strongSwan - Issue #2125

Priority of SPD will be updated after SAD created

28.09.2016 12:43 - Xiaoqiang Fu

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	kernel-interface		
Affected version:	5.5.0	**Resolution:**	Duplicate

Description

Hi,
I have found the issue [[https://wiki.strongswan.org/issues/1243]] in the history.
There is still such issue in 5.5.0, do we have any plan for fixing this issue?
Or do we have any method to avoid such issue?

Thanks!
Br,
Ferry

Related issues:

Is duplicate of Feature #1243: Add support for overlapping trap policies	**Closed**	**22.12.2015**

History

#1 - 28.09.2016 16:39 - Tobias Brunner

- Status changed from New to Feedback

What issue do you have exactly?

#2 - 29.09.2016 04:16 - Xiaoqiang Fu

two connections are configured as below:

```
conn ferry-test~ferry-test
        rekeymargin=6
        rekeyfuzz=100%
        keyexchange=ikev2
    left=44.65.21.98
        right=52.4.17.98
        leftsubnet=44.65.21.99/32
        rightsubnet=52.4.17.99/32
        authby=secret
        leftid=44.65.21.98
        rightid=%any
        ike=3des-sha256-modp768!
        esp=3des-sha1-noesn!
        type=tunnel
        ikelifetime=6000s
        keylife=6000s
        mobike=no
        auto=route
        replay_window=256
        reauth=no

conn priority-test~ferry-test
        rekeymargin=6
        rekeyfuzz=100%
        keyexchange=ikev2
        left=44.65.21.100
        right=52.4.17.100
        leftsubnet=44.65.21.0/24
        rightsubnet=52.4.17.0/24
        authby=secret
    leftid=44.65.21.100
        rightid=%any
        ike=3des-sha256-modp768!
```

```
        esp=3des-sha1-noesn!
        type=tunnel
        ikelifetime=6000s
        keylife=6000s
        mobike=no
        auto=route
        replay_window=256
        reauth=no

[root@24F-VFPC-065 ~]# ipsec status
Routed Connections:
priority-test~ferry-test{2}:  ROUTED, TUNNEL, reqid 2
priority-test~ferry-test{2}:   44.65.21.0/24 === 52.4.17.0/24
ferry-test~ferry-test{1}:  ROUTED, TUNNEL, reqid 1
ferry-test~ferry-test{1}:   44.65.21.99/32 === 52.4.17.99/32
Security Associations (0 up, 0 connecting):
  none
```

After "ipsec restart", the SPD is shown as below, we can see the SPD with 32 mask has higher priority(283616) than the priority(287712)with 24 mask.

```
[root@24F-VFPC-065 ~]# ip xfrm policy
src 44.65.21.0/24 dst 52.4.17.0/24
    dir fwd priority 287712 ptype main
src 52.4.17.0/24 dst 44.65.21.0/24
    dir fwd priority 287712 ptype main
    tmpl src 52.4.17.100 dst 44.65.21.100
        proto esp reqid 2 mode tunnel
src 52.4.17.0/24 dst 44.65.21.0/24
    dir in priority 287712 ptype main
    tmpl src 52.4.17.100 dst 44.65.21.100
        proto esp reqid 2 mode tunnel
src 44.65.21.0/24 dst 52.4.17.0/24
    dir out priority 287712 ptype main
    tmpl src 44.65.21.100 dst 52.4.17.100
        proto esp reqid 2 mode tunnel
src 44.65.21.99/32 dst 52.4.17.99/32
    dir fwd priority 283616 ptype main
src 52.4.17.99/32 dst 44.65.21.99/32
    dir fwd priority 283616 ptype main
    tmpl src 52.4.17.98 dst 44.65.21.98
        proto esp reqid 1 mode tunnel
src 52.4.17.99/32 dst 44.65.21.99/32
    dir in priority 283616 ptype main
    tmpl src 52.4.17.98 dst 44.65.21.98
        proto esp reqid 1 mode tunnel
src 44.65.21.99/32 dst 52.4.17.99/32
    dir out priority 283616 ptype main
    tmpl src 44.65.21.98 dst 52.4.17.98
        proto esp reqid 1 mode tunnel
```

Then I execute command like "ping 52.4.17.3 -I 44.65.21.3", the SPD priority with 24 mask is updated to 187712 which is higher than priority(283616) with 32 mask.

```
[root@24F-VFPC-065 ~]# ip xfrm policy
src 44.65.21.0/24 dst 52.4.17.0/24
    dir fwd priority 287712 ptype main
src 52.4.17.0/24 dst 44.65.21.0/24
    dir fwd priority 187712 ptype main
    tmpl src 52.4.17.100 dst 44.65.21.100
        proto esp reqid 2 mode tunnel
src 52.4.17.0/24 dst 44.65.21.0/24
    dir in priority 187712 ptype main
    tmpl src 52.4.17.100 dst 44.65.21.100
        proto esp reqid 2 mode tunnel
src 44.65.21.0/24 dst 52.4.17.0/24
    dir out priority 187712 ptype main
    tmpl src 44.65.21.100 dst 52.4.17.100
        proto esp reqid 2 mode tunnel
src 44.65.21.99/32 dst 52.4.17.99/32
    dir fwd priority 283616 ptype main
src 52.4.17.99/32 dst 44.65.21.99/32
    dir fwd priority 283616 ptype main
    tmpl src 52.4.17.98 dst 44.65.21.98
```

```
        proto esp reqid 1 mode tunnel
src 52.4.17.99/32 dst 44.65.21.99/32
    dir in priority 283616 ptype main
    tmpl src 52.4.17.98 dst 44.65.21.98
        proto esp reqid 1 mode tunnel
src 44.65.21.99/32 dst 52.4.17.99/32
    dir out priority 283616 ptype main
    tmpl src 44.65.21.98 dst 52.4.17.98
        proto esp reqid 1 mode tunnel

[root@24F-VFPC-065 ~]# ipsec status
Routed Connections:
priority-test~ferry-test{2}:  ROUTED, TUNNEL, reqid 2
priority-test~ferry-test{2}:   44.65.21.0/24 === 52.4.17.0/24
ferry-test~ferry-test{1}:  ROUTED, TUNNEL, reqid 1
ferry-test~ferry-test{1}:   44.65.21.99/32 === 52.4.17.99/32
Security Associations (1 up, 0 connecting):
priority-test~ferry-test[1]: ESTABLISHED 3 minutes ago, 44.65.21.100[44.65.21.100]...52.4.17.100[52.4.17.100]
priority-test~ferry-test{3}:  INSTALLED, TUNNEL, reqid 2, ESP SPIs: cecbb519_i c5c64325_o
priority-test~ferry-test{3}:   44.65.21.0/24 === 52.4.17.0/24
```

Then I execute "ping 52.4.17.99 -I 44.65.21.99", it always match the SPD with 24 mask. In other words, Routed connection "ferry-test~ferry-test" can not be up anymore by ping method.

```
[root@24F-VFPC-065 ~]#ip xfrm policy
src 44.65.21.0/24 dst 52.4.17.0/24
    dir fwd priority 287712 ptype main
src 52.4.17.0/24 dst 44.65.21.0/24
    dir fwd priority 187712 ptype main
    tmpl src 52.4.17.100 dst 44.65.21.100
        proto esp reqid 2 mode tunnel
src 52.4.17.0/24 dst 44.65.21.0/24
    dir in priority 187712 ptype main
    tmpl src 52.4.17.100 dst 44.65.21.100
        proto esp reqid 2 mode tunnel
src 44.65.21.0/24 dst 52.4.17.0/24
    dir out priority 187712 ptype main
    tmpl src 44.65.21.100 dst 52.4.17.100
        proto esp reqid 2 mode tunnel
src 44.65.21.99/32 dst 52.4.17.99/32
    dir fwd priority 283616 ptype main
src 52.4.17.99/32 dst 44.65.21.99/32
    dir fwd priority 283616 ptype main
    tmpl src 52.4.17.98 dst 44.65.21.98
        proto esp reqid 1 mode tunnel
src 52.4.17.99/32 dst 44.65.21.99/32
    dir in priority 283616 ptype main
    tmpl src 52.4.17.98 dst 44.65.21.98
        proto esp reqid 1 mode tunnel
src 44.65.21.99/32 dst 52.4.17.99/32
    dir out priority 283616 ptype main
    tmpl src 44.65.21.98 dst 52.4.17.98
        proto esp reqid 1 mode tunnel

[root@24F-VFPC-065 ~]# ipsec status
Routed Connections:
priority-test~ferry-test{2}:  ROUTED, TUNNEL, reqid 2
priority-test~ferry-test{2}:   44.65.21.0/24 === 52.4.17.0/24
ferry-test~ferry-test{1}:  ROUTED, TUNNEL, reqid 1
ferry-test~ferry-test{1}:   44.65.21.99/32 === 52.4.17.99/32
Security Associations (1 up, 0 connecting):
priority-test~ferry-test[1]: ESTABLISHED 8 minutes ago, 44.65.21.100[44.65.21.100]...52.4.17.100[52.4.17.100]
priority-test~ferry-test{3}:  INSTALLED, TUNNEL, reqid 2, ESP SPIs: cecbb519_i c5c64325_o
priority-test~ferry-test{3}:   44.65.21.0/24 === 52.4.17.0/24
```

#3 - 29.09.2016 10:06 - Tobias Brunner

- Is duplicate of Feature #1243: Add support for overlapping trap policies added

#4 - 29.09.2016 10:06 - Tobias Brunner

- Category set to kernel-interface

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Duplicate

OK, yes that's the same issue as the one described in #1243, which is due to the traffic selector overlap and how the priorities for trap policies are calculated. I'm closing this issue as a duplicate so we can track it in one place.

A possible workaround is to define the larger traffic selector so that it excludes the smaller traffic selector. Doesn't look nice when excluding single hosts, but should work (in this case you could define *leftsubnet=44.65.21.1/32,44.65.21.2/31,44.65.21.4/30,44.65.21.8/29,44.65.21.16/28,44.65.21.32/27,44.65.21.64/27,44.65.21.96/31,44.65.21.98/32,44.65.21.100/30,44.65.21.104/29,44.65.21.112/28,44.65.21.128/25* and *rightsubnet=52.4.17.1/32,52.4.17.2/31,52.4.17.4/30,52.4.17.8/29,52.4.17.16/28,52.4.17.32/27,52.4.17.64/27,52.4.17.96/31,52.4.17.98/32,52.4.17.100/30,52.4.17.104/29,52.4.17.112/28,52.4.17.128/25*).

Another possible workaround is using vici/swanctl.conf and manual priorities.

#5 - 29.09.2016 10:45 - Xiaoqiang Fu

Could you describe the workaround method in detail?
How to specify these ip address for the leftsubnet and right subnet?

#6 - 29.09.2016 13:15 - Tobias Brunner

> How to specify these ip address for the leftsubnet and right subnet?

What do you mean? Just configure them as described above.

If you, alternatively, want to use manual priorities you have to switch from ipsec.conf to a vici based config (e.g. swanctl.conf).

#7 - 30.09.2016 04:06 - Xiaoqiang Fu

Tobias Brunner wrote:

> > How to specify these ip address for the leftsubnet and right subnet?
>
> What do you mean? Just configure them as described above.
>
> If you, alternatively, want to use manual priorities you have to switch from ipsec.conf to a vici based config (e.g. swanctl.conf).

I can not fully understand why these IPs are configured as leftsubnet and rightsubnet, is there any rules for choosing the IP and subnet mask?

#8 - 30.09.2016 09:44 - Tobias Brunner

> I can not fully understand why these IPs are configured as leftsubnet and rightsubnet, is there any rules for choosing the IP and subnet mask?

Yes, you define them in a way that they cover all addresses expect the one(s) from the smaller traffic selector. In your example and referring to *leftsubnet* that's all the subnets in the ranges *44.65.21.0 - 44.65.21.98* and *44.65.21.100 - 44.65.21.255* (i.e. the complete *44.65.21.0/24* subnet except *44.65.21.99*).