strongSwan - Issue #1245

SPD with incorrect reqid is inserted when SAD created

23.12.2015 04:27 - heidi rao

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.3.5	**Resolution:**	No feedback

Description

Hi,
I configured connection on two host.

```
Initiator

conn RULEABC-1~VPNABC-1
        rekeymargin=600
        rekeyfuzz=100%
        keyexchange=ikev2
        left=35.6.6.205
        right=35.6.6.105
        leftsubnet=*_35.6.6.128/25_*
        rightsubnet=*_35.6.6.0/25_*
        leftprotoport=1
        rightprotoport=1
        authby=secret
        leftid=35.6.6.205
        rightid=%any
        ike=3des-sha1-modp2048!
        esp=3des-sha1!
        type=tunnel
        ikelifetime=6000s
        keylife=6000s
        mobike=no
        auto=route
        reauth=no

Responder

conn RULEABC-1~VPNABC-1
        rekeymargin=600
        rekeyfuzz=100%
        keyexchange=ikev2
        right=35.6.6.205
        left=35.6.6.105
        rightsubnet=*_35.6.6.0/24_*
        leftsubnet=*_35.6.6.0/24_*
        leftprotoport=1
        rightprotoport=1
        authby=secret
        leftid=35.6.6.105
        rightid=%any
        ike=3des-sha1-modp2048!
        esp=3des-sha1!
        type=tunnel
        ikelifetime=6000s
        keylife=6000s
        mobike=no
        auto=route
        reauth=no
```

After command "ipsec start" on responder, the SPD on initiator is as blow, the reqid is 2.

```
# ip xfrm policy
src 35.6.6.0/24 dst 35.6.6.0/24 proto icmp
        dir fwd priority 2882 ptype main
        tmpl src 35.6.6.205 dst 35.6.6.105
                proto esp reqid 2 mode tunnel
src 35.6.6.0/24 dst 35.6.6.0/24 proto icmp
        dir in priority 2882 ptype main
        tmpl src 35.6.6.205 dst 35.6.6.105
                proto esp reqid 2 mode tunnel
src 35.6.6.0/24 dst 35.6.6.0/24 proto icmp
        dir out priority 2882 ptype main
        tmpl src 35.6.6.105 dst 35.6.6.205
                proto esp reqid 2 mode tunnel
```

After command "ping 35.6.6.106 -I 35.6.6.206" on initiator, SPD on initiator is as blow, both SPD with mask 24 and mask 25 use reqid 2.

```
src 35.6.6.128/25 dst 35.6.6.0/25 proto icmp
        dir fwd priority 2874 ptype main
        tmpl src 35.6.6.205 dst 35.6.6.105
                proto esp *_reqid 2_* mode tunnel
src 35.6.6.128/25 dst 35.6.6.0/25 proto icmp
        dir in priority 2874 ptype main
        tmpl src 35.6.6.205 dst 35.6.6.105
                proto esp *_reqid 2_* mode tunnel
src 35.6.6.0/25 dst 35.6.6.128/25 proto icmp
        dir out priority 2874 ptype main
        tmpl src 35.6.6.105 dst 35.6.6.205
                proto esp *_reqid 2_* mode tunnel
src 35.6.6.0/24 dst 35.6.6.0/24 proto icmp
        dir fwd priority 2882 ptype main
        tmpl src 35.6.6.205 dst 35.6.6.105
                proto esp *_reqid 2_* mode tunnel
src 35.6.6.0/24 dst 35.6.6.0/24 proto icmp
        dir in priority 2882 ptype main
        tmpl src 35.6.6.205 dst 35.6.6.105
                proto esp *_reqid 2_* mode tunnel
src 35.6.6.0/24 dst 35.6.6.0/24 proto icmp
        dir out priority 2882 ptype main
        tmpl src 35.6.6.105 dst 35.6.6.205
                proto esp *_reqid 2_* mode tunnel

#ip xfrm state
src 35.6.6.105 dst 35.6.6.205
        proto esp spi 0xca474529 reqid 2 mode tunnel
        replay-window 32 flag 20
        auth hmac(sha1) 0xd0e3d14ec9b971095bce45ae45209f6e7041e76e
        enc cbc(des3_ede) 0x62453c137b81ea5da5c773e456f371f4e0ce9fcf9d57e2db
src 35.6.6.205 dst 35.6.6.105
        proto esp spi 0xcd79b716 reqid 2 mode tunnel
        replay-window 32 flag 20
        auth hmac(sha1) 0x7336dfaf6d8bea242820ae4b94006c40148f3240
        enc cbc(des3_ede) 0xc30ef161e8cb0cdd5a6c9f326ca3a1e411c5b4d1754c265b
```

Then execute "ping 35.6.6.20 -I 35.6.6.30", it match the SPD with mask 24, so it use the SAD (spi 0xcd79b716), the traffic fail.

Heidi

History

#1 - 23.12.2015 14:40 - Tobias Brunner

- Status changed from New to Feedback

- Priority changed from High to Normal

Yes, this is one of the issues when narrowing is used with *auto=route*. I guess this only really works with transport mode SAs as there the SA itself has a selector applied, which prevents traffic matching the trap policy but not the actual IPsec policy from using such an SA. Since a relative recent change all the traffic selectors are passed to the code that installs the SAs, we could use that information and also install selectors for tunnel mode SAs in case there is only one local and remote TS (the Linux kernel only supports one selector per SA).

#2 - 11.01.2019 23:46 - Noel Kuntze

- Category set to configuration

- Status changed from Feedback to Closed

- Resolution set to No feedback