

O ASA IKEv2 debuga para o VPN de Site-para-Site com PSK

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Edição de núcleo](#)

[Debuga usado](#)

[Configurações ASA](#)

[ASA1](#)

[ASA2](#)

[Debugs](#)

[A associação de segurança da criança debuga](#)

[Verificação do túnel](#)

[ISAKMP](#)

[IPSec](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece a informação para compreender que IKEv2 debuga na ferramenta de segurança adaptável (ASA) quando a chave preshared (PSK) é usada.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

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

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Edição de núcleo

O intercâmbio de pacotes em IKEv2 é radicalmente diferente do que estava em IKEv1. Considerando que em IKEv1 havia uma troca phase1 claramente delimitada que consistisse nos pacotes 6 seguidos por uma troca da fase 2 que consistido 3 pacotes, a troca IKEv2 é variável. Para informações mais detalhadas sobre das diferenças e de uma explicação do intercâmbio de pacotes, refira a [eliminação de erros do intercâmbio de pacotes IKEv2 e do nível de protocolo](#).

Debuga usado

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

Configurações 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 l2l_list extended permit ip host 192.168.1.1
 host 192.168.2.99
access-list l2l_list extended permit ip host 192.168.1.12
 host 192.168.2.99

crypto map outside_map 1 match address l2l_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 *****

```

Debugs

(Iniciad or) descrição de mensagem em ASA1	Debugs	(Que responde) descrição de mensagem em ASA2
ASA1 recebe um pacote que combin e o acl cripto para o par	<pre> 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 IKEv2-PLAT-3: (16) tp_name set to: IKEv2-PLAT-3: (16) tg_name set to: </pre>	

ASA 10.0.0.2 . Criação novatos SA.	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	
O primeiro par de mensag ens é a troca IKE_SA _INIT. Estas mensag ens negocia m algoritm os criptogr áficos, nonces da troca, e fazem um intercâ mbio Diffie- Hellman . Configu ração relevan te: crypto ikev2 policy 1 encrypti on aes-256 integrit y sha group 2 prf sha lifetime seconds 86400 crypto ikev2 enable outside	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_REC'D_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	

<p>Tunnel Group</p> <p>matching the identity name is present:</p> <p>tunnel-group 10.0.0.2 type ipsec-121 tunnel-group 10.0.0.2 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****</p>		
<p>O início do pacote IKE_INIT_SA. Contém:</p> <p>1. Encabeça</p>	<p>R_SPI=0000000000000000 (I) MsgID = 00000000</p> <p>CurState: I_BLD_INIT Event: EV_BLD_MSG</p> <p>IKEv2-PROTO-2: (16): Sending initial message IKEv2-PROTO-3: Tx [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: 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,</p>	

m
en
to
IS
AK
M
P -
SP
l/v
er
sio
n/fl
ag
s
2. SA
i1
-
alg
ori
tm
o
cri
pt
og
ráf
ico
qu
e
o
ini
cia
do
r
IK
E
ap
oia
3. KE
i -
Va
lor
de
ch
av
e
pú
bli

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 1d **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

<p>ca D H do ini cia do r 4. No nc e do N- ini cia do r</p>		
<p>O iniciado r é enviado .</p>	<pre>IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [10.0.0.1]:500->[10.0.0.2]:500</pre>	
<p>----- IKE_INIT_SA enviado iniciador -----></p>		
	<pre>IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [10.0.0.1]:500->[10.0.0.2]:500 InitSPI=0xdfa3b583a4369958 RespSPI=0x0000000000000000 MID=00000000</pre>	<p>O que respon de recebe IKEV_I NIT_SA .</p>
	<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,</pre>	<p>O que respon de inicia a criação SA para esse par.</p>

	<pre> 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>	
	<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 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: </pre>	<p>O que responde e verifica e processa a mensagem em IKE_INIT:</p> <ol style="list-style-type: none"> Escolhe a série cripto da qual as ofertas iniciadas pelo inicio

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_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
 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

r.
 2. Co
 m
 pu
 ta
 su
 a
 pr
 óp
 ria
 ch
 av
 e
 se
 cr
 et
 a
 D
 H.
 3. lg
 ua
 lm
 en
 te
 co
 m
 pu
 ta
 u
 m
 val
 or
 do
 sk
 eyi
 d,
 de
 qu
 e
 to
 da
 s
 as
 ch
 av
 es
 po

		de m se r de riv ad as pa ra es te IK E_ S A. To do s m as os en ca be ça m en to s de to da s as m en sa ge ns qu e se gu e m sã
--	--	---

		o cif ra do s e au te nti ca do s. As ch av es us ad as pa ra a pr ot eç ão da cri pt og raf ia e da int eg rid ad e sã o de riv ad as de S
--	--	---

		K E YI D e sa bi da s co m o: a. S K_ e (cr ipt og raf ia) . b. S K_ a (a ut en tic aç ão). c. S K_ d é de riv ad o e us ad o pa
--	--	--

ra
a
de
riv
aç
ão
de
u
m
m
at
eri
al
de
aj
us
te
m
ais
ad
ici
on
al
pa
ra
C
HI
LD
_S
As
. U
m
S
K_
e
e
u
m
S
K_
a
se
pa
ra
do
s

sã
o
co
m
pu
ta
do
s
pa
ra
ca
da
se
nti
do

**Configu
ração
relevan
te:**

```
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
```

		<pre> ipsec- l2l tunnel- group 10.0.0.1 ipsec- attribut es ikev2 remote- authenti cation pre- shared- key ***** ikev2 local- authenti cation pre- shared- key ***** </pre>
	<pre> 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 </pre>	<pre> ASA2 constrói a mensagem do que responde para a troca IKE_SA _INIT, que é recebido por ASA1. Este pacote contém: 1. Encabeçamen- to ISAK </pre>

M
P
(v
er
sã
o/
ba
nd
eir
as
S
PI/
)

2. Al
go
rit
m
o
S
Ar
1(
cr
yp
to
gr
ap
hic
qu
e
o
qu
e
re
sp
on
de
IK
E
es
col
he
)

3. K
Er
(v
al
or

de
ch
av
e
pú
bli
ca
D
H
do
qu
e
re
sp
on
de
)
4. No
nc
e
do
qu
e
re
sp
on
de

```
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
manda
a
mensag
em do
que
respon
de a
ASA1.

<----- IKE_INIT_SA enviado que responde ----->

ASA1
recebe
o
pacote
de
respost
a
IKE_SA
_INIT
de
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
```

O que
respon
de
começa
o
tempori
zador
para o
process
o do
AUTH.

		<pre> 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 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 verifica e process a a resposta: 1. A</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 </pre>	

ch
av
e
se
cr
et
a
do
ini
cia
do
r
D
H
é
co
m
pu
ta
da
2. O
sk
eyi
d
do
ini
cia
do
ré
ge
ra
do
igu
al
m
en
te

```
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

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:
```

	<pre> 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 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>A troca IKE_INIT_SA entre os ASA está agora completa.</p>	<pre> IKEv2-PROTO-3: (16): Complete SA init exchange </pre>	
<p>O início começa a troca "IKE_AUTH" e começa a geração do payload da</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 </pre>	

autentic
ação. O
pacote
IKE_AU
TH
contém:

1. En
ca
be
ça
m
en
to
IS
AK
M
P
(v
er
sã
o/
ba
nd
eir
as
SP
I/).
2. Idi
(a
ide
nti
da
de
do
ini
cia
do
r).
3. Pa
ylo
ad
do
A
UT
H.
4. SA
i2
(ini

```
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:
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-
```

cia
o
SA
-
si
mil
ar
à
fas
e
2
tra
nsf
or
m
a
m
a
tro
ca
do
gr
up
O
e
m
IK
Ev
1).
5. TS
ie
TS
r
(s
ele
tor
es
do
trá
fe
go
do
ini
cia
do
re
do

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

qu
e
re
sp
on
de
)
):
Co
nt
ê
m
o
en
de
re
ço
de
re
m
en
te
nt
e
e
de
sti
na
tár
io
do
ini
cia
do
re
o
qu
e
re
sp
on
de
re
sp
ect
iva
m
en

te
a
en
via
r/r
ec
eb
e
o
trá
fe
go
cri
pt
og
raf
ad
o.
A
es
cal
a
de
en
de
re
ço
es
pe
cifi
ca
qu
e
to
do
o
trá
fe
go
a
e
de
ss
a
es
cal
a

est
ar
á
es
ca
va
do
u
m
tú
nel
. Se
a
pr
op
ost
a
é
ac
eit
áv
el
ao
qu
e
re
sp
on
de
, en
via
ca
rg
as
út
eis
idê
nti
ca
s
TS
pa
ra
trá
s.

<p>O \emptyset CHILD_SA é criado para o par do proxy_IID que combina o pacote do disparador. Configuração relevante:</p> <pre>crypto ipsec ikev2 ipsec- proposal AES256 protocol esp encrypti on aes- 256 protocol esp integrit y sha-1 md5 access- list l2l_list extended permit ip host 10.0.0.2 host 10.0.0.1</pre>		
<p>ASA1 manda o pacote</p>	<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>	

IKE_AUTH a ASA2.		
----- IKE_AUTH enviado iniciador ----->		
	<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 recebe este pacote de 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, 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:</pre>	ASA2 para o temporizador do AUTH e verifica os dados de autenticação recebidos de ASA1. Então, gerencia seus próprios dados de autenticação, exatamente como ASA1 fez. Configuração relevante: crypto ipsec ikev2 ipsec-proposal AES256 protocol esp

```

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 =
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 =

```

```

encrypti
on
aes-
256
protocol
esp
integrit
y
sha-1
md5

```

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
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

```

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
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

```

O pacote IKE_AUTH enviado de ASA2 contém:

1. Encabeçamento ISAKMP (versão/bandeiras SPI).
2. IDr (identidade do que responde).
3. Pa

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:
 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

ylo
 ad
 do
 A
 U
 T
 H.
 4. S
 Ar
 2
 (in
 ici
 a
 o
 S
 A-
 si
 mil
 ar
 à
 fa
 se
 2
 tra
 ns
 for
 m
 a
 m
 a
 tro
 ca
 do
 gr
 up
 o
 e
 m
 IK
 Ev
 1).
 5. TS
 ie
 TS
 r
 (s
 el

et
or
es
do
trá
fe
go
do
ini
cia
do
re
do
qu
e
re
sp
on
de
):
Co
nt
ê
m
o
en
de
re
ço
de
re
m
en
te
nt
e
e
de
sti
na
tár
io
do
ini
cia
do
re

o
qu
e
re
sp
on
de
re
sp
ec
tiv
a
m
en
te
a
en
via
r/r
ec
eb
e
o
trá
fe
go
cri
pt
og
raf
ad
o.
A
es
cal
a
de
en
de
re
ço
es
pe
cifi
ca
qu
e

to
do
o
trá
fe
go
a
e
de
ss
a
es
cal
a
es
tar
á
es
ca
va
do
u
m
tú
ne
l.
Es
te
s
pa
râ
m
etr
os
sã
o
id
ên
tic
os
a
es
se
qu
e
foi
re

			ce bi do de A S A1
	<pre>IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.2]:500->[10.0.0.1]:500 InitSPI=0xdfa3b583a4369958 RespSPI=0x27c943c13fd94665 MID=00000001</pre>		O que responde e envia a resposta para IKE_AUTH.
<p><----- Que responde enviado -----></p> <p>-----</p>			
O iniciado r recebe uma resposta do que responde.	<pre>IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [10.0.0.2]:500-> [10.0.0.1]:500 InitSPI=0xdfa3b583a4369958 RespSPI=0x27c943c13fd94665 MID=00000001</pre>	<pre>IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958 R_SPI=27C943C13FD94665 (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=DFA3B583A4369958 R_SPI=27C943C13FD94665 (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=DFA3B583A4369958</pre>	O que responde e introduz uma entrada no TRISTE.

		R_SPI=27C943C13FD94 665 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_INSERT_IKE IKEv2-PROTO-2: (16): SA created; inserting SA into database	
ASA1 verifica e processa os dados de autentic ação neste pacote. ASA1 introduz então este SA no seu TRISTE		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: 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:
```

	<pre> 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 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>O túnel está acima no iniciado r.</p>	<p>CONNECTION STATUS: UP... peer: 10.0.0.2:500, phase1_id: 10.0.0.2 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958</p>	<p>CONNECTION STATUS: UP... peer: 10.0.0.1:500, phase1_id: 10.0.0.1 IKEv2-PROTO-5: (16): SM Trace-> SA: I_SPI=DFA3B583A4369958</p>	<p>O túnel está acima no que responde. O túnel do que</p>

	R_SPI=27C943C13FD94 665 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_REGISTER_SESSION	R_SPI=27C943C13FD94 665 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_REGISTER_SESSION	responde e vem geralmente acima antes do iniciado r.
Process o de registro IKEv2.	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: (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) 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: (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	Process o de registro IKEv2.

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

[A associação de segurança da criança debuga](#)

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

Descrição de mensagem em ASA1 CHILD_SA	Debugs	Descrição de mensagem em 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: </pre>	<pre> ASA2 inicia a troca CHILD_ SA. Este é o pedido CREAT E_CHIL D_SA. O pacote CHILD_ SA </pre>


```

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):
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,

```

contém tipicamente:

1. SAHDR (versão.n.f.lags/tipodatorca)
2. Nidone (opcional): Se o CHILD_SA é criadocomo parte do

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

ca
ini
cia
l,
u
m
se
gu
nd
o
pa
ylo
ad
e
o
no
nc
e
K
E
N
Ñ
O
D
E
V
E
M
se
r
en
via
do
s.
3. Pa
ylo
ad
S
A
4. K
Ei
(C
ha
ve
-
op
cio

na
l):
O
pe
di
do
C
R
E
A
T
E_
C
H
I
L
D
_S
A
P
Ô
D
E
op
cio
na
lm
en
te
co
nt
er
u
m
pa
ylo
ad
K
E
pa
ra
qu
e
u
m
a
tro
ca
ad
ici

on
al
D
H
pe
rm
ita
u
m
as
ga
ra
nti
as
m
ais
for
te
s
do
se
cr
eti
s
m
o
di
an
tei
ro
pa
ra
o
C
HI
LD
_S
A.
?
Se
as
of
ert
as
S
A
inc

		lu e m gr up os dif er en te s D H, K Ei D E V E se r u m el e m en to do gr up o qu e o ini cia do r es pe ra o qu e re sp
--	--	---

on
de
ac
eit
ar.
?
Se
su
põ
e
err
ad
a
m
en
te,
a
tro
ca
C
R
E
AT
E_
C
HI
LD
_S
A
fal
ha
rá,
e
ter
á
qu
e
ex
pe
ri
m
en
tar
de
no
vo
co

m
u
m
K
Ei
dif
er
en
te.

5. **N**
(n
oti
fiq
ue
pa
ylo
ad
-
op
cio
na
l):
O
pa
ylo
ad
da
no
tifi
ca
çã
o,
é
us
ad
o
pa
ra
tra
ns
mi
tir
da
do
s
inf
or

		m a t i v o s, t a i s c o m o c o n d i ç õ e s d e e r r o e t r a n s i ç õ e s d e e s t a d o , a u m p a r I K E. U m p a y l o a d a n o t i f i c a ç ã o p ô d e a p a r
--	--	--

		ec er e m u m m en sa ge m de re sp os ta (q ue es pe cifi ca ge ral m en te po rq ue u m pe di do foi rej eit ad o), e m u m a tro ca
--	--	--

IN
F
O
R
M
A
T
I
V
A
(p
a
r
a
r
e
l
a
t
a
r
u
m
e
r
r
o
n
e
e
m
u
m
p
e
d
i
d
o
I
K
E),
o
u
e
m
t
o
d
a
a
o
u
t
r
a
m
e
n
s
a
g
e
m
p
a
r
a
i
n
d
i
c
a
r

ca
pa
cid
ad
es
do
re
m
et
en
te
ou
pa
ra
alt
er
ar
o
sig
nifi
ca
do
do
pe
di
do
. Se
es
ta
tro
ca
C
R
E
AT
E_
C
HI
LD
_S
A
re
ke
yin
g
u

m
S
A
exi
st
en
te
a
nã
o
se
r
o
IK
E_
S
A,
o
pa
ylo
ad
pri
nci
pa
IN
do
tip
o
R
E
K
E
Y_
S
A
D
E
V
E
id
en
tifi
ca
r
o
S
A
qu
e

re
ke
ye
d.
?
Se
es
ta
tro
ca
C
R
E
AT
E_
C
HI
LD
_S
A
nã
o
re
ke
yin
g
u
m
S
A
exi
st
en
te,
o
pa
ylo
ad
N
D
E
V
E
se
r
o
mi

		tid o. 6. TS ie TS r(o pti on al) : lst o m os tra os sel et or es do trá fe go pa ra qu e o S A foi cri ad o. Ne st e ca so , es tá en tre an fitr
--	--	---

		<p>iõ es 19 2. 16 8. 1. 12 e 19 2. 16 8. 2. 99 .</p>	
<p>ASA1 recebe este pacote.</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 10.0.0.2:500/VRF i0:f0] m_id: 0x6</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 Trace-> SA: I_SPI=FD366326E1FED 6FE R_SPI=A75B9B2582AAE CB7 (I) MsgID = 00000006 CurState: CHILD_I_WAIT Event: EV_NO_EVENT</p>	<p>ASA2 envia este pacote para fora e espera a respost a.</p>
<p>ASA1 recebe este pacote exato de ASA2 e verifica- o.</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: 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:</p>		

	<pre> 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 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 constrói agora a respost a para a troca</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 </pre>	

<p>CHILD_SA. Esta é a resposta a CREATED_SA. O pacote CHILD_SA contém tipicamente: 1. SA H D R (v er sio n.fl ag s/ti po da tro ca) 2. Ni do no nc e (o pci on al) : Se o C HI LD _S A é cri</p>	<p>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_REC'D_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 = 00000006 CurState: CHILD_R_IPSEC Event: EV_OK IKEv2-PROTO-3: (225): Requesting SPI from IPsec IKEv2-PROTO-5: (225): SM Trace-> SA:I_SPI=FD366326E1FED6FE R_SPI=A75B9B2582AAECB7 (R) MsgID = 00000006 CurState: CHILD_R_WAIT_SPI Event: EV_OK_GOT_SPI 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_BLD_MSG 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 (R) MsgID = 00000006 CurState: CHILD_R_BLD_MSG 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: 3 AES-CBC?SHA96? IKEv2-PROTO-3: (225): Building packet for encryption; contents are: 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,</p>	
--	---	--

ad
o
c
o
m
o
p
a
r
t
e
d
a
t
r
o
c
a
i
n
i
c
i
a
l
,
u
m
s
e
g
u
n
d
o
p
a
y
l
o
a
d
e
o
n
c
e
K
E
N
Ñ
O
D
E
V
E
M
s
e
r
e
n
v
i
a
d
o
s.
3. Pa
y
l
o
a
d
S
A
4. KE
i

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,
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: Tx [L
10.0.0.1:500/R 10.0.0.2:500/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:
RESPONDER MSG-RESPONSE** IKEv2-PROTO-4:
Message id: 0x6, length: 172 ENCR?Next
payload: SA, reserved: 0x0, length: 144
Encrypted data: 140 bytes

(C
ha
ve
-
op
cio
nal
):
O
pe
did
o
C
R
EA
TE
_C
HI
LD
_S
A
P
O
D
E
op
cio
nal
m
en
te
co
nt
er
u
m
pa
ylo
ad
KE
pa
ra
qu
e
u
m
a

tro
ca
adi
cio
nal
D
H
pe
rm
ita
u
m
as
ga
ra
nti
as
m
ais
for
tes
do
se
cr
eti
sm
o
dia
nt
eir
o
pa
ra
o
C
HI
LD
_S
A.
?
Se
as
of
ert
as
SA
inc

lue
m
gr
up
os
dif
er
en
tes
D
H,
KE
i
D
EV
E
se
r
u
m
ele
m
en
to
do
gr
up
o
qu
e
o
ini
cia
do
r
es
pe
ra
o
qu
e
re
sp
on
de
ac
eit

ar.
?
Se
su
põ
e
err
ad
a
m
en
te,
a
tro
ca
C
R
EA
TE
_C
HI
LD
_S
A
fal
ha
, e
ter
á
qu
e
ex
pe
ri
m
en
tar
de
no
vo
co
m
u
m
KE
i
dif

er
en
te.

5. **N**
(n
otif
iqu
e
pa
ylo
ad
-
op
cio
nal
):
O
pa
ylo
ad
da
no
tifi
ca
çã
o
é
us
ad
o
pa
ra
tra
ns
mit
ir
da
do
s
inf
or
m
ati
vo
s,
tai
s

co
m
o
o
err
o?
co
ndi
çõ
es
e
tra
nsi
çõ
es
de
est
ad
o,
a
u
m
pa
r
IK
E.
?
U
m
pa
ylo
ad
da
no
tifi
ca
çã
o
pô
de
ap
ar
ec
er
e
m
u

m
m
en
sa
ge
m
de
re
sp
ost
a
(e
sp
eci
fic
a
ge
ral
m
en
te
po
rq
ue
u
m
pe
did
o
foi
rej
eit
ad
o),
e
m
u
m
a
tro
ca
IN
F
O
R
M
AT

IV
A
(p
ar
a
rel
at
ar
u
m
err
o
nã
o
e
m
u
m
pe
did
o
IK
E),
ou
e
m
to
da
a
ou
tra
m
en
sa
ge
m
pa
ra
ind
ica
r
ca
pa
cid
ad
es
do

re
m
et
en
te
ou
pa
ra
ra
alt
er
ar
o
sig
nifi
ca
do
do
pe
did
o.
Se
est
a
tro
ca
C
R
EA
TE
_C
HI
LD
_S
A
re
ke
yin
g
u
m
SA
exi
ste
nt
e
a
nã

o
se
r o
IK
E_
SA
, o
pa
ylo
ad
pri
nci
pal
N
do
tip
o
R
EK
EY
_S
A
D
EV
E
ide
ntif
ica
r o
SA
qu
e
re
ke
ye
d.
?
Se
est
a
tro
ca
C
R
EA
TE
_C

HI
LD
_S
A
nã
o
re
ke
yin
g
u
m
SA
exi
ste
nt
e,
o
pa
ylo
ad
N
D
EV
E
se
r
o
mit
ido

6. TS
ie
TS
r
(o
pci
on
ais
):
lst
o
m
ost
ra
os
sel

<p>et or es do trá fe go pa ra qu e o SA foi cri ad o. Ne ste ca so, est á en tre an fitri õe s 19 2. 16 8. 1. 12 e 19 2. 16 8. 2. 99 .</p>		
---	--	--

<p>ASA1 envia a respost a para</p>	<p>IKEv2-PLAT-4: SENT PKT [CREATE_CHILD_SA] [10.0.0.1]:500-> [10.0.0.2]:500 InitSPI=0xfd366326e</p>	<p>IKEv2-PLAT-4: RCV PKT [CREATE_CHILD_SA] [10.0.0.1]:500-> [10.0.0.2]:500</p>	<p>ASA2 recebe este pacote.</p>
--	---	--	---

<p>fora.</p>	<p>1fed6fe RespSPI=0xa75b9b258 2aaecb7 MID=00000006</p>	<p>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>	
	<pre> 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, 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 </pre>		<p>ASA2 verifica agora o pacote</p>

	<pre> 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>		
<p>ASA1 introduz esta entrada criança SA no base de dados da associa ção de seguran ça.</p>	<pre> IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED 6FE R_SPI=A75B9B2582AAE 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> IKEv2-PROTO-5: (225): SM Trace-> SA: I_SPI=FD366326E1FED 6FE R_SPI=A75B9B2582AAE CB7 (I) MsgID = 00000006 CurState: CHILD_I_DONE Event: EV_OK IKEv2-PROTO- 2: (225): SA created; inserting SA into database </pre>	<p>ASA2 introduz esta entrada criança SA no base de dados da associa ção de seguran ça.</p>

[Verificação do túnel](#)

[ISAKMP](#)

Comando

show crypto isakmp sa det

Saída

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
```

Comando

```
show crypto ipsec sa
```

Saída

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 121_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 121_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 121_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 121_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
```

Você pode igualmente verificar a saída do comando `crypto ikev2 sa da mostra`. Isto dá uma saída idêntica à saída do comando `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				

[Informações Relacionadas](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)