strongSwan - Issue #1553

Keeping create child SA with Cisco IOS

05.07.2016 20:33 - Kris Jobs

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	dr|rc|master	**Resolution:**	No feedback

Description

The IOS router using SVTI connect to strongswan server, conf like:

```
conn ikev2
    type=tunnel
    left=%defaultroute
    keyexchange=ikev2
    ike=aes256-sha1-modp1024,aes256-sha1-modp2048
    esp=aes256-sha1,aes128-sha1
    leftsubnet=0.0.0.0/0
    leftauth=pubkey
    leftcert=crt.pem
    leftsendcert=always
    leftid=@test.local
    right=%any
    rightsourceip=192.168.92.0/24
    rightauth=eap-mschapv2
    rightsendcert=never
    eap_identity=%any
    rekey=no
    reauth=no
    ikelifetime=1440m
    lifetime=1440m
    keylife=60m
    rekeymargin=3m
    keyingtries=1
    forceencaps = yes
    auto=add
```

It almost works, but every 60s, IOS create child SA req, strongswan log like:

```
07[NET] received packet: from a.b.c.154[4500] to x.y.z.126[4500] (204 bytes)
07[ENC] parsed CREATE_CHILD_SA request 6 [ SA No TSi TSr ]
07[IKE] CHILD_SA ikev2{2} established with SPIs cf62d19a_i 5a0b77ed_o and TS 0.0.0.0/0 === 192.168
.92.1/32
07[ENC] generating CREATE_CHILD_SA response 6 [ SA No TSi TSr ]
07[NET] sending packet: from x.y.z.126[4500] to a.b.c.154[4500] (204 bytes)
```

IOS debug log:

```
*Jul  6 01:46:46.248: [] -> [ACL automatic]: message ACL for always up maps
*Jul  6 01:46:46.248: [ACL automatic]: message = ACL for always up maps
*Jul  6 01:46:46.248: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= a.b.c.154:500, remote= x.y.z.126:500,
    local_proxy= 0.0.0.0/0.0.0.0/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0,
    protocol= ESP, transform= esp-aes esp-sha-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Jul  6 01:46:46.248: [ACL automatic] -> [ACL automatic]: delayed (60000 msec) message ACL for alw
ays up maps
*Jul  6 01:46:46.249: IKEv2:Searching Policy with fvrf 0, local address a.b.c.154
*Jul  6 01:46:46.249: IKEv2:Found Policy 'po1'
```

```
*Jul  6 01:46:46.249: IKEv2:(SESSION ID = 1,SA ID = 1):Check for IPSEC rekey
*Jul  6 01:46:46.249: IKEv2:(SESSION ID = 1,SA ID = 1):Set IPSEC DH group
*Jul  6 01:46:46.250: IKEv2:(SESSION ID = 1,SA ID = 1):Checking for PFS configuration
*Jul  6 01:46:46.250: IKEv2:(SESSION ID = 1,SA ID = 1):PFS not configured
*Jul  6 01:46:46.250: IKEv2:(SESSION ID = 1,SA ID = 1):Generating CREATE_CHILD_SA exchange
*Jul  6 01:46:46.250: IKEv2:(SESSION ID = 1,SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec negotia
tion),
Num. transforms: 3
   AES-CBC   SHA96   Don't use ESN
*Jul  6 01:46:46.250: IKEv2:(SESSION ID = 1,SA ID = 1):Building packet for encryption.
Payload contents:
 SA  Next payload: N, reserved: 0x0, length: 44
  last proposal: 0x0, reserved: 0x0, length: 40
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3    last transform: 0x3, reserved: 0x0: len
gth: 12
    type: 1, reserved: 0x0, id: AES-CBC
    last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA96
    last transform: 0x0, reserved: 0x0: length: 8
    type: 5, reserved: 0x0, id: Don't use ESN
 N  Next payload: TSi, reserved: 0x0, length: 36
 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: 0.0.0.0, end addr: 255.255.255.255
 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: 0.0.0.0, end addr: 255.255.255.255

*Jul  6 01:46:46.252: IKEv2:(SESSION ID = 1,SA ID = 1):Checking if request will fit in peer window


*Jul  6 01:46:46.253: IKEv2:(SESSION ID = 1,SA ID = 1):Sending Packet [To x.y.z.126:4500/From a.b.
c.154:4500/VRF i0:f0]
Initiator SPI : 1F80C3B5B995479A - Responder SPI : C3E3600EF2594AD2 Message id: 6
IKEv2 CREATE_CHILD_SA Exchange REQUEST
*Jul  6 01:46:46.253: IKEv2-PAK:(SESSION ID = 1,SA ID = 1):Next payload: ENCR, version: 2.0 Exchan
ge type: CREATE_CHILD_SA, flags: INITIATOR Message id: 6, length: 204
Payload contents:
 ENCR  Next payload: SA, reserved: 0x0, length: 176

*Jul  6 01:46:46.471: IKEv2:(SESSION ID = 1,SA ID = 1):Received Packet [From x.y.z.126:4500/To a.b
.c.154:4500/VRF i0:f0]
Initiator SPI : 1F80C3B5B995479A - Responder SPI : C3E3600EF2594AD2 Message id: 6
IKEv2 CREATE_CHILD_SA Exchange RESPONSE
*Jul  6 01:46:46.471: IKEv2-PAK:(SESSION ID = 1,SA ID = 1):Next payload: ENCR, version: 2.0 Exchan
ge type: CREATE_CHILD_SA, flags: RESPONDER MSG-RESPONSE Message id: 6, length: 204
Payload contents:
 SA  Next payload: N, reserved: 0x0, length: 44
  last proposal: 0x0, reserved: 0x0, length: 40
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3    last transform: 0x3, reserved: 0x0: len
gth: 12
    type: 1, reserved: 0x0, id: AES-CBC
    last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA96
    last transform: 0x0, reserved: 0x0: length: 8
    type: 5, reserved: 0x0, id: Don't use ESN
 N  Next payload: TSi, reserved: 0x0, length: 36
 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: 192.168.92.1, end addr: 192.168.92.1
 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: 0.0.0.0, end addr: 255.255.255.255

*Jul  6 01:46:46.473: IKEv2:(SESSION ID = 1,SA ID = 1):Processing any notify-messages in child SA
exchange
*Jul  6 01:46:46.473: IKEv2:(SESSION ID = 1,SA ID = 1):Validating create child message
*Jul  6 01:46:46.474: IKEv2:(SESSION ID = 1,SA ID = 1):Processing CREATE_CHILD_SA exchange
*Jul  6 01:46:46.474: IKEv2:IPSec policy validate request sent for profile 126 with psh index 1.

*Jul  6 01:46:46.474: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Jul  6 01:46:46.474: IPSEC(ipsec_get_crypto_session_id):
Invalid Payload Id
*Jul  6 01:46:46.474: IPSEC(validate_proposal_request): proposal part #1
*Jul  6 01:46:46.474: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= a.b.c.154:0, remote= x.y.z.126:0,
    local_proxy= 192.168.92.1/255.255.255.255/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0,
    protocol= ESP, transform= esp-aes esp-sha-hmac  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Jul  6 01:46:46.475: Crypto mapdb : proxy_match
    src addr     : 192.168.92.1
    dst addr     : 0.0.0.0
    protocol     : 0
    src port     : 0
    dst port     : 0
*Jul  6 01:46:46.475: (ipsec_process_proposal)Map Accepted: Tunnel0-head-0, 65537
*Jul  6 01:46:46.475: IKEv2:(SA ID = 1):[IPsec -> IKEv2] Callback received for the validate propos
al - PASSED.

*Jul  6 01:46:46.475: IKEv2:(SESSION ID = 1,SA ID = 1):Checking for PFS configuration
*Jul  6 01:46:46.475: IKEv2:(SESSION ID = 1,SA ID = 1):PFS not configured
*Jul  6 01:46:46.476: IKEv2:(SESSION ID = 1,SA ID = 1):Checking if IKE SA rekey
*Jul  6 01:46:46.476: IKEv2:(SESSION ID = 1,SA ID = 1):Load IPSEC key material
*Jul  6 01:46:46.476: IKEv2:(SA ID = 1):[IKEv2 -> IPsec] Create IPsec SA into IPsec database
*Jul  6 01:46:46.476: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Jul  6 01:46:46.476: IPSEC(ipsec_get_crypto_session_id):
Invalid Payload Id
*Jul  6 01:46:46.477: Crypto mapdb : proxy_match
    src addr     : 192.168.92.1
    dst addr     : 0.0.0.0
    protocol     : 256
    src port     : 0
    dst port     : 0
*Jul  6 01:46:46.477: IPSEC:(SESSION ID = 1) (crypto_ipsec_create_ipsec_sas) Map found Tunnel0-hea
d-0, 65537
*Jul  6 01:46:46.477: [] -> [SADB Tunnel0-head-0:a.b.c]: message SADB root KMI message processing
*Jul  6 01:46:46.477: [SADB Tunnel0-head-0:a.b.c]: message = SADB root KMI message processing
*Jul  6 01:46:46.477: IPSEC:(SESSION ID = 1) (STATES) SADB_ROOT_SM (sadb_root_process_kmi_message)
 called static seqno 65537 dynamic seqno 0
*Jul  6 01:46:46.477: [SADB Tunnel0-head-0:a.b.c] -> [ACL automatic]: message ACL KMI create SA
*Jul  6 01:46:46.477: [ACL automatic]: message = ACL KMI create SA
*Jul  6 01:46:46.477: [ACL automatic]: state = ACL KMI create SA for PtoP
*Jul  6 01:46:46.477: [KMI Forward]: state = KMI Initializing
*Jul  6 01:46:46.477: [ACL automatic] -> [KMI Forward]: message Forward KMI message
*Jul  6 01:46:46.478: [KMI Forward]: message = Forward KMI message
*Jul  6 01:46:46.478: [KMI Forward] -> [Ident 8000001D]: message Ping
*Jul  6 01:46:46.478: [Ident 8000001D]: message = Ping
*Jul  6 01:46:46.478: [KMI Forward]: state = change priority
*Jul  6 01:46:46.478: [KMI Forward]: state = forward
*Jul  6 01:46:46.478: [KMI Forward] -> [Ident 8000001D]: message Message - Create SA
*Jul  6 01:46:46.478: [Ident 8000001D]: message = Message - Create SA
*Jul  6 01:46:46.478: [Ident 8000001D]: state = Check redundant request
*Jul  6 01:46:46.478: [Ident 8000001D]: state = Allocate Session
*Jul  6 01:46:46.478: [Ident 8000001D]: state = Insert Peer
```

```
*Jul  6 01:46:46.478: [Ident 8000001D] -> [Session]: message Session Inserting Peer
*Jul  6 01:46:46.478: [Session]: message = Session Inserting Peer
*Jul  6 01:46:46.479: [Ident 8000001D]: state = Allocate Sibling
*Jul  6 01:46:46.479: [Sibling]: state = Sibling Initialization
*Jul  6 01:46:46.479: [Ident 8000001D]: state = Create In/Outbound SAs
*Jul  6 01:46:46.479: [Ident 8000001D]: state = Ident Set Replay
*Jul  6 01:46:46.479: [Ident 8000001D]: state = Send SAs to sibling and install them
*Jul  6 01:46:46.479: [Ident 8000001D] -> [Sibling]: message Message - Create Inbound SA
*Jul  6 01:46:46.480: [Sibling]: message = Message - Create Inbound SA
*Jul  6 01:46:46.480: [Sibling]: state = Hook Session
*Jul  6 01:46:46.480: [Sibling] -> [Session]: message Message - In Use
*Jul  6 01:46:46.480: [Session]: message = Message - In Use
*Jul  6 01:46:46.480: [Session]: state = Add Sibling to Session List
*Jul  6 01:46:46.480: [Sibling]: state = Fill Sibling with CE data
*Jul  6 01:46:46.480: [Sibling 5A0B77ED]: state = Hook SA Struct to Sibling
*Jul  6 01:46:46.480: IPSEC:(SESSION ID = 1) (create_sa) sa created,
  (sa) sa_dest= a.b.c.154, sa_proto= 50,
    sa_spi= 0x5A0B77ED(1510701037),
    sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 5478
    sa_lifetime(k/sec)= (4608000/3600),
  (identity) local= a.b.c.154:0, remote= x.y.z.126:0,
    local_proxy= 192.168.92.1/255.255.255.255/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0
*Jul  6 01:46:46.481: IPSEC:(SESSION ID = 1) (create_sa) sa created,
  (sa) sa_dest= x.y.z.126, sa_proto= 50,
    sa_spi= 0xCF62D19A(3479359898),
    sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 5477
    sa_lifetime(k/sec)= (4608000/3600),
  (identity) local= a.b.c.154:0, remote= x.y.z.126:0,
    local_proxy= 192.168.92.1/255.255.255.255/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0
*Jul  6 01:46:46.481: [Sibling 5A0B77ED]: state = Install SPI
*Jul  6 01:46:46.483: IPSEC(MESSAGE): SADB_ROOT_SM (print_message_to_acl_state_machine) Sent MSG_A
CL_CREATE_PTOP_SA message to ACL, static seqno 65537, dynamic seqno 0
*Jul  6 01:46:46.497: [Sibling 5A0B77ED]: state = Del Transient SPI
*Jul  6 01:46:46.497: [Ident 8000001D]: state = Check Outbound Enable Status
*Jul  6 01:46:46.497: [Ident 8000001D]: state = Got Enable Outbound SA
*Jul  6 01:46:46.497: [Ident 8000001D]: state = Select Outbound SA
*Jul  6 01:46:46.497: [Ident 8000001D]: state = Install Existing Outbound SA
*Jul  6 01:46:46.497: IPSEC:(SESSION ID = 1) (update_current_outbound_sa) updated peer x.y.z.126 c
urrent outbound sa to SPI CF62D19A
*Jul  6 01:46:46.598: [Ident 8000001D]: state = Set flow_installed
*Jul  6 01:46:46.598: IPSEC:(SESSION ID = 1) (STATES) ident_set_flow_installed_action Sending cryp
to_ss_connection_open

*Jul  6 01:46:46.598: [Ident 8000001D]: state = Check Install SA Declare Success
*Jul  6 01:46:46.598: [Ident 8000001D]: state = Declare success
*Jul  6 01:46:46.598: [KMI Forward]: state = success
*Jul  6 01:46:46.598: [KMI Forward]: deleting state machine
*Jul  6 01:46:46.598: [ACL automatic]: state = ACL KMI check result
*Jul  6 01:46:46.598: IKEv2:(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec SA into IPsec database
PASSED
*Jul  6 01:46:46.599: IKEv2:(SESSION ID = 1,SA ID = 1):IKEV2 SA created; inserting SA into databas
e. SA lifetime timer (86400 sec) started
```

Maybe this the bug from strongswan side? Thanks for any info.

History

#1 - 06.07.2016 09:48 - Tobias Brunner

- Status changed from New to Feedback

> Maybe this the bug from strongswan side?

Um, why would you think that if it is the Cisco box that does something strange?

> It almost works, but every 60s, IOS create child SA req

Maybe ask Cisco what their box is doing exactly?

#2 - 18.07.2016 16:43 - Kris Jobs

Tobias Brunner wrote:

> > Maybe this the bug from strongswan side?
>
> Um, why would you think that if it is the Cisco box that does something strange?
>
> > It almost works, but every 60s, IOS create child SA req
>
> Maybe ask Cisco what their box is doing exactly?

Hello, Tobias. Maybe this is the problem? http://reinoutpennings.blogspot.com/2016/03/barracuda-cisco-strongswan-ikev2-bug.html

#3 - 19.07.2016 10:19 - Tobias Brunner

> > Maybe ask Cisco what their box is doing exactly?
>
> Hello, Tobias. Maybe this is the problem? http://reinoutpennings.blogspot.com/2016/03/barracuda-cisco-strongswan-ikev2-bug.html

No idea, although it's quite unclear what bug he actually describes (or how it manifests itself).

#4 - 19.07.2016 10:44 - Kris Jobs

Tobias Brunner wrote:

> > > Maybe ask Cisco what their box is doing exactly?
> >
> > Hello, Tobias. Maybe this is the problem? http://reinoutpennings.blogspot.com/2016/03/barracuda-cisco-strongswan-ikev2-bug.html
>
> No idea, although it's quite unclear what bug he actually describes (or how it manifests itself).

It looks very like SPI's problem, "Cisco expects a new SPI for each SA. The current implementation on a barracuda(Strongswan) uses the same SPI which results in a communication mismatch which can't be resolved with multiple ACL's."

#5 - 19.07.2016 10:56 - Tobias Brunner

> "Cisco expects a new SPI for each SA. The current implementation on a barracuda(Strongswan) uses the same SPI which results in a communication mismatch which can't be resolved with multiple ACL's."

That does not describe what the bug actually is: What SPIs, what SAs, when does this happen exactly, what is the effect.

#6 - 19.07.2016 11:06 - Kris Jobs

Tobias Brunner wrote:

> > "Cisco expects a new SPI for each SA. The current implementation on a barracuda(Strongswan) uses the same SPI which results in a communication mismatch which can't be resolved with multiple ACL's."
>
> That does not describe what the bug actually is: What SPIs, what SAs, when does this happen exactly, what is the effect.

Is not this one? "source of the bug / misinterpretation: https://tools.ietf.org/html/rfc5996#page-30"

Sorry, I am not so familiar with IPSec, can't provide much info.

#7 - 19.07.2016 11:20 - Tobias Brunner

> Is not this one? "source of the bug / misinterpretation: https://tools.ietf.org/html/rfc5996#page-30"

No, that does not explain anything. Nothing there is ambiguous and open for misinterpretation.

> Sorry, I am not so familiar with IPSec, can't provide much info.

Then ask Cisco what their box is doing. Since you obviously paid them money exactly for this occasion, no?

#8 - 19.07.2016 11:28 - Kris Jobs

Tobias Brunner wrote:

> > Is not this one? "source of the bug / misinterpretation: https://tools.ietf.org/html/rfc5996#page-30"
>
> No, that does not explain anything. Nothing there is ambiguous and open for misinterpretation.
>
> > Sorry, I am not so familiar with IPSec, can't provide much info.
>
> Then ask Cisco what their box is doing. Since you obviously paid them money exactly for this occasion, no?

Thanks for the replies, since have no active contact with Cisco, I just don't go to Cisco's support.

#9 - 19.07.2016 11:46 - Tobias Brunner

> > > Sorry, I am not so familiar with IPSec, can't provide much info.
> >
> > Then ask Cisco what their box is doing. Since you obviously paid them money exactly for this occasion, no?
>
> Thanks for the replies, since have no active contact with Cisco, I just don't go to Cisco's support.

I see. As responder strongSwan can't do much else but to respond to the requests by the peer. Without knowing what exactly triggers the CRATE_CHILD_SA exchange every minute we can't really change anything. However, in the Cisco log there is this: delayed (60000 msec) message ACL for always up maps, which indicates it is configured to do something after 60s - but I'm not familiar with iOS, so I don't really know what a *message ACL* or an *always up map* is or why it could be delayed, or why an additional SA is created if one with the same traffic selectors was established already with the IKE_SA earlier.

#10 - 31.05.2017 00:46 - Noel Kuntze

- Status changed from Feedback to Closed

- Resolution set to No feedback