0x0:
  length: 12 type: 1, reserved: 0x0, id:
AES-CBC
IKEv2-PROTO-4: last transform: 0x3,
reserved: 0x0:
  length: 8 type: 3, reserved: 0x0, id:
SHA96
IKEv2-PROTO-4: last transform: 0x0,
reserved: 0x0:
  length: 8 type: 5, reserved: 0x0, id:

  TSi Next payload: TSr, reserved: 0x0,
length: 24 Num of TSs: 1, reserved 0x0,
reserved 0x0 TS type: TS_IPV4_ADDR_RANGE,
proto id: 0, length: 16 start port: 0,
end port: 65535 start addr: 192.168.1.1,
end addr: 192.168.1.1 TSr Next payload:
NOTIFY, reserved: 0x0, length: 24 Num of
TSs: 1, reserved 0x0, reserved 0x0 TS
type: TS_IPV4_ADDR_RANGE, proto id: 0,
length: 16 start port: 0, end port: 65535
start addr: 192.168.2.99, end addr:
192.168.2.99 IKEv2-PROTO-5: Parse Notify
Payload: ESP_TFC_NO_SUPPORT
NOTIFY(ESP_TFC_NO_SUPPORT) Next payload:
NOTIFY, reserved: 0x0, length: 8 Security
protocol id: IKE, spi size: 0, type:
ESP_TFC_NO_SUPPORT IKEv2-PROTO-5: Parse
Notify Payload: NON_FIRST_FRAGS
NOTIFY(NON_FIRST_FRAGS) Next payload:
NONE, reserved: 0x0, length: 8 Security
protocol id: IKE, spi size: 0, type:
NON_FIRST_FRAGS Decrypted packet:Data:
236 bytes IKEv2-PROTO-5: (16): SM Trace->
SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
```

```
00000001 CurState: I_WAIT_AUTH Event:
EV_RECV_AUTH IKEv2-PROTO-5: (16): Action:
Action_Null IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_CHK4_NOTIFY IKEv2-PROTO-2: (16):
Process auth response notify IKEv2-PROTO-
5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_PROC_MSG IKEv2-PLAT-3: (16) peer auth
method set to: 2 IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_
FOR_PROF_SEL IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_GET_POLICY_BY_PEERID IKEv2-PROTO-3:
(16): Getting configured policies IKEv2-
PLAT-3: connection initiated with tunnel
group 10.0.0.2 IKEv2-PLAT-3: (16) tg_name
set to: 10.0.0.2 IKEv2-PLAT-3: (16) tunn
grp type set to: L2L IKEv2-PLAT-3:
my_auth_method = 2 IKEv2-PLAT-3:
supported_peers_auth_method = 2 IKEv2-
PLAT-3: P1 ID = 0 IKEv2-PLAT-3:
Translating IKE_ID_AUTO to = 255 IKEv2-
PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_VERIFY_POLICY_BY_PEERID IKEv2-PROTO-3:
(16): Verify peer's policy IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_CHK_AUTH_TYPE IKEv2-PROTO-3: (16): Get
peer authentication method IKEv2-PROTO-5:
(16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_GET_PRESHR_KEY IKEv2-PROTO-3: (16):
Get peer's preshared key for 10.0.0.2
IKEv2-PROTO-5: (16): SM Trace-> SA:
I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_VERIFY_AUTH IKEv2-PROTO-3: (16):
Verify authentication data IKEv2-PROTO-3:
(16): Use preshared key for id 10.0.0.2,
key len 5 IKEv2-PROTO-5: (16): SM Trace->
SA: I_SPI=DFA3B583A4369958
R_SPI=27C943C13FD94665 (I) MsgID =
00000001 CurState: I_PROC_AUTH Event:
EV_CHK_EAP IKEv2-PROTO-3: (16): Check for
EAP exchange IKEv2-PROTO-5: (16): SM
Trace-> SA: I_SPI=DFA3B583A4369958
```

	<pre> R_SPI=27C943C13FD94665 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_CONFIG_MODE IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_IKE_ONLY IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_PROC_SA_TS IKEv2-PROTO-2: (16): Processing auth message IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK IKEv2-PROTO-5: (16): Action: Action_Null IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_PKI_SESH_CLOSE IKEv2-PROTO-3: (16): Closing the PKI session IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_INSERT_IKE IKEv2-PROTO-2: (16): SA created; inserting SA into database </pre>		
<p>Туннель подключен на Инициаторе.</p>	<pre> CONNECTION STATUS: UP... peer: 10.0.0.2:500, phase1_id: 10.0.0.2 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_REGISTER_SESSION </pre>	<pre> CONNECTION STATUS: UP... peer: 10.0.0.1:500, phase1_id: 10.0.0.1 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_REGISTER_SESSION </pre>	<p>Туннель подключен на Респонденте. Туннель Респондента обычно подходит ит перед Инициатором.</p>
<p>Процес с регистрации IKEv2.</p>	<pre> IKEv2-PLAT-3: (16) connection auth hdl set to 15 IKEv2-PLAT-3: AAA conn attribute retrieval successfully queued for register session request. IKEv2-PROTO-3: (16): </pre>	<pre> IKEv2-PLAT-3: (16) connection auth hdl set to 15 IKEv2-PLAT-3: AAA conn attribute retrieval successfully queued for register session request. IKEv2-PROTO-3: (16): IKEv2-PROTO-5: </pre>	<p>Процес с регистрации IKEv2.</p>

<pre> IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_NO_EVENT IKEv2-PLAT-3: (16) idle timeout set to: 30 IKEv2-PLAT-3: (16) session timeout set to: 0 IKEv2-PLAT-3: (16) group policy set to DfltGrpPolicy IKEv2-PLAT-3: (16) class attr set IKEv2-PLAT-3: (16) tunnel protocol set to: 0x5c IKEv2-PLAT-3: IPv4 filter ID not configured for connection IKEv2-PLAT-3: (16) group lock set to: none IKEv2-PLAT-3: IPv6 filter ID not configured for connection IKEv2-PLAT-3: (16) connection attribues set valid to TRUE IKEv2-PLAT-3: Successfully retrieved conn attrs IKEv2-PLAT-3: Session registration after conn attr retrieval PASSED, No error IKEv2-PLAT-3: CONNECTION STATUS: REGISTERED... peer: </pre>	<pre> (16): SM Trace-> SA: I_SPI=DFA3B583A4369 958 R_SPI=27C943C13FD94 665 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_NO_EVENT IKEv2-PLAT-3: (16) idle timeout set to: 30 IKEv2-PLAT-3: (16) session timeout set to: 0 IKEv2-PLAT-3: (16) group policy set to DfltGrpPolicy IKEv2-PLAT-3: (16) class attr set IKEv2-PLAT-3: (16) tunnel protocol set to: 0x5c IKEv2-PLAT-3: IPv4 filter ID not configured for connection IKEv2-PLAT-3: (16) group lock set to: none IKEv2-PLAT-3: IPv6 filter ID not configured for connection attribues set valid to TRUE IKEv2-PLAT-3: Successfully retrieved conn attrs IKEv2-PLAT-3: Session registration after conn attr retrieval PASSED, No error IKEv2-PLAT-3: CONNECTION STATUS: REGISTERED... peer: 10.0.0.1:500, phase1_id: 10.0.0.1 </pre>	
--	--	--

10.0.0.2:500, phase1_id: 10.0.0.2		
--------------------------------------	--	--

Дочерние отладки сопоставления безопасности

Этот обмен состоит из одиночной пары запроса/ответа и упоминался как обмен фазы 2 в IKEv1. Это MIGHT инициироваться к любому концу IKE_SA после начальных обменов завершено.

Описание сообщения ASA1 CHILD_SA	Отладка	Описание сообщения ASA2 CHILD_SA
	<pre> IKEv2-PLAT-5: INVALID PSH HANDLE IKEv2-PLAT-3: attempting to find tunnel group for IP: 10.0.0.1 IKEv2-PLAT-3: mapped to tunnel group 10.0.0.1 using peer IP IKEv2-PLAT-3: my_auth_method = 2 IKEv2-PLAT-3: supported_peers_auth_method = 2 IKEv2-PLAT-3: P1 ID = 0 IKEv2-PLAT-3: Translating IKE_ID_AUTO to = 255 IKEv2-PLAT-3: (226) tp_name set to: IKEv2-PLAT-3: (226) tg_name set to: 10.0.0.1 IKEv2-PLAT-3: (226) tunn grp type set to: L2L IKEv2-PLAT-3: PSH cleanup IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000001 CurState: READY Event: EV_INIT_CREATE_CHILD IKEv2- PROTO-5: (225): Action: Action_Null IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000001 CurState: CHILD_I_INIT Event: EV_INIT_CREATE_CHILD IKEv2-PROTO-5: (225): Action: Action_Null IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000001 CurState: CHILD_I_IPSEC Event: EV_INIT_CREATE_CHILD IKEv2-PROTO-3: (225): Check for IPSEC rekey IKEv2-PROTO- 5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000001 CurState: CHILD_I_IPSEC Event: EV_SET_IPSEC_DH_GRP IKEv2-PROTO-3: (225): Set IPSEC DH group IKEv2-PROTO-5: (225): </pre>	<p>ASA2 инициирует обмен CHILD_SA. Это - запрос CREATE_CHILD_SA. Пакет CHILD_SA, как правило, содержит:</p> <p style="text-align: center;">1. H D R S A (v er sio n.f la gs /e xc ha ng e</p>

ти
п)
2. Параметр (дополнительный) Ni: Если CHILD_SA создана как часть начальной обмена на , в оро еи н ф о р ма ци

```
SM Trace-> SA: I_SPI=FD366326E1FED6FE
R_SPI=A75B9B2582AAECB7 (I) MsgID =
00000001 CurState: CHILD_I_IPSEC Event:
EV_CHK4_PFS IKEv2-PROTO-3: (225):
Checking for PFS configuration IKEv2-
PROTO-5: (225): SM Trace-> SA:
I_SPI=FD366326E1FED6FE
R_SPI=A75B9B2582AAECB7 (I) MsgID =
00000001 CurState: CHILD_I_IPSEC Event:
EV_BLD_MSG IKEv2-PROTO-2: (225): Sending
child SA exchange IKEv2-PROTO-3:?ESP
Proposal: 1, SPI size: 4 (IPSec
negotiation), num. transforms: 4 AES-
CBC?SHA96?MD596 IKEv2-PROTO-3: (225):
Building packet for encryption; contents
are: SA?Next payload: N, reserved: 0x0,
length: 52 IKEv2-PROTO-4:?last proposal:
0x0, reserved: 0x0, length: 48 Proposal:
1, Protocol id: ESP, SPI size: 4, #trans:
4 IKEv2-PROTO-4:?last transform: 0x3,
reserved: 0x0: length: 12 type: 1,
reserved: 0x0, id: AES-CBC IKEv2-PROTO-
4:?last transform: 0x3, reserved: 0x0:
length: 8 type: 3, reserved: 0x0, id:
SHA96 IKEv2-PROTO-4:?last transform: 0x3,
reserved: 0x0: length: 8 type: 3,
reserved: 0x0, id: MD596 IKEv2-PROTO-
4:?last transform: 0x0, reserved: 0x0:
length: 8 type: 5, reserved: 0x0, id: N
Next payload: TSi, reserved: 0x0, length:
24 2d 3e ec 11 e0 c7 5d 67 d5 23 25 76 1d
50 0d 05 fa b7 f0 48 TSi?Next payload:
TSr, reserved: 0x0, length: 24 Num of
TSs: 1, reserved 0x0, reserved 0x0 TS
type: TS_IPV4_ADDR_RANGE, proto id: 0,
length: 16 start port: 0, end port: 65535
start addr: 192.168.2.99, end addr:
192.168.2.99 TSr?Next payload: NONE,
reserved: 0x0, length: 24 Num of TSs: 1,
reserved 0x0, reserved 0x0 TS type:
TS_IPV4_ADDR_RANGE, proto id: 0, length:
16 start port: 0, end port: 65535 start
addr: 192.168.1.12, end addr:
192.168.1.12 IKEv2-PROTO-3: (225):
Checking if request will fit in peer
window IKEv2-PROTO-3: Tx [L
10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0]
m_id: 0x6 IKEv2-PROTO-3:
HDR[i:FD366326E1FED6FE - r:
A75B9B2582AAECB7] IKEv2-PROTO-4: IKEV2
HDR ispi: FD366326E1FED6FE - rspi:
A75B9B2582AAECB7 IKEv2-PROTO-4: Next
payload: ENCR, version: 2.0 IKEv2-PROTO-
4: Exchange type: CREATE_CHILD_SA, flags:
INITIATOR IKEv2-PROTO-4: Message id: 0x6,
length: 180 ENCR?Next payload: SA,
reserved: 0x0, length: 152 Encrypted
data: 148 bytes
```

он
но
е
на
по
лн
ен
ие
К
Е
и
па
ра
ме
тр
не
Д
О
Л
Ж
Н
Ы
бы
ть
пе
ре
да
ны

3. Ин
ф
ор
ма
ци
он
но
е
на
по
лн
ен
ие
S
A

4. (К
лю
че

ВО
Й
ДО
ПО
ЛН
ИТ
ЕЛ
ЬН
ЫЙ
)
К
Ei:
C
R
E
AT
E_
C
HI
LD
_S
A
за
пр
а
ш
ив
аю
т,
чт
об
ы
MI
G
H
T
до
по
лн
ит
ел
ьн
о
со
де
рж
ал

		ин ф ор ма ци он но е на по лн ен ие К Е дл я до по лн ит ел ьн ог о об ме на Д Н дл я вк лю че ни я бо ле е си ль ны х га ра нт
--	--	--

ий
пр
ям
ой
се
кр
ет
но
ст
и
дл
я
С
Н
I
L
D
_S
A.
?
Ес
ли
пр
ед
ло
же
ни
я
S
A
вк
лю
ча
ют
др
уг
ие
гр
уп
пы
D
H,
K
Ei,
M
U
ST
яв
ля

		ет ся эл ем ен то м гр уп пы , ко то ру ю ин иц иа то р ож ид ае т, чт о ре сп он де нт пр им ет. ? Ес ли эт о не уг ад ае т, то об ме
--	--	--

Н
С
Р
Е
А
Т
Е_
С
Н
И
Л
Д
_S
А
от
ка
же
т,
и
эт
о
до
лж
но
бу
де
т
по
вт
ор
ит
ь с
др
уг
им
К
Еі.

5. **Н**
(У
ве
до
мл
яю
т
до
по
лн
ит
ел
ьн

		ый ин ф ор ма ци он ны м на по лн ен ие м): Ув ед ом ля ть Ин ф ор ма ци он но е на по лн ен ие , ис по ль зу ет ся дл я пе ре да чи ин
--	--	---

		ф ор ма ци он ны х да нн ых , та ки х ка к со ст оя ни я о ш иб ки и из ме не ни я со ст оя ни я, к уз лу К Е. Ув ед ом ля ть Ин
--	--	--

		ф ор ма ци он но е на по лн ен ие мо гл о бы по яв ит ьс я в от ве тн ом со об щ ен ии (о бы чн о оп ре де ле ни е, по че му за пр ос
--	--	---

бы
л
от
клон
ен
)
в
И
Н
Ф
О
Р
М
А
Ц
И
О
Н
Н
О
М
Ex
ch
an
ge
(д
ля
со
зд
ан
ия
от
че
то
в
об
о
ш
иб
ке
не
в
за
пр
ос
е

		И К Е), ил и в лю бо м др уг ом со об щ ен ии , чт об ы ук аз ат ь на во зм ож но ст и от пр ав ит ел я ил и мо ди ф иц ир ов ат ь
--	--	---

		зн ач ен ие за пр ос а. Ес ли эт от об ме н С R E A T E_ C H I L D _S A по вт ор но вв од ит су щ ес тв ую щ ий S A кр ом е I K E_ S
--	--	--

А,
пр
од
ви
же
ни
е
N
ин
ф
ор
ма
ци
он
но
е
на
по
лн
ен
ие
ти
па
R
E
K
E
Y_
S
A,
M
U
ST
оп
ре
де
ля
ет
S
A,
ко
то
ры
й
по
вт
ор

		НО ВВ ЕД ЕН .? Ес ли эт от об ме н С R Е АТ Е_ С НІ LD _S А не по вт ор но ВВ од ит су щ ес тв ую щ ий S А, ин ф ор ма ци он но е
--	--	---

на
по
лн
ен
ие
N,
M
U
ST
оп
у
щ
ен

.
6. TS
I и
(д
оп
ол
ни
те
ль
ны
й)
TS
г:
Эт
о
по
ка
зы
ва
ет
се
ле
кт
ор
ы
тр
а
ф
ик
а,
дл
я
ко
то

		<p>ры х бы л с о з д ан S A. В эт ом сл уч ае эт о ме жд у хо ст ам и 19 2. 16 8. 1. 12 и 19 2. 16 8. 2. 99 .</p>	
<p>ASA1 получа ет этот пакет.</p>	<p>IKEv2-PLAT-4: RECV PKT [CREATE_CHILD_SA] [10.0.0.2]:500-> [10.0.0.1]:500 InitSPI=0xfd366326e 1fed6fe RespSPI=0xa75b9b258 2aaecb7 MID=00000006 IKEv2- PROTO-3: Rx [L 10.0.0.1:500/R</p>	<p>IKEv2-PLAT-4: SENT PKT [CREATE_CHILD_SA] [10.0.0.2]:500-> [10.0.0.1]:500 InitSPI=0xfd366326e 1fed6fe RespSPI=0xa75b9b258 2aaecb7 MID=00000006 IKEv2- PROTO-5: (225): SM</p>	<p>ASA2 переда ет этот пакет и ждет ответа.</p>

	10.0.0.2:500/VRF i0:f0] m_id: 0x6	Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAE CB7 (I) MsgID = 00000006 CurState: CHILD_I_WAIT Event: EV_NO_EVENT	
ASA1 получает этот точный пакет от ASA2 и проверяет его.	IKEv2-PROTO-3: HDR[i:FD366326E1FED6FE - r: A75B9B2582AAE CB7] IKEv2-PROTO-4: IKEV2 HDR ispi: FD366326E1FED6FE - rspi: A75B9B2582AAE CB7 IKEv2-PROTO-4: Next payload: ENCR, version: 2.0 IKEv2-PROTO-4: Exchange type: CREATE_CHILD_SA, flags: INITIATOR IKEv2-PROTO-4: Message id: 0x6, length: 180 IKEv2-PROTO-5: (225): Request has mess_id 6; expected 6 through 6 REAL Decrypted packet:Data: 124 bytes SA?Next payload: N, reserved: 0x0, length: 52 IKEv2-PROTO-4:?last proposal: 0x0, reserved: 0x0, length: 48 Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 4 IKEv2-PROTO-4:?last transform: 0x3, reserved: 0x0: length: 12 ype: 1, reserved: 0x0, id: AES-CBC IKEv2-PROTO-4:?last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 IKEv2-PROTO-4:?last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: MD596 IKEv2-PROTO-4:?last transform: 0x0, reserved: 0x0: length: 8 type: 5, reserved: 0x0, id: N Next payload: TSi, reserved: 0x0, length: 24 2d 3e ec 11 e0 c7 5d 67 d5 23 25 76 1d 50 0d 05 fa b7 f0 48 TSi Next payload: TSr, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 192.168.2.99, end addr: 192.168.2.99 TSr ?Next payload: NONE, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 192.168.1.12, end addr: 192.168.1.12 Decrypted packet:Data: 180 bytes IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE		

	<pre> R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: READY Event: EV_RECV_CREATE_CHILD IKEv2-PROTO-5: (225): Action: Action_Null IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: CHILD_R_INIT Event: EV_RECV_CREATE_CHILD IKEv2-PROTO-5: (225): Action: Action_Null IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: CHILD_R_INIT Event: EV_VERIFY_MSG IKEv2-PROTO-3: (225): Validating create child message IKEv2- PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 urState: CHILD_R_INIT Event: EV_CHK_CC_TYPE </pre>	
<p>ASA1 теперь создает ответ для обмена CHILD_ SA. Это - Ответ CREAT E_CHIL D_SA. Пакет CHILD_ SA, как правил о, содерж ит:</p> <p>1. H D R SA (v er sio n.fl ag s/e xc ha ng e ти</p>	<pre> IKEv2-PROTO-3: (225): Check for create child response message type IKEv2-PROTO-5: (225): SM Trace-> SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: CHILD_R_IPSEC Event: EV_PROC_MSG IKEv2-PROTO-2: (225): Processing child SA exchange IKEv2-PLAT-3: Selector received from peer is accepted IKEv2-PLAT-3: PROXY MATCH on crypto map outside_map seq 1 IKEv2-PROTO-5: (225): SM Trace-> SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: CHILD_R_IPSEC Event: EV_NO_EVENT IKEv2-PROTO-5: (225): SM Trace-> SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000005 CurState: EXIT Event: EV_FREE_NEG IKEv2-PROTO-5: (225): Deleting negotiation context for peer message ID: 0x5 IKEv2-PROTO-5: (225): SM Trace-> SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: CHILD_R_IPSEC Event: EV_OK_RECD_IPSEC_RESP IKEv2-PROTO-5: (225): Action: Action_Null IKEv2-PROTO-5: (225): SM Trace-> SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: CHILD_R_IPSEC Event: EV_PROC_MSG IKEv2-PROTO-2: (225): Processing child SA exchange IKEv2-PROTO- 5: (225): SM Trace-> SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: CHILD_R_IPSEC Event: EV_SET_IPSEC_DH_GRP IKEv2-PROTO-3: (225): Set IPSEC DH group IKEv2-PROTO-5: (225): SM Trace-> SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = </pre>	

п) 00000006 CurState: CHILD_R_IPSEC Event:
2. **П** EV_OK IKEv2-PROTO-3: (225): Requesting
а SPI from IPsec IKEv2-PROTO-5: (225): SM
р Trace-> SA:I_SPI=FD366326E1FED6FE
а R_SPI=A75B9B2582AAECB7 (R) MsgID =
е 00000006 CurState: CHILD_R_WAIT_SPI
т Event: EV_OK_GOT_SPI IKEv2-PROTO-5:
р (225): Action: Action_Null IKEv2-PROTO-5:
((225): SM Trace->
д SA:I_SPI=FD366326E1FED6FE
о R_SPI=A75B9B2582AAECB7 (R) MsgID =
п 00000006 CurState: CHILD_R_BLD_MSG Event:
и EV_CHK4_PFS IKEv2-PROTO-3: (225):
т Checking for PFS configuration IKEv2-
е PROTO-5: (225): SM Trace->
ль SA:I_SPI=FD366326E1FED6FE
ны R_SPI=A75B9B2582AAECB7 (R) MsgID =
й) 00000006 CurState: CHILD_R_BLD_MSG Event:
№: EV_BLD_MSG IKEv2-PROTO-2: (225): **Sending**
Ес **child SA exchange** IKEv2-PROTO-3:?ESP
ли Proposal: 1, SPI size: 4 (IPsec
С negotiation), Num. transforms: 3 AES-
Н CBC?SHA96? IKEv2-PROTO-3: (225): Building
И packet for encryption; contents are: SA
LD Next payload: N, reserved: 0x0, length:
_S 44 IKEv2-PROTO-4:?last proposal: 0x0,
А reserved: 0x0, length: 40 Proposal: 1,
со Protocol id: ESP, SPI size: 4, #trans: 3
зд IKEv2-PROTO-4:?last transform: 0x3,
ан reserved: 0x0: length: 12 type: 1,
ка reserved: 0x0, id: AES-CBC IKEv2-PROTO-
к 4:?last transform: 0x3, reserved: 0x0:
ча length: 8 type: 3, reserved: 0x0, id:
ст SHA96 IKEv2-PROTO-4:?last transform: 0x0,
ь reserved: 0x0: length: 8 type: 5,
на reserved: 0x0, id: N?Next payload: TSi,
ча reserved: 0x0, length: 24 b7 6a c6 75 53
ль 55 99 5a df ee 05 18 1a 27 a6 cb 01 56 22
но ad **TSi** Next payload: TSr, reserved: 0x0,
го length: 24 Num of TSs: 1, reserved 0x0,
об reserved 0x0 TS type: TS_IPV4_ADDR_RANGE,
ме proto id: 0, length: 16 start port: 0,
на end port: 65535 start addr: 192.168.2.99,
, end addr: 192.168.2.99 **TSr**?Next payload:
в NONE, reserved: 0x0, length: 24 Num of
т TSs: 1, reserved 0x0, reserved 0x0 TS
ор type: TS_IPV4_ADDR_RANGE, proto id: 0,
ое length: 16 start port: 0, end port: 65535
ин start addr: 192.168.1.12, end addr:
ф 192.168.1.12 IKEv2-PROTO-3: Tx [L
ор 10.0.0.1:500/R 10.0.0.2:500/VRF i0:f0]
ма m_id: 0x6 IKEv2-PROTO-3:
ци HDR[i:FD366326E1FED6FE - r:
он A75B9B2582AAECB7] IKEv2-PROTO-4: **IKEV2**
он HDR ispi: FD366326E1FED6FE - rspi:
A75B9B2582AAECB7 IKEv2-PROTO-4: Next
payload: ENCR, version: 2.0 IKEv2-PROTO-
4: **Exchange type: CREATE_CHILD_SA, flags:**
RESPONDER MSG-RESPONSE IKEv2-PROTO-4:
Message id: 0x6, length: 172 ENCR?Next
payload: SA, reserved: 0x0, length: 144
Encrypted data: 140 bytes

но
е
на
по
лн
ен
ие
КЕ
и
па
ра
ме
тр
не
Д
О
Л
Ж
Н
Ы
бы
ть
пе
ре
да
ны
.

3. Ин
ф
ор
ма
ци
он
но
е
на
по
лн
ен
ие
SA

4. (К
лю
че
во
й
до

ПО
ЛН
ИТ
ЕЛ
ЬН
ЫЙ
)
КЕ
і:
С
R
ЕА
ТЕ
_С
НІ
LD
_S
А
за
пр
а
ш
ив
аю
т,
чт
об
ы
М
АУ
до
по
лн
ит
ел
ьн
о
со
де
рж
ал
ин
ф
ор
ма
ци
он

но
е
на
по
лн
ен
ие
КЕ
дл
я
до
по
лн
ит
ел
ьн
ог
о
об
ме
на
D
H
дл
я
вк
лю
че
ни
я
бо
ле
е
си
ль
ны
х
га
ра
нт
ий
пр
ям
ой
се
кр
ет

НО
СТ
И
ДЛ
Я
С
НІ
LD
_S
А.
?
Ес
ли
пр
ед
ло
же
ни
я
SA
вк
лю
ча
ют
др
уг
ие
гр
уп
пы
D
H,
KE
і,
M
U
ST
яв
ля
ет
ся
эл
ем
ен
то
м
гр

уп
пы
,
ко
то
ру
ю
ин
иц
иа
то
р
ож
ид
ае
т,
чт
о
ре
сп
он
де
нт
пр
им
ет.
?
Ес
ли
эт
о
не
уг
ад
ыв
ае
т,
сб
ои
об
ме
на
С
R
ЕА
ТЕ
_С

Н
Л
_S
А,
и
эт
о
до
лж
но
бу
де
т
по
вт
ор
ит
ь с
др
уг
им
КЕ
і.

5. N
(У
ве
до
мл
яю
т
до
по
лн
ит
ел
ьн
ый
ин
ф
ор
ма
ци
он
ны
м
на
по

лн
ен
ие
м):
Ув
ед
ом
ля
ть
Ин
ф
ор
ма
ци
он
но
е
на
по
лн
ен
ие
ис
по
ль
зу
ет
ся
дл
я
пе
ре
да
чи
ин
ф
ор
ма
ци
он
ны
х
да
нн
ых
,
та

ки
х
ка
к
о
ш
иб
ка
?
ус
ло
ви
я
и
из
ме
не
ни
я
со
ст
оя
ни
я,
к
уз
лу
К
Е.
?
Ув
ед
ом
ля
ть
Ин
ф
ор
ма
ци
он
но
е
на
по
лн
ен

ие
мо
гл
о
бы
по
яв
ит
ьс
я
в
от
ве
тн
ом
со
об
щ
ен
ии
(о
бы
чн
о
за
да
ет,
по
че
му
за
пр
ос
бы
л
от
кл
он
ен
),
в
И
Н
Ф
О
Р
М

А
Ц
И
О
Н
Н
О
М
Ex
ch
an
ge
(д
ля
со
зд
ан
ия
от
че
то
в
об
о
ш
иб
ке
не
в
за
пр
ос
е
IK
E),
ил
и
в
лю
бо
м
др
уг
ом
со
об
щ

ен
ии
,
чт
об
ы
ук
аз
ат
ь
на
во
зм
ож
но
ст
и
от
пр
ав
ит
ел
я
ил
и
мо
ди
ф
иц
ир
ов
ат
ь
зн
ач
ен
ие
за
пр
ос
а.
Ес
ли
эт
от
об
ме

Н
С
R
E
A
T
E
_C
H
I
L
D
_S
A
по
в
т
о
р
н
о
в
в
о
д
и
т
с
у
щ
е
с
т
в
у
ю
щ
и
й
S
A
кр
ом
е
I
K
E_
S
A
, пр
од
ви
же
ни
е
N
ин
ф
ор
ма
ци
он
но
е

на
по
лн
ен
ие
ти
па
R
EK
EY
_S
A,
M
U
ST
оп
ре
де
ля
ет
SA
,
ко
то
ры
й
по
вт
ор
но
вв
ед
ен
.?
Ес
ли
эт
от
об
ме
н
C
R
EA
TE
_C
HI

<p>LD _S A не по вт ор но вв од ит су щ ес тв ую щ ий SA , ин ф ор ма ци он но е на по лн ен ие N, M U ST оп ущ ен . 6. TS I и (д оп ол ни</p>		
--	--	--

те
ль
ны
й)
TS
г:
Эт
о
по
ка
зы
ва
ет
се
ле
кт
ор
ы
тр
а
ф
ик
а,
дл
я
ко
то
ры
х
бы
л
со
зд
ан
SA
. В
эт
ом
сл
уч
ае
эт
о
ме
жд
у
хо

<p>СТ ам и 19 2. 16 8. 1. 12 и 19 2. 16 8. 2. 99 .</p>			
<p>ASA1 отсыла ет ответ.</p>	<p>IKEv2-PLAT-4: SENT PKT [CREATE_CHILD_SA] [10.0.0.1]:500-> [10.0.0.2]:500 InitSPI=0xfd366326e 1fed6fe RespSPI=0xa75b9b258 2aaecb7 MID=00000006</p>	<p>IKEv2-PLAT-4: RECV PKT [CREATE_CHILD_SA] [10.0.0.1]:500-> [10.0.0.2]:500 InitSPI=0xfd366326e 1fed6fe RespSPI=0xa75b9b258 2aaecb7 MID=00000006 IKEv2- PROTO-3: Rx [L 10.0.0.2:500/R 10.0.0.1:500/VRF i0:f0] m_id: 0x6</p>	<p>ASA2 получа ет этот пакет.</p>
	<p>IKEv2-PROTO-3: HDR[i:FD366326E1FED6FE - r: A75B9B2582AAECB7] IKEv2-PROTO-4: IKEV2 HDR ispi: FD366326E1FED6FE - rspi: A75B9B2582AAECB7 IKEv2-PROTO-4: Next payload: ENCR, version: 2.0 IKEv2-PROTO- 4: Exchange type: CREATE_CHILD_SA, flags: RESPONDER MSG-RESPONSE IKEv2-PROTO-4: Message id: 0x6, length: 172 REAL Decrypted packet:Data: 116 bytes SA Next payload: N, reserved: 0x0, length: 44 IKEv2-PROTO-4:?last proposal: 0x0, reserved: 0x0, length: 40 Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 IKEv2-PROTO-4:?last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC IKEv2-PROTO- 4:?last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 IKEv2-PROTO-4:?last transform: 0x0, reserved: 0x0: length: 8 type: 5, reserved: 0x0, id: N?Next payload: TSi, reserved: 0x0, length: 24 b7 6a c6 75 53 55 99 5a df ee 05 18 1a 27 a6 cb 01 56 22 ad TSi?Next payload: TSr, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0,</p>	<p>ASA2 теперь провер яет пакет</p>	

	<pre> reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 192.168.2.99, end addr: 192.168.2.99 Tsr Next payload: NONE, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 192.168.1.12, end addr: 192.168.1.12 Decrypted packet:Data: 172 bytes IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000006 CurState: CHILD_I_WAIT Event: EV_RECV_CREATE_CHILD IKEv2-PROTO-5: (225): Action: Action_Null IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000006 CurState: CHILD_I_PROC Event: EV_CHK4_NOTIFY IKEv2-PROTO-2: (225): Processing any notify-messages in child SA exchange IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000006 CurState: CHILD_I_PROC Event: EV_VERIFY_MSG IKEv2-PROTO-3: (225): Validating create child message IKEv2- PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000006 CurState: CHILD_I_PROC Event: EV_PROC_MSG IKEv2-PROTO-2: (225): Processing child SA exchange IKEv2-PROTO- 5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000006 CurState: CHILD_I_PROC Event: EV_CHK4_PFS IKEv2-PROTO-3: (225): Checking for PFS configuration IKEv2- PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000006 CurState: CHILD_I_PROC Event: EV_CHK_IKE_REKEY IKEv2-PROTO-3: (225): Checking if IKE SA rekey IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (I) MsgID = 00000006 CurState: CHILD_I_PROC Event: EV_GEN_LOAD_IPSEC IKEv2-PROTO-3: (225): Load IPSEC key material IKEv2-PLAT-3: PROXY MATCH on crypto map outside_map seq 1 IKEv2-PLAT-3: (225) DPD Max Time will be: 10 IKEv2-PLAT-3: (225) DPD Max Time will be: 10 </pre>		
ASA1 вставля ет эту дочерн юю запись	<pre> IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED 6FE R_SPI=A75B9B2582AAE </pre>	<pre> IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED 6FE R_SPI=A75B9B2582AAE </pre>	ASA2 вставл яет эту дочерн юю запись

<p>SA в базу данных сопоставления безопасности.</p>	<pre> CB7 (R) MsgID = 00000006 CurState: CHILD_R_DONE Event: EV_OK IKEv2-PROTO- 2: (225): SA created; inserting SA into database IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED 6FE R_SPI=A75B9B2582AAE CB7 (R) MsgID = 00000006 CurState: CHILD_R_DONE Event: EV_START_DEL_NEG_TM R </pre>	<pre> CB7 (I) MsgID = 00000006 CurState: CHILD_I_DONE Event: EV_OK IKEv2-PROTO- 2: (225): SA created; inserting SA into database </pre>	<p>SA в базу данных сопоставления безопасности.</p>
---	---	---	---

Туннельная проверка

ISAKMP

Команда

```
show crypto isakmp sa det
```

Выходные данные

ASA1

```

ASA1(config)#sh cry isa sa det There are no IKEv1 SAs IKEv2
SAs:Session-id:99220, Status:UP-ACTIVE, IKE count:1, CHILD
count:2 Tunnel-id Local Remote Status Role 1889403559
10.0.0.1/500 10.0.0.2/500 READY RESPONDER Encr: 3DES, Hash:
MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK Life/Active
Time: 86400/195 sec Session-id: 99220 Status Description:
Negotiation done Local spi: A75B9B2582AAECB7 Remote spi:
FD366326E1FED6FE Local id: 10.0.0.1 Remote id: 10.0.0.2 Local
req mess id: 14 Remote req mess id: 16 Local next mess id: 14
Remote next mess id: 16 Local req queued: 14 Remote req
queued: 16 Local window: 1 Remote window: 1 DPD configured
for 10 seconds, retry 2 NAT-T is not detected Child sa: local
selector 192.168.1.12/0 - 192.168.1.12/65535 remote selector
192.168.2.99/0 - 192.168.2.99/65535 ESP spi in/out:
0x8564387d/0x8717a5a AH spi in/out: 0x0/0x0 CPI in/out:
0x0/0x0 Encr: AES-CBC, keysize: 256, esp_hmac: SHA96 ah_hmac:
None, comp: IPCOMP_NONE, mode tunnel Child sa: local selector
192.168.1.1/0 - 192.168.1.1/65535 remote selector
192.168.2.99/0 - 192.168.2.99/65535 ESP spi in/out:
0x74756292/0xf0d97b2a AH spi in/out: 0x0/0x0 CPI in/out:
0x0/0x0 Encr: AES-CBC, keysize: 256, esp_hmac: SHA96 ah_hmac:
None, comp: IPCOMP_NONE, mode tunnel

```

ASA2

```

ASA2(config)#sh cry isa sa det There are no IKEv1 SAs IKEv2
SAs: Session-id:99220, Status:UP-ACTIVE, IKE count:1, CHILD

```



```
count:2 Tunnel-id???????????????? Local????????????????
Remote??? Status???????? Role 472237395????????
10.0.0.2/500???????? 10.0.0.1/500????? READY?? INITIATOR ?????
Encr: 3DES, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth
verify: PSK ????? Life/Active Time: 86400/190 sec ?????
Session-id: 99220 ????? Status Description: Negotiation done
????? Local spi: FD366326E1FED6FE?????? Remote spi:
A75B9B2582AAECB7 ????? Local id: 10.0.0.2 ????? Remote id:
10.0.0.1 ????? Local req mess id: 16????????????? Remote req
mess id: 13 ????? Local next mess id: 16????????????? Remote
next mess id: 13 ????? Local req queued: 16?????????????
Remote req queued: 13 ????? Local window: 1????????????????
Remote window: 1 ????? DPD configured for 10 seconds, retry 2
????? NAT-T is not detected ? Child sa: local selector?
192.168.2.99/0 - 192.168.2.99/65535 ?????????? remote selector
192.168.1.12/0 - 192.168.1.12/65535 ?????????? ESP spi in/out:
0x8717a5a/0x8564387d ? ?????????? AH spi in/out: 0x0/0x0 ?
????????? CPI in/out: 0x0/0x0 ? ?????????? Encr: AES-CBC,
keysize: 256, esp_hmac: SHA96 ?????????? ah_hmac: None, comp:
IPCOMP_NONE, mode tunnel Child sa: local selector?
192.168.2.99/0 - 192.168.2.99/65535 ?????????? remote selector
192.168.1.1/0 - 192.168.1.1/65535 ?????????? ESP spi in/out:
0xf0d97b2a/0x74756292 ? ?????????? AH spi in/out: 0x0/0x0 ?
????????? CPI in/out: 0x0/0x0 ? ?????????? Encr: AES-CBC,
keysize: 256, esp_hmac: SHA96 ?????????? ah_hmac: None, comp:
IPCOMP_NONE, mode tunnel
```

IPSec

Команда

```
show crypto ipsec sa
```

Выходные данные

ASA1

```
ASA1(config)#sh cry ipsec sa interface: outside Crypto map
tag: outside_map, seq num: 1, local addr: 10.0.0.1 access-
list l2l_list extended permit ip host 192.168.1.1 host
192.168.2.99 local ident (addr/mask/prot/port):
(192.168.1.1/255.255.255.255/0/0) remote ident
(addr/mask/prot/port): ( 192.168.2.99/255.255.255.255/0/0)
current_peer: 10.0.0.2 #pkts encaps: 3, #pkts encrypt: 3,
#pkts digest: 3 #pkts decaps: 3, #pkts decrypt: 3, #pkts
verify: 3 #pkts compressed: 0, #pkts decompressed: 0 #pkts
not compressed: 3, #pkts comp failed: 0, #pkts decomp failed:
0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs
needing reassembly: 0 #send errors: 0, #recv errors: 0 local
crypto endpt.: 10.0.0.1/500, remote crypto endpt.:
10.0.0.2/500 path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: F0D97B2A current inbound spi : 74756292
inbound esp sas: spi: 0x74756292 (1953850002) transform: esp-
aes-256 esp-sha-hmac no compression in use settings ={L2L,
Tunnel, } slot: 0, conn_id: 137990144, crypto-map:
outside_map sa timing: remaining key lifetime (kB/sec):
(4008959/28628) IV size: 16 bytes replay detection support: Y
Anti replay bitmap: 0x00000000 0x0000000F outbound esp sas:
spi: 0xF0D97B2A (4040784682) transform: esp-aes-256 esp-sha-
hmac no compression in use settings ={L2L, Tunnel, } slot: 0,
```

```

conn_id: 137990144, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (4147199/28628) IV size: 16
bytes replay detection support: Y Anti replay bitmap:
0x00000000 0x00000001 Crypto map tag: outside_map, seq num:
1, local addr: 10.0.0.1 access-list l2l_list extended permit
ip host 192.168.1.12 host 192.168.2.99 local ident
(addr/mask/prot/port): ( 192.168.1.12/255.255.255.255/0/0)
remote ident (addr/mask/prot/port):
(192.168.2.99/255.255.255.255/0/0) current_peer: 10.0.0.2
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3 #pkts
decaps: 3, #pkts decrypt: 3, #pkts verify: 3 #pkts
compressed: 0, #pkts decompressed: 0 #pkts not compressed: 3,
#pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag
successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0 #send errors: 0, #recv errors: 0 local crypto
endpt.: 10.0.0.1/500, remote crypto endpt.: 10.0.0.2/500 path
mtu 1500, ipsec overhead 74, media mtu 1500 current outbound
spi: 08717A5A current inbound spi : 8564387D inbound esp sas:
spi: 0x8564387D (2237937789) transform: esp-aes-256 esp-sha-
hmac no compression in use settings ={L2L, Tunnel, } slot: 0,
conn_id: 137990144, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (4285439/28734) IV size: 16
bytes replay detection support: Y Anti replay bitmap:
0x00000000 0x0000000F outbound esp sas: spi: 0x08717A5A
(141654618) transform: esp-aes-256 esp-sha-hmac no
compression in use settings ={L2L, Tunnel, } slot: 0,
conn_id: 137990144, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (4055039/28734) IV size: 16
bytes replay detection support: Y Anti replay bitmap:
0x00000000 0x00000001

```

ASA2

```

ASA2(config)#sh cry ipsec sa interface: outside Crypto map
tag: outside_map, seq num: 1, local addr: 10.0.0.2 access-
list l2l_list extended permit ip host 192.168.2.99 host
192.168.1.12 local ident (addr/mask/prot/port):
(192.168.2.99/255.255.255.255/0/0) remote ident
(addr/mask/prot/port): (192.168.1.12/255.255.255.255/0/0)
current_peer: 10.0.0.1 #pkts encaps: 3, #pkts encrypt: 3,
#pkts digest: 3 #pkts decaps: 3, #pkts decrypt: 3, #pkts
verify: 3 #pkts compressed: 0, #pkts decompressed: 0 #pkts
not compressed: 3, #pkts comp failed: 0, #pkts decomp failed:
0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs
needing reassembly: 0 #send errors: 0, #recv errors: 0 local
crypto endpt.: 10.0.0.2/500, remote crypto endpt.:
10.0.0.1/500 path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 8564387D current inbound spi : 08717A5A
inbound esp sas: spi: 0x08717A5A (141654618) transform: esp-
aes-256 esp-sha-hmac no compression in use settings ={L2L,
Tunnel, } slot: 0, conn_id: 137973760, crypto-map:
outside_map sa timing: remaining key lifetime (kB/sec):
(4193279/28770) IV size: 16 bytes replay detection support: Y
Anti replay bitmap: 0x00000000 0x0000000F outbound esp sas:
spi: 0x8564387D (2237937789) transform: esp-aes-256 esp-sha-
hmac no compression in use settings ={L2L, Tunnel, } slot: 0,
conn_id: 137973760, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (4055039/28770) IV size: 16
bytes replay detection support: Y Anti replay bitmap:
0x00000000 0x00000001 Crypto map tag: outside_map, seq num:
1, local addr: 10.0.0.2 access-list l2l_list extended permit

```

```

ip host 192.168.2.99 host 192.168.1.1 local ident
(addr/mask/prot/port): ( 192.168.2.99/255.255.255.255/0/0)
remote ident (addr/mask/prot/port):
(192.168.1.1/255.255.255.255/0/0) current_peer: 10.0.0.1
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3 #pkts
decaps: 3, #pkts decrypt: 3, #pkts verify: 3 #pkts
compressed: 0, #pkts decompressed: 0 #pkts not compressed: 3,
#pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag
successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0 #send errors: 0, #recv errors: 0 local crypto
endpt.: 10.0.0.2/500, remote crypto endpt.: 10.0.0.1/500 path
mtu 1500, ipsec overhead 74, media mtu 1500 current outbound
spi: 74756292 current inbound spi : F0D97B2A inbound esp sas:
spi: 0xF0D97B2A (4040784682) transform: esp-aes-256 esp-sha-
hmac no compression in use settings = {L2L, Tunnel, } slot: 0,
conn_id: 137973760, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (4285439/28663) IV size: 16
bytes replay detection support: Y Anti replay bitmap:
0x00000000 0x0000000F outbound esp sas: spi: 0x74756292
(1953850002) transform: esp-aes-256 esp-sha-hmac no
compression in use settings = {L2L, Tunnel, } slot: 0,
conn_id: 137973760, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (4331519/28663) IV size: 16
bytes replay detection support: Y Anti replay bitmap:
0x00000000 0x00000001

```

Можно также проверить выходные данные команды **show crypto ikev2 sa**. Это дает выходные данные, идентичные выходным данным команды **show crypto isakmp sa**:

IKEv2 SAs:

Session-id:99220, Status:UP-ACTIVE, IKE count:1, CHILD count:2

Tunnel-id	Local	Remote	Status	Role
1889403559	10.0.0.1/500	10.0.0.2/500	READY	RESPONDER
Encr: 3DES, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK				
Life/Active Time: 86400/179 sec				
Child sa: local selector 192.168.1.12/0 - 192.168.1.12/65535				
remote selector 192.168.2.99/0 - 192.168.2.99/65535				
ESP spi in/out: 0x8564387d/0x8717a5a				
Child sa: local selector 192.168.1.1/0 - 192.168.1.1/65535				
remote selector 192.168.2.99/0 - 192.168.2.99/65535				
ESP spi in/out: 0x74756292/0xf0d97b2a				

[Дополнительные сведения](#)

- [Cisco Systems – техническая поддержка и документация](#)