strongSwan - Issue #758

Strongswan only receives one traffic selector for remote subnet that has several IPs in it.

04.11.2014 15:36 - Matthew Pilon

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	charon		
Affected version:	5.1.2	**Resolution:**	No change required

Description

Hi Tobias-

I am wondering what is my issue here.

Running strongSwan 5.1.2 on a cloud server.

Successfully connecting Windows and OSX clients using a private subnet.

Successfully connecting my cloud server as gateway to a larger network that is using a Cisco ASA VPN as the interface that handles our site to site connection.

Cisco ASA assigns a fixed private IP (172.xx.x.250) to our gateway running strongSwan within the larger remote network .

We NAT all of our outgoing traffic for our private subnet to the private IP (172.xx.x.250) so that our private subnet can access internal resources on the larger remote network.

This **almost** works. We can see one (and only one) of the remote internal resources determined by what we set as first item in the right subnet parameter in the "strongswan_to_cisco" connection. If we try to to specify more resources in the remote subnet it fails to match a traffic selector. It only matches the first subnet in the right subnet parameter, and the order matters--first always wins. The first subnet works perfectly, but none of the others work...

Apparently this is a problem with my configuration related to how traffic selectors are doled out, but I am lost.

IPSEC.CONF

```
config setup
        keyexchange=ikev2
        nat_traversal=yes
        ikelifetime=86400s
        lifetime=28800s
        rekeymargin=3m
        keyingtries=10
        compress=yes
conn strongswan_to_cisco
        dpdaction=restart
        type=tunnel
        auto=start
        leftauth=psk
        leftid=54.XXX.XX.XX ## our strongSwan public IP.
        leftsubnet=172.xx.x.250/32 ## The IP assigned to our Gateway on the Cisco VPN
        lefthostaccess=yes
        right=65.XXX.XX.XX  ## Public IP of the Cisco VPN device
        rightsubnet=10.zzz.zz.70/32,10.zzz.zz.11/32
        rightauth=psk
        ike=3des-sha1-modp1024
        esp=3des-sha1-modp1024
conn ios
        ...

conn win
        ...
```

SYSLOG

```
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[CFG] received proposals: ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT
_SEQ
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[CFG] configured proposals: ESP:3DES_CBC/HMAC_SHA1_96/MODP
_1024/NO_EXT_SEQ, ESP:AES_CBC_128/AES_CBC_192/AES_CBC_256/3DES_CBC/BLOWFISH_CBC_256/HMAC_SHA1_96/A
ES_X
CBC_96/HMAC_MD5_96/NO_EXT_SEQ
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[CFG] selected proposal: ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_
SEQ
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[CFG] selecting traffic selectors for us:
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[CFG]  config: 172.xx.x.250/32, received: 172.xx.x.250/32
=> match: 172.xx.x.250/32
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[CFG] selecting traffic selectors for other:
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[CFG]  config: 10.zzz.zz.70/32, received: 10.zzz.zz.70/32
=> match: 10.zzz.zz.70/32
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[CFG]  config: 10.zzz.zz.11/32, received: 10.zzz.zz.70/32
=> no match
Nov  4 14:20:15 ip-10-0-0-190 charon: 02[IKE] CHILD_SA strongswan_to_cisco{1} established with SPI
s cf0f4980_i 1958e37a_o and TS 172.xx.x.250/32 === 10.zzz.zz.70/32
```

History

#1 - 05.11.2014 10:33 - Martin Willi

- Status changed from New to Feedback

- Assignee deleted (Tobias Brunner)

Hi,

> rightsubnet=10.zzz.zz.70/32,10.zzz.zz.11/32

> ```
> 02[CFG] selecting traffic selectors for other:
> 02[CFG]  config: 10.zzz.zz.70/32, received: 10.zzz.zz.70/32 => match: 10.zzz.zz.70/32
> 02[CFG]  config: 10.zzz.zz.11/32, received: 10.zzz.zz.70/32 => no match
> 02[IKE] CHILD_SA strongswan_to_cisco{1} established with SPIs cf0f4980_i 1958e37a_o and TS 172.xx.x.250/32
>  === 10.zzz.zz.70/32
> ```

While you are offering two subnets, it seems that your responder selects only a subnset of the proposed selectors. This is valid in IKEv2, and called traffic selector narrowing.

Check your responder configuration for its traffic selector configuration. You most likely need to include both subnets there as well.

Regards
Martin

#2 - 05.11.2014 10:58 - Tobias Brunner

> Check your responder configuration for its traffic selector configuration. You most likely need to include both subnets there as well.

As a workaround you could probably also define separate connections for each remote subnet, like so:

```
conn strongswan_to_cisco
        dpdaction=restart
        type=tunnel
        # no auto here
        leftauth=psk
        leftid=54.XXX.XX.XX ## our strongSwan public IP.
        leftsubnet=172.xx.x.250/32 ## The IP assigned to our Gateway on the Cisco VPN
        lefthostaccess=yes
        right=65.XXX.XX.XX  ## Public IP of the Cisco VPN device
        # no rightsubnet here
        rightauth=psk
        ike=3des-sha1-modp1024
        esp=3des-sha1-modp1024

conn strongswan_to_cisco_1
```

```
        also=strongswan_to_cisco
        rightsubnet=10.zzz.zz.70/32
        auto=start

conn strongswan_to_cisco_2
        also=strongswan_to_cisco
        rightsubnet=10.zzz.zz.11/32
        auto=start
```

#3 - 05.11.2014 18:33 - Matthew Pilon

Thanks much for these suggestions.

> Check your responder configuration for its traffic selector configuration. You most likely need to include both subnets there as well.

There is a little bit of an access issue there, but thanks for the suggestion. But also, if it were the case that the responder did not have both subnets included, then it would only match the same internal resource on the responder side every time, but that doesn't happen. It only matches the first address suggested by the "rightsubnet" parameter. If I set "rightsubnet" to 0.0.0.0/0 we just get the remote internal resource available to us that is numerically the first IP, in this case 10.zzz.zz.11/32.

> As a workaround you could probably also define separate connections for each remote subnet, like so:

Sweet!

#4 - 07.07.2015 15:40 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to No change required

#5 - 30.10.2015 00:24 - Anonymous

actually this is still a bit of a problem for example when connecting to AWS VPC VPN and/or a hardware VPN solution
AWS VPC only supports sending all subnets over the same SA. when setting up a different connection a new SA is negotiated and traffic is being dropped. for example if you need the tunnel IPs (169.x) **AND** the actual VPC subnet to work. One can still accomplish this by manually adding the xfrm policies after the tunnel is established or some hacky updown script. but that's not that clean and probably for a lot of people not doable. I'd imagine the fix for this wouldn't be too difficult since all that's needed is the additional xfrm policys for the same reqid....